

RFP for Acquiring Technology & Services Of Social Media Threats For The Boston Police Department Released 05-Oct-16



Verint Technology Inc.
Response to RFP
Dated 31-Oct-16

Table of Contents

1	EXECUTIVE SUMMARY	6
2	SYSTEM PROPOSAL	8
2.1	FORWARD.....	8
2.2	THE CHALLENGE OF TODAY’S INTELLIGENCE.....	8
2.3	CONDUCTING INVESTIGATIONS IN A MULTI-WEB SOURCES BIG DATA ENVIRONMENT	9
2.3.1	<i>Data Overload</i>	9
2.3.2	<i>Data Credibility</i>	10
2.3.3	<i>Globalization</i>	10
2.3.4	<i>Call for a Distinct Investigation Approach</i>	10
2.3.5	<i>Towards a Solution</i>	11
2.4	VERINT® WEBINT™ SOLUTION OVERVIEW.....	11
2.5	VERINT® WEBINT™ ARCHITECTURE.....	14
2.6	WEBINT-COLLECT	14
2.6.1	<i>Deep & Dark Web Collection Methods</i>	16
2.6.1.1	<i>Deep Web Access</i>	16
2.6.1.2	<i>Dark Web Access</i>	16
2.6.2	<i>Covert Collection of Web Data</i>	17
2.6.2.1	<i>User Behavior Emulation</i>	17
2.6.2.2	<i>Browser Type Emulation</i>	17
2.6.2.3	<i>Overcome Error Messages and CAPTCHA</i>	18
2.6.2.4	<i>Meet Website Policy and Limitations</i>	19
2.6.2.5	<i>Web Strategy</i>	19
2.6.2.6	<i>Layered Architecture Summary</i>	20
2.6.3	<i>Scalable Architecture</i>	21
2.6.4	<i>Intuitive Graphical Designer for Webflow (Robot) Design</i>	21
2.6.5	<i>Continuous & Robust Collection</i>	22
2.6.5.1	<i>Collection task management</i>	22
2.6.5.2	<i>Virtual Agent (Avatar) Management</i>	23
2.6.5.3	<i>Proxy Management</i>	24
2.6.5.4	<i>Pooling System Resources to Support Enhanced Collection Strategies</i>	24
2.6.6	<i>Command & Control Monitoring Capabilities</i>	25
2.6.6.1	<i>Collection Management Monitoring</i>	25
2.6.6.2	<i>Easy Dashboard Setup</i>	25
2.6.6.2.1	<i>Crawler Monitors</i>	25
2.6.6.2.2	<i>Collection Reports</i>	26
2.6.7	<i>Web Data Extraction Methods</i>	26
2.6.7.1	<i>Scenario-based Web Data Extraction (Structured Data Web Extraction)</i>	26
2.6.7.2	<i>Scenario-less Web Data Collection (Unstructured Collection)</i>	26
2.6.8	<i>Data Collection Engines</i>	27
2.6.8.1	<i>Static Web Page Engines</i>	27
2.6.8.2	<i>RSS-based Collection Engines</i>	27

2.6.8.3	Browser-based Engines.....	27
2.6.8.4	Website API-based Engines	27
2.6.8.5	API Stream-based Engines.....	28
2.6.9	Built-in Webflows for Collecting Data from the Major Websites.....	28
2.6.10	WebInt-Collect Main Components.....	29
2.7	WEBINT-INVESTIGATE.....	30
2.7.1	Analysis and Research.....	32
2.7.1.1	Data Search & Discovery	32
2.7.1.1.1	Simple and Advanced Textual Searches	33
2.7.1.1.2	Facet-based Discovery.....	33
2.7.1.1.3	Geospatial Searches	34
2.7.1.2	Visual Link Analysis.....	34
2.7.1.3	Geospatial Analysis.....	35
2.7.1.4	Social Analysis.....	35
2.7.1.5	Text Analysis	35
2.7.1.6	Entity Resolution Analysis.....	35
2.7.2	Managing the Investigation Process.....	36
2.7.2.1	Investigation Management	36
2.7.2.2	Investigation Overview Dashboard.....	37
2.7.2.3	Target View.....	38
2.7.2.4	Summary Reports	38
2.7.2.5	Search-Based Alerts.....	39
2.7.2.6	Collaboration	39
2.7.2.7	Security and Compartmentalization	39
2.7.3	Person Identify Search.....	40
2.7.4	Fully Integrated with the Collection Platform	41
2.7.4.1	Reconstruction of a Web Profile	42
2.8	WEBINT BROWSER ADD-ON	43
2.8.1	Enhanced Security Environment.....	43
2.8.2	Avatar Management.....	43
2.8.3	Added layers of information	44
2.8.4	Extracting Content While Browsing	45
2.9	WEBINT-CONNECTIVITY LAYER	45
2.9.1	Manage and Control Collected Data Distribution.....	46
2.9.2	Security.....	46
2.9.3	Cleaning and Cleansing Data	46
2.9.4	Ingesting, Modeling and Enriching Loaded Data	46
2.9.4.1	Enriching Data	46
2.9.4.2	Distributing Data	47
2.9.5	WebInt-CENTER API	47
2.10	INTRODUCTION TO VERINT® WEBALERT™	48
2.10.1	Web Alert Functions	48
2.10.2	Web Alert Benefits.....	49
2.10.3	Data Channels.....	49
2.10.4	Languages and Emojis	50

2.11	WEBALERT SYSTEM FEATURES.....	50
2.11.1	Queries.....	51
2.11.2	Live Monitoring.....	53
2.11.3	Alerts.....	55
2.11.4	People.....	56
2.11.5	Subjects.....	58
2.11.6	Historic Search.....	58
2.11.7	Tags.....	59
2.11.8	Image Retention.....	59
2.11.9	Reports.....	59
2.11.10	Top Authors View.....	59
2.11.11	Sentiment Analysis.....	59
2.11.12	Capture Screenshot of Posts.....	59
2.12	WEBALERT TECHNICAL OVERVIEW.....	59
2.12.1	Architecture Flow.....	60
2.12.2	Technical Capabilities.....	60
2.12.3	Backfill & History.....	61
2.12.4	Technical Requirements.....	61
2.12.5	Security.....	61
2.12.6	Data Policy.....	61
2.12.7	User Levels.....	62
2.13	PROPOSED SOLUTION FOR BOSTON PD.....	63
2.13.1	Verint® WebInt™ - Collect Configuration.....	63
2.13.2	Verint® WebInt™ - Analytics Configuration.....	63
2.13.3	Verint® WebInt™ - Web Flows.....	64
2.13.4	Verint® WebInt™ - Hardware.....	64
2.13.4.1	Collection Server.....	65
2.13.4.2	Analytics Server.....	66
2.13.4.3	Indexing Server.....	67
2.13.4.4	Management Server.....	68
2.13.4.5	Geo Server.....	69
2.13.5	Verint® WebInt™ - OS & Third Party Software.....	69
2.13.6	Verint® WebAlert™ - SaaS Configuration.....	70
2.14	RESPONSE TO RFP SECTION 7A – OVERVIEW.....	72
2.14.1	Proactive Alert/ Warning Capabilities.....	73
2.14.2	Analysis/ Crowdsourcing/ Social Threat Monitoring.....	73
2.14.3	Investigative Capabilities For Public Safety.....	73
3	TECHNICAL DESCRIPTION.....	74
3.1	RESPONSE TO RFP SECTIONS 7B & SECTIONS 8C-G.....	74
3.1.1	Summary Requirement 1 – Collection (RFP Section 7B1).....	74
3.1.2	Summary Requirement 2 – Analysis (RFP Section 7B2).....	86
3.1.2.1	Plan of Services – Analysis (RFP Section 8D).....	89
3.1.3	Summary Requirement 3 – Investigative (RFP Section 7B3).....	98
3.1.3.1	Plan of Services – Investigative (RFP Section 8E).....	100

3.1.4	Summary Requirement 4 – Geospatial (RFP Section 7B4).....	105
3.1.4.1	Plan of Services – Geo Spatial (RFP Section 8F)	107
3.1.5	Summary Requirement 5 – Administrative (RFP Section 7B5)	109
3.1.5.1	Plan of Services – Administrative (RFP Section 8G)	111
4	IMPLEMENTATION PLAN	114
4.1	PROJECT MANAGEMENT PROCESSES & PROGRAMS	114
4.2	PROJECT SCOPING PROCESS.....	114
4.3	PROJECT STRATEGY PLANNING.....	115
4.4	PROJECT EXECUTION PROCESS.....	115
4.5	PROJECT GO LIVE PLAN & STRATEGY	117
4.5.1	Overview	117
4.5.2	Key Elements.....	117
4.5.3	Success Criteria	118
4.6	PROJECT COMMUNICATION & COOPERATION WITH CUSTOMER.....	118
4.7	TYPICAL SOW TIMELINE	119
4.8	SUPPORT SERVICES OFFERED.....	120
4.8.1	Definitions.....	120
4.8.2	Scope of Services.....	122
4.8.2.1	Help Desk.....	122
4.8.2.2	Remote Access.....	123
4.8.2.3	On Site Support.....	123
4.8.2.4	Software Maintenance	123
4.8.2.5	Collected Web Site Changes	124
4.8.2.6	Collected Web Site Change – Tracing	124
4.8.2.7	Collected Web Site Change – Coverage	124
4.8.2.7.1	Problem Correction.....	125
4.8.2.7.2	Upgrades.....	125
4.8.2.8	Antivirus Software Maintenance Policy.....	126
4.8.2.9	Hardware Maintenance (If H/W provided by Verint)	126
4.8.2.9.1	Hardware Repair	126
4.8.2.9.2	SWAP – Replacement of Critical Part	126
4.8.2.9.3	Repair Material Authorization (RMA) Procedure	127
4.8.2.9.4	Packaging.....	127
4.8.2.9.5	Delivery.....	127
4.8.2.10	Third Party Software Installations	127
4.8.2.11	Life Cycle.....	128
4.8.3	Multi-Tier Problem Resolution	128
4.8.4	Support Plan Summary.....	130
4.8.5	Service Level Agreement Annual Cost	131
5	QUALIFICATIONS & EXPERIENCE	134
5.1	VERINT’S EXPERIENCE	134
5.2	RESPONSE TO RFP SECTIONS 8A & B	137
5.2.1	Plan of Services – Company (RFP Section 8A)	137

5.2.2	Plan of Services – Delivery & Implementation (RFP Section 8B)	146
6	FINANCIAL STATEMENTS	149
7	TRAINING PLAN	150
7.1	AVAILABLE PROFESSIONAL SERVICES	150
7.2	METHODOLOGY AND TRAINING	151
7.3	PROPOSED TRAINING AND PROFESSIONAL SERVICES	151
7.3.1	Verint® WebInt Training – Analytics (10 Days)	152
7.3.2	Verint® WebAlert Training	153
7.3.3	On-Site Analyst Training	154
8	SPECIFICATION SHEETS	157
9	REFERENCES	158
10	INSURANCE REQUIREMENTS	160
11	CITY OF BOSTON PROCURMENT FORMS (RFP SECTION 14)	162
11.1	STANDARD CONTRACT & GENERAL CONDITIONS (FORM CM-10 & 11)	162
11.2	CONTRACTOR CERTIFICATION (FORM CM-09)	163
11.3	CERTIFICATION OF AUTHORITY (FORM CM-06)	167
11.4	CORI (FORM CM-15A)	169
11.5	WAGE THEFT (FORM CM-16)	172
11.6	LIVING WAGE (FORM LW-2)	175
11.7	LIVING WAGE AFFIDAVIT (FORM LW-8)	179
12	PROFILE DOCUMENTS (RFP SECTION 3)	183
13	MINIMUM EVALUATION CRITERION (RFP SECTION 11)	187
14	APPENDIX	190

1 EXECUTIVE SUMMARY

Verint Technology Inc. (a wholly owned subsidiary of Verint Systems Inc.) is pleased to submit to the Boston Police Department (Boston PD) a proposal for an open source WEB Intelligence platform based on the Verint® Web Intelligence Center product line consisting of both our Verint® WebInt™ as well as our Verint® WebAlert™ products.

We are confident that the Verint® Web Intelligence Center platform will enable the Boston PD to analyze and investigate open source information collected from the Web and potentially additional sources in order to uncover potential threats and future trends. It is important to note the Verint Web Intelligence Center solution is a tool, and like any tool it is incumbent primarily on the user to ensure it is used in a lawful and appropriate manner. It is also important to acknowledge that technological changes by social media platforms, which may include increased encryption or reduced access to content, stress the importance of aligning with a vendor which can quickly respond and adjust to such activity. Verint is uniquely positioned to be that vendor to the Boston Regional Intelligence Center.

The end-to-end Verint® Web Intelligence Center solution collects and analyzes open-source Web content and transforms it into Actionable Intelligence®.

Verint® Web Intelligence Center applies the latest open-source Web intelligence methodologies to continuously access information from a multitude of open Web sources to extract and analyze the information contained therein.

Using the most advanced technologies available today, Verint® Web Intelligence Center streamlines the integration of the vast amounts of open-source Web data, generates new leads and tracks negative influencers, thus optimizing the investigation process. With the modular, scalable architecture and browser-based user interface of the solution, users do not have to install any applications when deploying the solution and therefore can keep IT involvement to a minimum.

Verint® Web Intelligence Center was specifically designed with the unique requirements of the intelligence, law enforcement and security communities in mind. Verint® Web Intelligence Center places a focus on the confidentiality of the investigation's process. The system topology and the crawling algorithms are developed in such a manner that even if one of the crawler's tasks is exposed, the investigation's target still remains covert.

From the data collaboration and information sharing point of view, the open architecture of the system enables smooth connectivity to other intelligence systems in the organization, using standard and proprietary protocols.

Unlike many other open-source Web intelligence solutions in the market, Verint® Web Intelligence Center offers an end-to-end turnkey solution with a single unified user management interface – both for data collection and data analysis. The benefits of this comprehensive solution are far beyond the sum of its parts – instead of inefficient and prone-to-error data transformation processes between the system modules, the integrated approach provides continuous and automatic interaction between the different subsystems, ultimately resulting in more relevant leads, increased detail about the topics and persons of interest and faster time to intelligence.

Verint is pleased to present this proposal while taking into account your requirements to the best of our understanding. If you find that some topics or features are not in line with the organization's workflow and requirements, we will be more than happy to jointly explore the necessary adjustments in order to reach the best fit to your needs.

This proposal document is structured according to the mandated RFP submittal requirements. The document has been organized in accordance with Section 9 of the RFP and follows the content and sequence as dictated.

Verint commits to provide the goods and services as outlined in the proposal for an amount not to exceed \$1,392,669.00 as mandated by the RFP.

Should you have any inquiries regarding this proposal, please do not hesitate to contact:

Chris Polito
Vice President, North America
Communications & Cyber Intelligence Solutions
Verint Systems Inc.
Email: Christopher.polito@verint.com

2 SYSTEM PROPOSAL

2.1 Forward

Open-source Web data can provide invaluable operational information and offer excellent opportunities for extracting target-based and public-behavior intelligence, making Internet monitoring valuable to any investigation workflow. Despite its extraordinary potential, the Internet poses a number of challenges to intelligence agencies around the world. To efficiently realize the tremendous potential of open-source Web data and transform it into usable intelligence, such agencies must deal with huge quantities of structured and unstructured information; inaccessible and unindexed deep web and dark net Web data; diverse applications, languages, and types of media; and the constant risk that investigations will be exposed.

Some of the main advantages of open-source Web intelligence:

- **Bypasses the Communications' Encryption Challenges**

As the threat of IP communications encryption becomes a reality, open-source Web intelligence offers a new source of unencrypted information, which should be used to complement existing legacy intelligence tools.

- **Does not depend on targets' means of communication or geographic location**

Regardless of how or where a target accesses the Web, open-source intelligence tools collect and analyze open-source data generated by the target.

- **Provides access to targets' historical data**

Unlike common methods of interception, which begin data collection only when a warrant has been issued, open-source intelligence tools can build a historical picture of a target's online activities.

- **Usually does not require warrants**

In most countries, data that is uploaded to the public Internet is available to all and can be investigated and collected without a warrant or court order.

2.2 The Challenge of Today's Intelligence

In today's complex world, intelligence operations face multiple challenges:

- Terror and crime are increasingly global, highly sophisticated, often not physical but virtual
- New digital technologies generate an exponential growth of data from multiple sources, often in incompatible formats, of varying type, structure, availability, reliability and value

- Ever greater expectations from government and the public for quick, effective and powerful law enforcement actions

In the face of these and other challenges, intelligence organizations struggle to process big data to find the needle in the haystack.



Figure 1 – Data Sources

The demand for a truly effective solution that delivers accurate, timely and actionable intelligence, which can be easily shared among local and international partners, has never been greater – or more urgent.

Introducing the Verint Web Intelligence Center – a single point of access to ALL web data to enable enterprise-wide investigation, management and analysis.

2.3 Conducting Investigations in a Multi-Web Sources Big Data Environment

2.3.1 Data Overload

Intelligence relevant for today's investigations needs to be garnered from enormous amounts of data. Gathered from highly specialized and sophisticated web sources,

Faced with the ever-increasing volume of data derived from web and social media activities on the open, deep, and dark web, it's no wonder that intelligence organizations struggle to effectively gather, merge, and distill the available information.

The ability to produce a clear, coherent picture from all diverse sources is both an immense challenge and an urgent necessity. Any solution designed to deliver accurate and timely intelligence must exploit the most

efficient automated analytics to unify this diverse data flow, creating a uniform language with a single point of access.

2.3.2 Data Credibility

Data relevancy is a critical parameter when attempting to solve crime. Am I looking at the right person? Did I gather their correct identifiers? Is my subject profile up-to-date?

In most cases, only a very small percentage of incoming or existing data is actually relevant to the current investigation. Linking data from multiple sources to any specific entity is complicated, because a single individual may be using multiple identities across multiple on-line and physical locations.

Intelligence is normally only partial information – sometimes unreliable and occasionally contradictory, depending on the source, its availability, and even previous interpretations.

Classification is also a critical factor, calling for increasingly efficient compartmentalization. Data type, data source, classification level, personnel level, access permissions, and ad hoc investigation needs must all be taken into consideration.

Investigators need assistance in focusing on the relevant data.

2.3.3 Globalization

The globalization of crime and terror and their increasing sophistication, taking place not only in the physical world but also in the virtual worlds, raises new technical obstacles for investigators: virtual web identities, encryption, dark-net, and virtual currencies.

The investigation landscape presents huge challenges: new spheres of crime (cybercrime, identity theft, etc.); source data processing (increasing volumes, velocity and variety, versus lower veracity and value) and the sheer size and depth of the data; and expectations on the part of government and the general public for quick, effective and powerful law enforcement – enabled by modern technology and increasingly trained manpower. As a result, law enforcement and intelligence agencies are placed under immense pressure, forcing a scale-up of their investigative abilities, in both scope and scale.

2.3.4 Call for a Distinct Investigation Approach

For each investigation, the truly decisive clues might be found by connecting completely different types of web data, and finding them sometimes requires a fresh approach and flexible work processes.

Content differs, too – at times, specific per suspect or event, and at other times, a mass of data with no clear direction. Investigation needs also affect the work requirements: for example, whether they apply to a past, present, or future event, to a known vs. unknown/hypothetical crime, to a specific thread, or to a search through masses of data.

Conventional investigation approaches based on relational databases are adequate for clear-cut query scenarios. But when the links and relationships become more complex, a conventional approach is insufficient

due to relational database limitations. This leads to the next issue in the investigation picture – there is rarely a fixed path or fixed scenario for intelligence analysis. Distinct investigation approaches are required.

2.3.5 Towards a Solution

Clearly, an advanced Web intelligence System is required to contend with multi-faceted needs, not only to support current source types and volumes, data unification, functionality and analytical needs, but also to prepare for unknown future factors and changing political and legal landscapes. Flexibility, openness, robustness, and maintainability are the essence of such a system, supporting differences between organizations, methodologies, and changing needs, above and beyond generic, industry-standard analytics systems.

Any such system must be able to seamlessly combine and fuse data, provide speedy access to meaningful intelligence, generate new insights that answer investigation needs, help identify emerging threats, and actively help to thwart them. A system of this level of sophistication must be highly usable, intuitive, and open to add-ons. It must be able to provide actionable intelligence, today and in the future. At the end of the day, the testing point of any such system will be its ability to deliver fast, accurate and insightful intelligence.

2.4 Verint[®] WebInt[™] Solution Overview

WebInt-CENTER consists of two integrated subsystems that autonomously interact with each other:

- **WebInt-COLLECT**

An advanced data extraction and collection solution, capable of extracting data from vast amounts of web sites. WebInt-COLLECT includes a simple and intuitive site and content definition tool, sophisticated scanning and collection engines, and virtually endless scalability to concurrently handle the ocean of data.

- **WebInt-INVESTIGATE**

Platform which analyses vast amounts of diverse, open-source content to enable rapid identification and tracking of events, targets, threats, and related activity. WebInt-INVESTIGATE combines' topic (top-down) and target (bottom-up) investigation mechanisms in one integrated solution.

The WebInt open-source Web intelligence solution offers these key benefits:

Best Fit for Intelligence and Security Organizations Needs

- An intelligence-driven design provides automated engines, rules, and workflows that serve the intelligence organization's tasks. Dedicated rule engines ensure the collection of relevant data only, while automated analysis mechanisms provide potential links, reveal new user identities, and generate alerts regarding suspect activities or users. Sophisticated search tools support access to Deep Web and Dark Web data, overcome anti-bot measures, and mimic human access behavior, to ultimately reach data that is otherwise blocked to search engines.

All-In-One Open-Source Web Intelligence Solution

- WebInt supports all stages of open-source Web Intelligence investigation, including data collection, data analysis, dossiers management, alert generation, and reporting.

Designed for the Dynamic World of the Social Networks

- The *Web Intelligence Center* suite is designed to give the analyst a set of tools to cope with the special challenges of analyzing the social media world, with vast amounts of information that need to be quickly analyzed and filtered into understandable data.

Built on Comprehensive Investigation Methodology

- Verint's experience and expertise in the intelligence solutions field assure that the system is built on field-proven, sophisticated, and logical investigation methodology that is integrated in the system workflow.

Topic investigation

- Topic analysis and general tracking of developments allow tracking general and specific group activities. Keeping track of mentions over the Web helps reduce surprise factors and can help maintain public safety.

Target investigation

- Target characterization provides immense background information; automated alerts reveal investigation leads, and interactive links and facets allow investigation drill-down. A Target unification approach unifies the various accounts of similar entities, actively proposing a relation between them, and possibly indicating the different accounts/names of the same target.

Scalable Topology

- Customers can start off with a system configuration designed to cover a specific scope of Web activity and targets, and over time expand to support increasing numbers of websites, targets, and data capacity.

Centralized Solution

- The centralized architecture enables centralized control of all collection units, storage of collected data, and complementary intelligence activities between mass and target analyses.

Worldwide Coverage

- Data can be harvested from virtually anywhere in the world, regardless of the target's geographical location.

Security and Confidentiality

- Customer anonymity and network security are preserved through decoupling of networks, dynamic use

of proxy servers, and more.

Verint Web Intelligence Center provides security specialists with centralized access to intelligence data from multiple web sources, offering them dedicated tools to investigate and identify potential threats of organized crime, terrorism, infrastructure sabotage, money-laundering, fraud and more.

Verint WebInt Center offers not only a viable technological solution, but also the methodology, functionality and know-how required to extract dedicated Actionable Intelligence®. This unique environment provides a complementary set of search and analysis tools to enable in-depth professional investigation.

ALL YOUR WEB DATA FUSED INTO ONE ACTIONABLE KNOWLEDGE BASE

Verint WebInt-CENTER enables you to:

- FOCUS ON WHAT'S RELEVANT
- GAIN FASTER TIME TO INTELLIGENCE
- REVEAL PREVIOUSLY UNAVAILABLE INTELLIGENCE
- CREATE GREATER SYNERGY AMONG TEAMS
- PRESERVE & ACCUMULATE KNOWLEDGE

And delivers the following benefits:

- SINGLE-POINT INTELLIGENCE ENVIRONMENT
- FASTER TIME TO INTELLIGENCE
- COLLABORATIVE POOL OF DATA
- SECURED & COMPARTMENTALIZED
- FLEXIBILITY & FUTURE-ORIENTED APPROACH

2.5 Verint® WebInt™ Architecture

Since its inception, Verint WebInt-CENTER has been geared up to meet the complex challenges of the intelligence organization in a fast moving and ever-changing environment. Based on both an intelligence-oriented technological and operational architecture, it promotes a highly effective user experience.

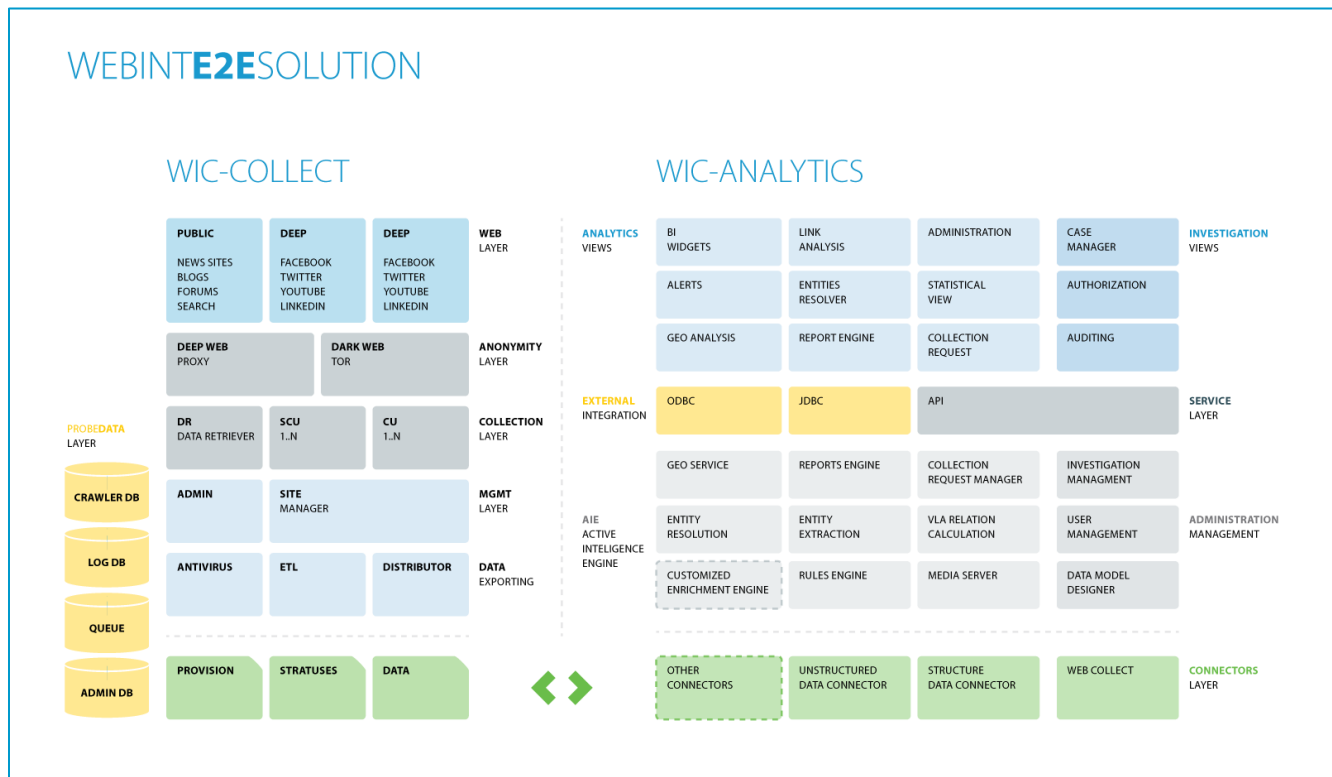


Figure 2 – WebInt-CENTER Architecture

2.6 WebInt-COLLECT

WebInt-Collect provides an independent, flexible, and scalable platform for extracting web content, along with advanced management solutions for operational monitoring.

This solution supports web data extraction from virtually any HTML-based website, offering site-specialized crawlers, sophisticated crawling capabilities and collection strategies.

The solution supports collection from Standard, Deep (including accessing password-protected websites) and Dark web.

The core architecture of the solution was designed to meet the security requirements of governmental agencies, including:

- Covert collection capabilities
- Network separations
- Access to private content
- Access to Dark web

WebInt-Collect manages large amounts of parallel collection tasks and utilizes the various platform collection resources (virtual agents, proxies, crawlers), while supporting a mechanism to automatically overcome failures.

The above set of capabilities enables support for a continuous, robust, and unattended 24x7 collection process.

Solution Highlights

Data Extraction from HTML-based Web Sources enables virtually full coverage of the data that matters

- WebInt-Collect is capable of managed extraction of data from virtually any HTML-based Web source, including social network sites, portals, forums, blogs, news, and more. Handles simple static HTML-based sites, rich dynamic Web pages, and even password-protected and dark websites.

Scalable Architecture to meet the new information extraction challenges the web is posing

- The platform's architecture easily incorporates additional crawling power. The system supports multiple, distributed crawler units; each crawler unit running several concurrent collection tasks – working synchronously, but still independently of one another.

Covert web data Extraction to protect your investigation

- The platform supports built-in tools to enable covert-crawling processes. The system crawling tools are implemented as layers on top of the Webflow (robot) collection, and various monitoring and evasion tactics are applied to enable crawlers to perform their tasks in a covert and unhindered manner. This includes distributed crawlers, use of anonymous proxies, simulated human actions and activities, randomized activities, etc.

Advanced Monitoring Capabilities

- The management and monitoring console enables the optimization of bandwidth usage by monitoring the efficiency of resource utilization, including bandwidth, crawler units, crawler tasks and more. In addition, it provides ongoing operational monitoring, as well as alerts on any malfunction or problem.

Deep and Dark Web Support

- The platform employs various strategies and mechanisms to reach data found in Deep Web and Dark Web layers, which is much larger in scale than the “standard” Web data. Deep Web includes dynamic pages that require domain knowledge, unlinked content that

is difficult to reach (for example, data secured by user-password login or access blocked by CAPTCHAS). Dark Website collection enables collecting data from the web layers that are inaccessible from regular Web browsers.

Visual Webflow Definition

- Designing web scraping projects is easy with the visual Webflow editor. Simply load the website in the built-in Web browser and click on the content you wish to extract. The Webflow editor contains tools that assist in developing the collection, breaking down the collection into sub-Webflows for reuse, and simplifying data extraction patterns. This is all possible using simple point-and-click operations.

Out-of-the-Box Support for Popular Social Network and Forum Platforms data extraction

- The solution includes a built-in package of maintained Webflows for the most used social networks, blogs, and discussion platforms.

2.6.1 Deep & Dark Web Collection Methods

The platform enables the customer to harvest and extract information hidden in the Deep and Dark webs.

2.6.1.1 Deep Web Access

In order to collect data from the Deep web (for example, data secured by user-password login, dynamic pages that require domain knowledge), the platform supports various collection strategies, among them:

- Pool of virtual agents and their respective geographical origins (such as IP addresses) that are used to access the content on behalf of the customer
- Browser-based and API-based crawling engines
- Automatic bypass of CAPTCHAs

All these collection strategies work while running automated engines to remain below the radar of bot detectors.

2.6.1.2 Dark Web Access

Verint's solution supports the collection of information hidden in the Dark Web.

In order to collect from the Dark Web, the system accesses the sites using TOR (refer to 2.6.2.5 for more details about TOR access) and utilizes multiple tools to attain access to such sites.

Verint proposes this functionally as an option.

2.6.2 Covert Collection of Web Data

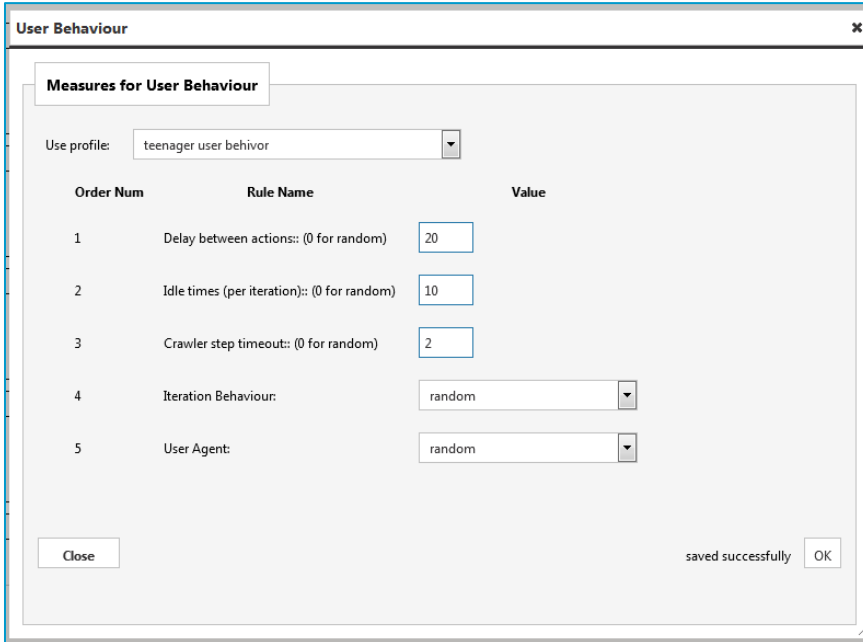
The platform provides a rich set of engines and strategies for extracting vast amounts of Web data without detection.

The Webflow (robot) defines the navigation and extraction of data. The platform then wraps the Webflow, using built-in tools with the required security, covertness, and stability to allow covert collection. This enables the user to focus on extracting the relevant content, requiring only minimal user involvement to maintain a covert collection process.

2.6.2.1 User Behavior Emulation

Unlike humans, automatic collection scrapers pass through all the links on route to the required information one by one, in order, with no delay. There are no “wasted” steps and no routine of steps in a loop. Humans, on the other hand, behave differently, and that difference can be utilized by website protection tools to identify and limit the automatic collection process.

The platform provides easy to define, user behavior emulation, which can be defined once and then reused by any Webflow for data collection.



User Behaviour

Measures for User Behaviour

Use profile: teenager user behavior

Order Num	Rule Name	Value
1	Delay between actions: (0 for random)	20
2	Idle times (per iteration): (0 for random)	10
3	Crawler step timeout: (0 for random)	2
4	Iteration Behaviour:	random
5	User Agent:	random

Close

saved successfully OK

Figure 3 – User Behavior Emulation

2.6.2.2 Browser Type Emulation

The user can define what browser type and browser version should be used by the system for each specific site (e.g., Firefox, Internet Explorer, or Chrome).

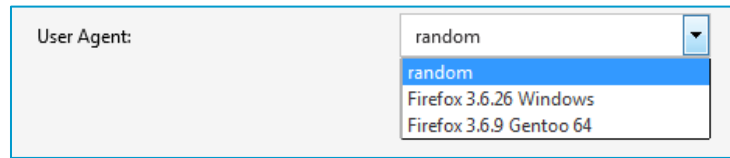


Figure 4 – Browser Behavior Emulation

2.6.2.3 Overcome Error Messages and CAPTCHA

While surfing the Web, many error messages and CAPTCHA challenges (scribble letters the user needs to identify) may be presented to the user. While a human user easily manages to overcome the Web server errors and CAPTCHAs, automatic collection machines tend to get stuck on those unexpected events.

The platform supplies an easy-to-define event handler to preconfigure the appropriate behavior to overcome error messages, buttons that no longer exist, CAPTCHAs, and other unexpected events. The event handler can be defined once and applied over multiple Webflows.

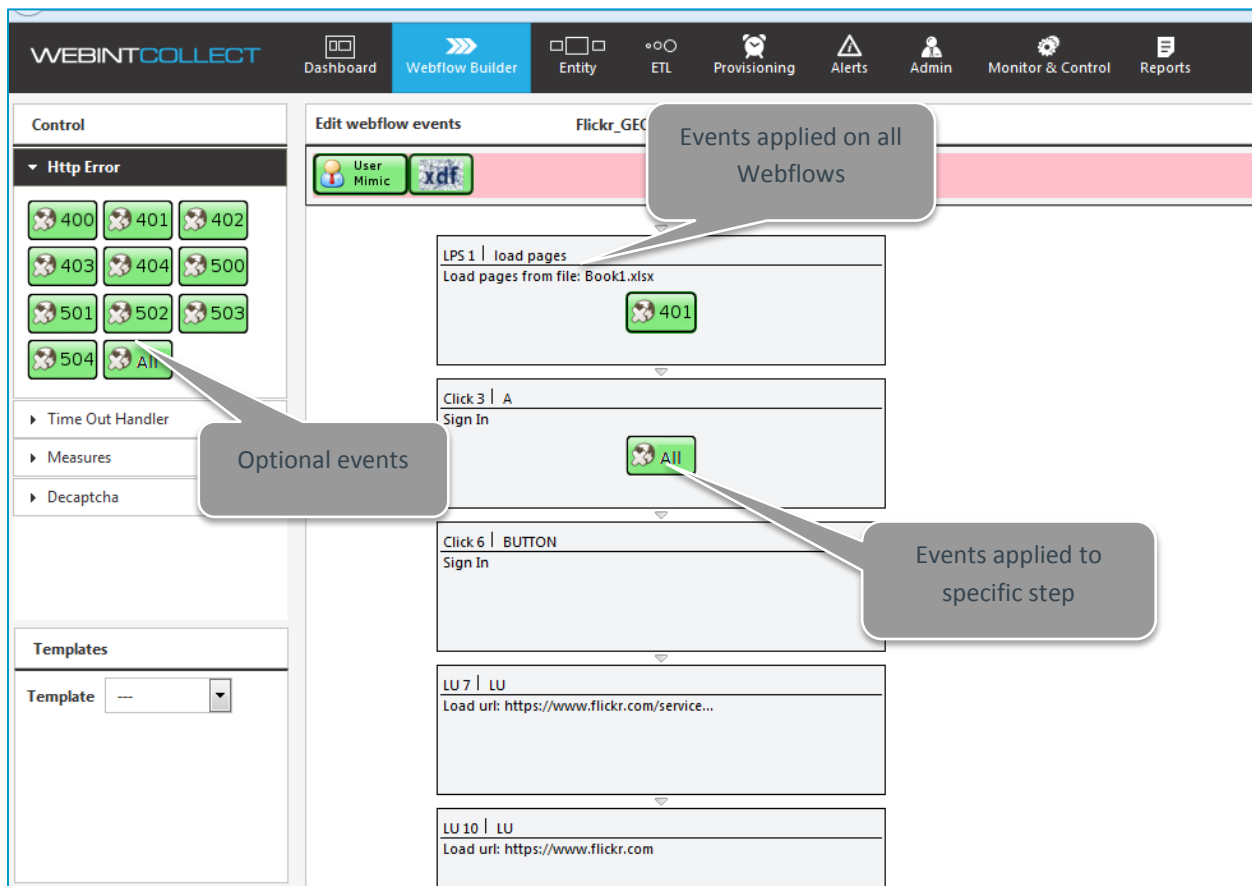


Figure 5 – Overcoming Error Messages and CAPTCHA

2.6.2.4 Meet Website Policy and Limitations

Users do not have to be concerned by limitations such as geographical location, number of parallel logins for the same account, or rate limitation flows.

The platform envelops the Webflow with constraints that allow the user to define the limitations to be applied on run-time; for example, select randomly available logins fit to that site, use each login no more than twice in parallel, and make sure that the website login is consistent in terms of geographic location.

2.6.2.5 Web Strategy

When defining a collection task using an existing Webflow, the user can define what web strategy to use to meet the specific needs of the collection task. That Webflow can be freely switched between web surfing strategies as needed.

- **Direct IP** is the default strategy that uses regular web surfing. This option is recommended for a regular data collection task, where there are no special limitations, as it is the fastest surfing method.
- **ProxiEra** is a built-in mechanism used to hide the customer IP address, for example, for the following reasons:
 1. **Virtual agent** – It's important to tie a virtual agent to a set of IP addresses, especially for use in social networks like Facebook. Social networks prevent access and alert when simultaneous logins are detected from either the same IP address or from different IP addresses. Therefore, the system needs to assign each virtual agent a preferred IP address and verify that the IP address looks genuine.
 2. **Access geo-location restricted websites** – Some websites are accessible only from specific geographical areas. To bypass this limitation, proxies installed in that area can be used.
 3. **Disguise customer IP address** – Prevent revealing customer origin and intentions.
 - **TOR** is a system that directs internet traffic through a worldwide volunteer network of servers. To enable anonymity while surfing, TOR hides the collection system and enables it to access websites available only through TOR (parts of the Dark web). To get the Webflow to work through TOR, the user needs only to define the network strategy.
 - **Streaming for Twitter.** Using Twitter's API, WebInt-COLLECT is capable of sending streaming requests as defined by the users in order to structure content in the same way as web flow collected data, but without the need to actually access the pages collected. This further improves the protection of your agency's identity and enables not only the collection of historic data, but also the monitoring of new Twitter content as it is published, when it is most needed.

2.6.2.6 Layered Architecture Summary

The WebInt platform envelops the collection task and provides it with the entire environment to run successfully. The Webflow, once created, can be applied with many different conditions to collect data without change. With minimal user involvement, from scheduling up to web strategy, the process is managed by the system to ensure continuous collection.

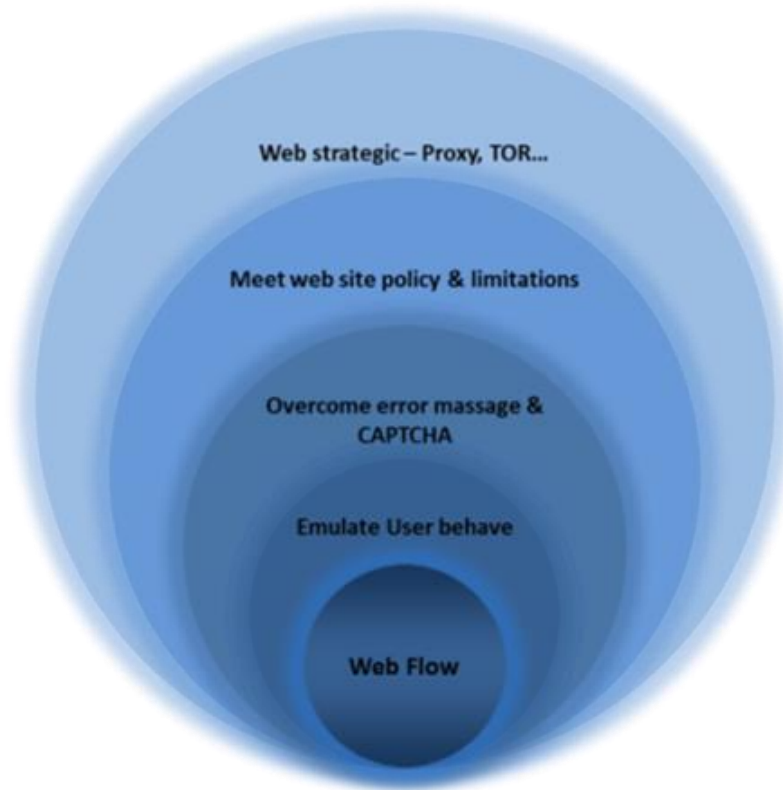


Figure 6 – Layered Platform

2.6.3 Scalable Architecture

The platform offers a highly scalable solution, capable of adapting to any changes in requirements, traffic loads, and types of engines, content coverage, storage, and more.

- **Scalable Collection Support by adding additional crawler units** – The platform automatically incorporates newly added crawlers units. Each crawler unit can run several concurrent collection tasks (e.g., crawler engines). Adding crawler units enables the support of additional collection resources.
- **Scalable proxy support by adding additional proxy machines** – The platform automatically incorporates newly added proxies to utilize additional IP addresses to access the data without being hit by site policies, to stay below bot radars, and to limit the exposure rate.
- **Scalable proxy support by adding additional virtual agents** – The platform automatically incorporates newly added virtual agents to consume more content in less time.
- **Scalable ETL process by adding additional servers** – To meet future needs for content analysis to highlight the changes and transform content into the customer data model, the system can scale out by incorporating additional index and ingestion servers.

2.6.4 Intuitive Graphical Designer for Webflow (Robot) Design

Webflows are set up using simple block diagrams. Users define the step-by-step actions required by the Webflow by defining each step as a block in a flow diagram. For each step, users can apply “human-like” behavior requests. If requested, the Webflow adopts human-like behavior to evade detection as a machine. Users can also apply blocks for the treatment of HTTP error codes (such as HTTP 404 error, page does not exist), thereby defining the required behavior for the Webflow, for example, when unexpected information is received from the server.

WebInt-COLLECT’s web browser client allows users to access the target site and teach the Webflow the required steps to collect the necessary information. The steps are organized in actions that are performed by the crawler in an automated fashion. Examples include clicking on a given part of the screen website, accessing content from a table, filling out a form, submitting it and extracting the results, and interacting with the page by hovering in one place.

Webflow setup can be browser-based or browser-less, depending on the site structure and whether it is static or not.

All steps are easily set up in a graphic flow diagram, where each step is presented by a block in the flow and defined within the site by selecting and defining the necessary sections on the site page.

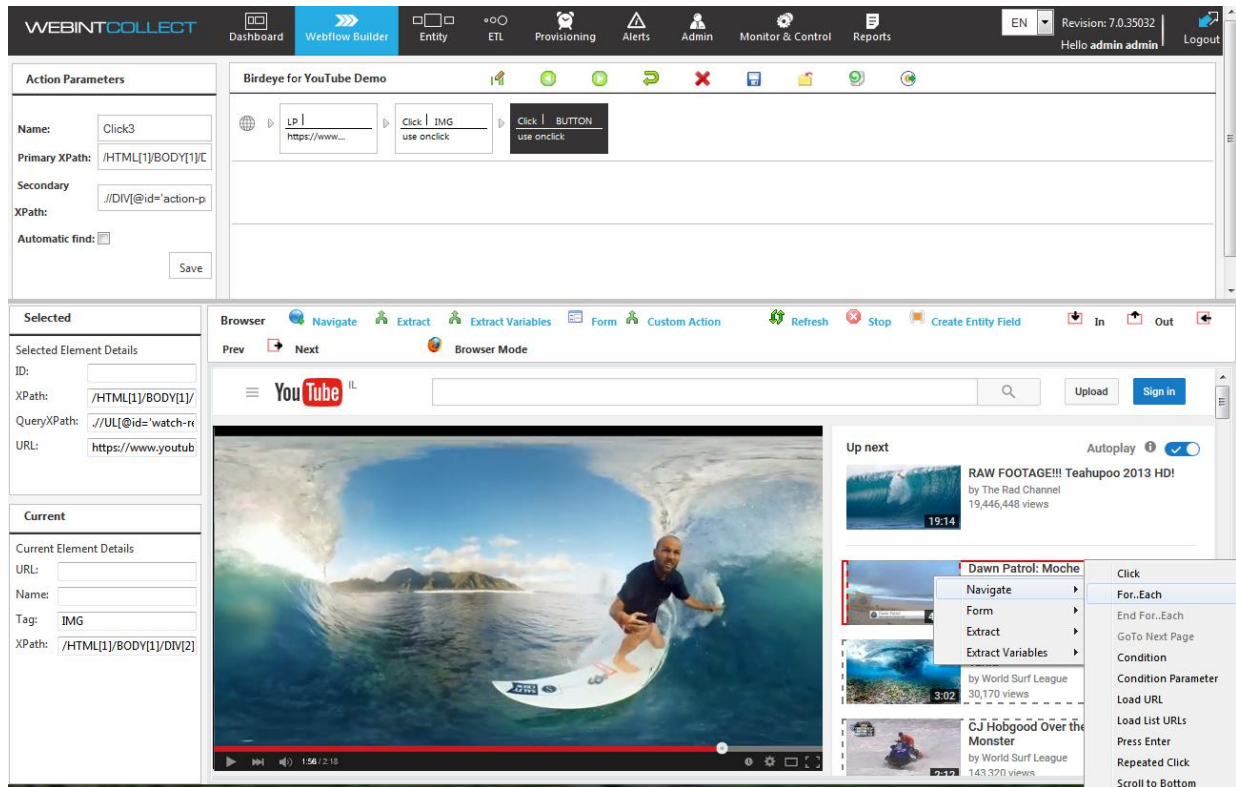


Figure 7 – Webflow design page

2.6.5 Continuous & Robust Collection

Unattended, continuous & robust 24x7 collection poses many challenges, websites can be unavailable, proxies can stop working, virtual agents can be suspended, CAPTCHAs can be raised, power, network and hardware failures can occur and more. To enable a continuous and robust collection process, the Verint command and control collection platform automatically detects the incidents, overcomes them, and provides a centralized monitoring view, with alerts and reporting capabilities.

2.6.5.1 Collection task management

There are many strategies to be applied when collecting web content, including, but not limited to, metrics to:

- **Faster collection times** by distribute and hence parallel sub collection tasks between the different crawler units and crawler tasks.
- **Overcome website policies** by accessing different sections using different collection tasks and identities.

The platform has a sophisticated job and tasks executer that manages all of these tasks and ensures that collection is performed in an optimal way while staying below the radar of the targeted website.

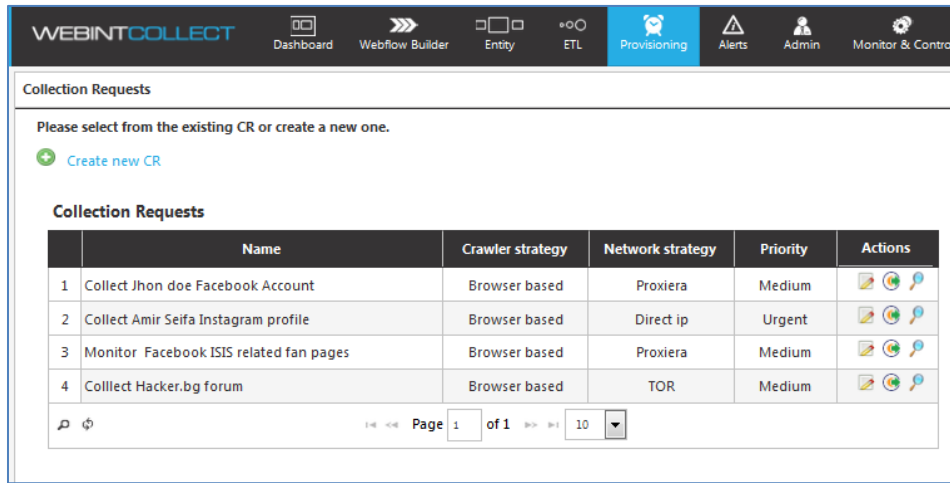


Figure 8 – Collection Manager

2.6.5.2 Virtual Agent (Avatar) Management

In order to access restricted web content (e.g., websites that require login), the system maintains a managed virtual agent pool. The virtual pool maintains the virtual agent’s identifiers: user name, password, and IP address for use with the virtual agent.

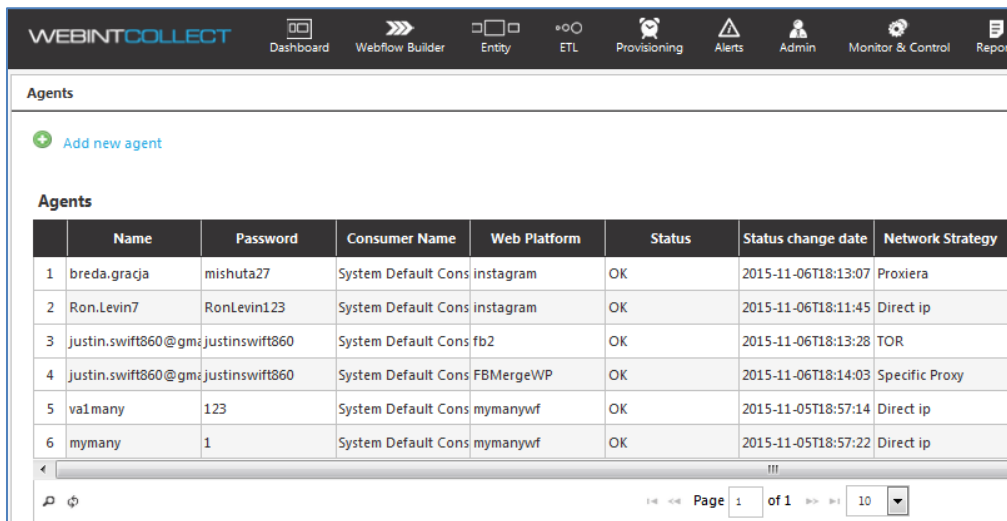


Figure 9 – Virtual Agent Management

2.6.5.3 Proxy Management

The Proxy Management mechanism enables management of the proxy pool, checks each proxy validation, and verifies that they are used in an optimal way, adhering to security measures to stay below the radar of websites and anti-bot tools.

	Host and Port	Insert Date	Last Used	Last Accessed	Status	Country
1	50.23.3.1:9090	09.11.2015 15:29:44	09.11.2015 15:29:44	09.11.2015 15:29:44	ACTIVE	United States
2	2.32.0.0:80	09.11.2015 15:32:32	09.11.2015 15:32:32	09.11.2015 15:32:32	ACTIVE	Italy
3	27.50.16.0:8080	09.11.2015 15:32:59	09.11.2015 15:32:59	09.11.2015 15:32:59	ACTIVE	Indonesia
4	1.0.32.0:1222	09.11.2015 15:31:25	09.11.2015 15:31:25	09.11.2015 15:31:25	ACTIVE	China
5	72.38.42.2:8080	09.11.2015 15:29:29	09.11.2015 15:29:29	09.11.2015 15:29:29	ACTIVE	Canada
6	50.23.3.2:1234	09.11.2015 15:29:57	09.11.2015 15:29:57	09.11.2015 15:29:57	ACTIVE	China

Figure 10 – Proxy Management

2.6.5.4 Pooling System Resources to Support Enhanced Collection Strategies

Combining the various collection resources enables support for several collection strategies. For example, the following strategy enables optimal utilization of system resources when targeting a specific profile collection.

This strategy reduces the risk of exposure and reduces the collection time. Used in parallel on multiple virtual agents and multiple different IP address, this strategy enables spreading the work between the different virtual agents (e.g., one virtual agent originated from a specific IP address collects some of the target profile posts, while another virtual agent originated from a different IP address collects some of the albums). Such a strategy reduces the blockage rate and introduces a more robust collection process.

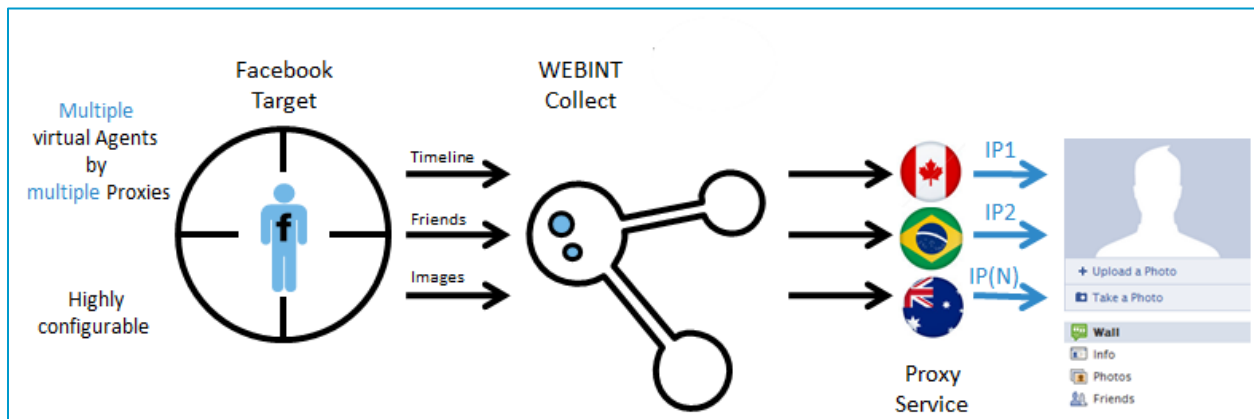


Figure 11 – Combined Collection Flow

2.6.6 Command & Control Monitoring Capabilities

The platform offers centralized command and control capabilities that enable issuance of provisioning requests, system monitoring, and the export of collected data

2.6.6.1 Collection Management Monitoring

The platform supports a monitoring dashboard that enables users to view the existing Webflows, set schedules for running, view historical runs and running errors, and monitor the outcome of the collected data. The dashboard provides a graphic display of the operational status of all the system's Webflows and servers, allowing quick monitoring and troubleshooting to ensure system functionality around the clock, and to prevent unnecessary breakdowns.

2.6.6.2 Easy Dashboard Setup

A preset selection of options provides the monitoring options required for the system. In addition, a graph selection pane allows users to drag and drop new graphs or monitored controls onto the dashboard to meet any ad hoc monitoring needs.

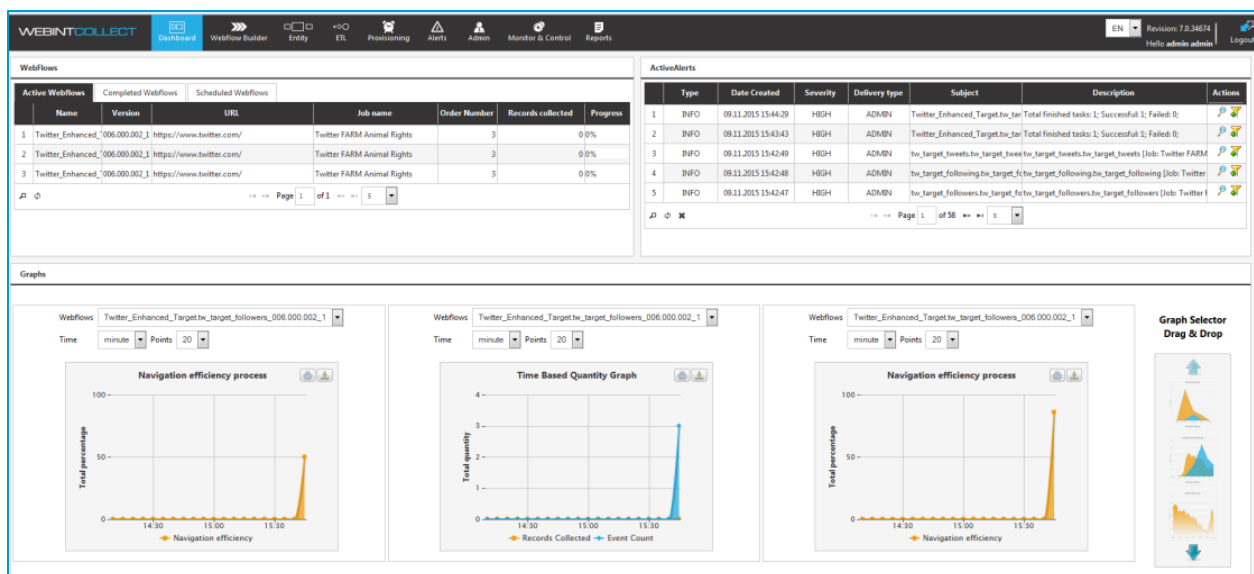


Figure 12 – Dashboard Monitoring

2.6.6.2.1 Crawler Monitors

The crawler monitors indicate which crawlers are overloaded or have malfunctioned. A built-in mechanism performs validity checks on the site, checking to what extent the site responds to the crawl, to ensure that the crawler adjusts its activity and to avoid overloading the site. Depending on the scenario, the system might be able to adjust automatically; otherwise an administrator must make the adjustment.

2.6.6.2.2 Collection Reports

Collection reports display the information over the Webflow history – how many times the crawler ran, what problems were detected during operation, what was collected, and so on. The report also displays Webflow performance characteristics and proxy performance, to learn about bandwidth consumption, blockages, etc.

2.6.7 Web Data Extraction Methods

2.6.7.1 Scenario-based Web Data Extraction (Structured Data Web Extraction)

Scenario-based, web data extraction is used to collect the web data and store it in a structured form. For example, to extract a Facebook profile including related friends, related activities and more. Using scenario-based collection, the user can determine the necessary navigation actions, which data to extract and how to model it.

The operator can set up a “Webflow” (e.g., robot) to achieve this capability.

The data collection and extraction process is based on the following concepts:

- **Define Webflow (Robot) template per site to access the site’s data.** Steps are defined in order to search for subjects of interest, navigation, and extraction of data from the website, based on specific locations within the site page. The steps are organized in action sequences that are performed by the crawler running the Webflow. Examples for such actions include: clicking on a given part of the site, accessing content from a table, filling out a form, or interacting with the page by hovering in one place. The user can decide whether to scrape the content from the targeted HTML page, use the website API, or even use a hybrid approach (API & scraping) to achieve the best results.
- **Test and schedule the Webflow.** After defining and saving the Webflow, the user can test the Webflow behavior on different input parameters. After the test phase, the Webflow can be published and used to define schedules and seeds with parameters to be collected. Any problem arising from the running Webflow is identified and corrected at once, to enable smooth running of the Webflow and efficient data collection.
- **Monitor and Control.** The platform provides a centralized control and monitoring tool for monitoring crawler activities and general system functionality. A graphic dashboard display of operational levels and health monitoring mechanisms ensures smooth performance, and alerts users on any forthcoming problem. Crawler monitors indicate crawler activities, ensuring no crawler is blocked or overloaded.

2.6.7.2 Scenario-less Web Data Collection (Unstructured Collection)

In addition to the structured (scenario-based) collection, the system supports collecting unstructured web data. The operator can issue unstructured collection requests to news sites, blogs, and other public websites –

without the need for a predefined Webflow for those websites. By inserting URL ranges, the system crawlers approach said web pages and collects data and directly linked pages in an optimal structured manner while trying to identify the main content of the page, author name, publish date, and more.

2.6.8 Data Collection Engines

The platform includes various data collection engines to ensure effective web data extraction suited to virtually any type of website. The collection engines can work in hybrid mode to maximize the access and coverage of data while utilizing the platform resources. This capability enables, for example, collecting part of data that is accessible via Web API using the API engine and the rest of the data, which is not accessible in that mode, using the browser-based engines.

2.6.8.1 Static Web Page Engines

Static Web page engines are designed to collect static HTML-based sites, where collection can usually be executed via a simple HTTP client request. This type of engine usually fits traditional news sites, blogs, and other Web 1.0 websites (i.e., sites that do not use AJAX or related Web 2.0 technologies).

2.6.8.2 RSS-based Collection Engines

Many websites publish site content using RSS channels. For example, Facebook offers RSS support for all fan pages, on CNN.com all article content is available via RSS, and Google Alerts offers their service using RSS.

The platform offers advanced RSS collection engines that can transform streams of RSS links into structured web data that fit the data models.

2.6.8.3 Browser-based Engines

Modern websites, including most social networks and e-commerce sites, use AJAX and other related technology (commonly referred to as Web 2.0 technology). This technology enables data rendition on-the-fly and provides enhanced user experiences. Even news sites and blogs that embed integration with social network comments fall into this categorization. Static web page engines do not work in those cases. The only way to access this content is via browser-based engines – engines that run a browser or browser engines, which enable consumption of this content.

2.6.8.4 Website API-based Engines

APIs usually exist on big sites, and allow collecting a large amount of data quickly, with low web traffic and low maintenance. Web API is usually executed after authentication by sending an HTTP request to the Website asking for data, and getting a response in JSON or XML format with the requested data from the Website. Working with the website's API is more stable, as modifications in the Website GUI do not affect the collection process, and transformed data is clean without graphics or formatting. As a result, this data is less prone to change and is collected much faster than other types of data.

The end user can use scripting language to extract content from websites that support this method.

2.6.8.5 API Stream-based Engines

Another method of collection that is relevant to Twitter only is Twitter's Streaming API, which pushes data as it happens in near real-time. With Twitter's Streaming API, the analyst can define a list of tracked keywords, twitter profiles, and geo-location areas to be monitored. The data is then streamed to WebInt-INVESTIGATE providing near time collection and analysis.

WebInt-COLLECT supports Twitter streaming as part of the GA web flows, the basic supported web flows that are part of the system and are periodically updated by Verint. Additional streaming APIs such as Instagram and others can be purchased from Verint professional services.

2.6.9 Built-in Webflows for Collecting Data from the Major Websites

The WebInt-COLLECT solution is delivered with the following built-in, generic collection Webflows:

- Facebook – Profile, Search, Page, Event, Group and Reconstruct
- Twitter – Profile, Search and GEO
- YouTube – Channel or Search
- LinkedIn – Target and Search
- Google search – brings the main content from each result
- Instagram – Profile, Search and GEO
- Flickr – Profile, Search and GEO
- Pinterest - Target, Search
- PasteBin - Search
- Dark web search engines
- Tumbler - Target

Additional Webflows (Robots) can be created by the system administrators using the platform or provided by Verint at additional cost.

2.6.10 WebInt-Collect Main Components

- **Distributed Crawler Units** – The Crawler Units are the components that actually access the web and collect the data. One collection solution can include one or more Crawler Units based on the amount of collection requests and the expected amount of data. Each collection unit requests tasks from the Collection Manager. Once the task is received, each Collection Unit works independently, collecting data, normalizing it, running an antivirus check and passing it back to the central storage. Adding Crawler Units to an existing working solution is simple and does not require any system downtime. A Crawler Unit can access the web using four different methods: direct crawling, proxies, dedicated proxies, and TOR.
- **TOR Router** – If a collection request is defined to use TOR to access the target website, the Crawler Unit uses a TOR connection from its TOR connection pool. During TOR crawling, the TOR manager monitors the traffic and reconnects with a new identity when needed.
- **WebInt-Collect Web Application** – The Web Application is the access point for the collection administrator, the Webflow builder operator, and the end user who provision the system using an intuitive user interface. The Administrator can set configuration, monitor running and queued collection requests, change priority, stop collection request, monitor crawler units, etc. The Webflow builder (operator) can use it to build Webflows, test them and publish them for the use of the end users. The web application also supports an API Layer for collection provisioning and monitoring.
- **Proxies' farm** – The customer can set and install dedicated proxies' farm on a hosting cloud service provider such as Amazon elastic cloud. These proxies allow the system to easily collect information from various IP addresses originated from different countries.
- **Collection Manager Server** – The Collection Manager orchestrates data collection, assigns virtual agents and proxies to collection tasks, manages queues and load balancing the collection, and handles failures (for example, if task fails due to virtual agent blockage, the collection manager can select a different virtual agent and resend that task with the new virtual agent).
- **Virtual Agent (Avatar) Manager** – The built-in virtual agent (avatar) management component supports the collection manager when retrieving content from restricted websites. The mechanism manages (plan, coordinate and synchronize) the army of virtual agents in an optimal way and enables WebInt-Collect to extract vast amounts of restricted targeted profiles, while supporting continuous (24x7) robust and covert (stay behind the radar of anti-bot detector tools) collection processes.
- **Proxy Management** – A built-in mechanism used to hide the customer IP address. This service is necessary for the following reasons:
 - **Virtual agent** – It's important to tie a virtual agent to a set of IP addresses, especially for use in social networks like Facebook. Social networks prevent access and alert when simultaneous logins are detected from either the same IP address or from different IP addresses. Therefore, the system needs to assign each virtual agent a preferred IP address and verify that the IP address looks genuine.

- **Access geo-location restricted websites** – Some websites are accessible only from specific geographical areas. To bypass this limitation, proxies installed in that area can be used.
- **Disguise customer IP address** – Prevent revealing customer origin and intentions.
- **Administration DB** – The Administration DB holds the Webflow definition, virtual agents, collection requests configuration, and all additional information required for the continuous collection system.

2.7 WebInt-INVESTIGATE

WebInt-INVESTIGATE analyzes vast amounts of diverse, open-source content to enable rapid identification and tracking of events, targets, threats, and related activity. Topic (top-down) and target (bottom-up) investigation mechanisms are combined in one integrated solution.



Figure 11 – WebInt-INVESTIGATE

Key benefits of WebInt-INVESTIGATE include:

- **Connecting the dots** – Advanced analytics capabilities, including social, statistical, and visual link analysis.
- **High Quality, Relevant Data** – Focus on monitoring and analyzing the content you are looking for, without spending time on irrelevant data.

- **Revealing the unknown** – Automated recommendation engine informs you of web accounts that have high probability of belonging to the same person related to your investigation, helping you achieve more comprehensive coverage in your investigation.
- **Restricted Profile Reconstruction** – Using advanced algorithms; WebInt-INVESTIGATE can build up a social profile picture of a user that chooses to limit the access to his account (using potential leads). Currently, WebInt-INVESTIGATE supports the reconstruction of Facebook profiles. Restricted Profile Reconstruction capability can be extended to support profiles from other social networks upon customer request.
- **Investigation methodology** – Verint’s experience and expertise in the intelligence solutions field assures that the system is built on field-proven, sophisticated, and logical investigation methodology, which is integrated in the system’s workflow.
- **Topic investigation** – Emerging events analysis, and general tracking of developments issues allow law enforcement organizations to track general and specific group activities. Keeping track of emerging events helps reduce surprise factors, and can help maintain public safety.
- **Target investigation** – Target characterization provides immense background information, automated alerts reveal investigation leads, and interactive links allow investigation drill-down. A target unification approach unifies the accounts of similar entities together, by actively proposing a relation between them, and possibly indicating the different accounts/names of the same person.
- **Be Forewarned by Alerts** – Alerts and early warnings can be generated based on customizable triggers and adjustable thresholds. Trigger scenarios can be based on levels of activity, keyword combinations, etc. The definition of specific authors, sources, and levels of activity per keyword provides timely alerts on suspect behaviors and more.
- **Manage and Control Collection** – This solution schedules the tasks, manages resources and logins to sites and follow-up on the collection until receiving the output data.

2.7.1 Analysis and Research

Verint WebInt-INVESTIGATE is specially designed to facilitate the intelligence investigators' workflow. It provides users with an extensive suite of analytical tools to visualize and analyze information from multiple angles. These include a combination of quick and easy tools for general questions, dedicated tools to drill down into investigations of relational, geospatial, statistical, and behavioral links and associations, timeline-based research, and report and summary tools to disseminate information to colleagues and other departments.

This rich combination of purpose-built tools helps users navigate the investigation. Once they find a clue or lead, users can choose from a multitude of steps using different physical, deductive, and conceptual links between types of views. This facilitates a "dialogue" between the user and the data, allowing them to simulate different investigatory options by trial-and-error, the very essence of their daily work.

2.7.1.1 Data Search & Discovery

Verint WebInt-INVESTIGATE enables search on all textual content in the system, including raw source content and metadata, entities' content, and vetted content such as analyst insights and summaries. Textual indexing based on Unicode allows it to support simple textual searches for all character sets, and therefore all languages.

Simple, advanced, and structured search modes offer users a series of options to combine different search criteria and filtering options across all data, ensuring that all relevant entities, patterns, or links are identified as quickly as possible.

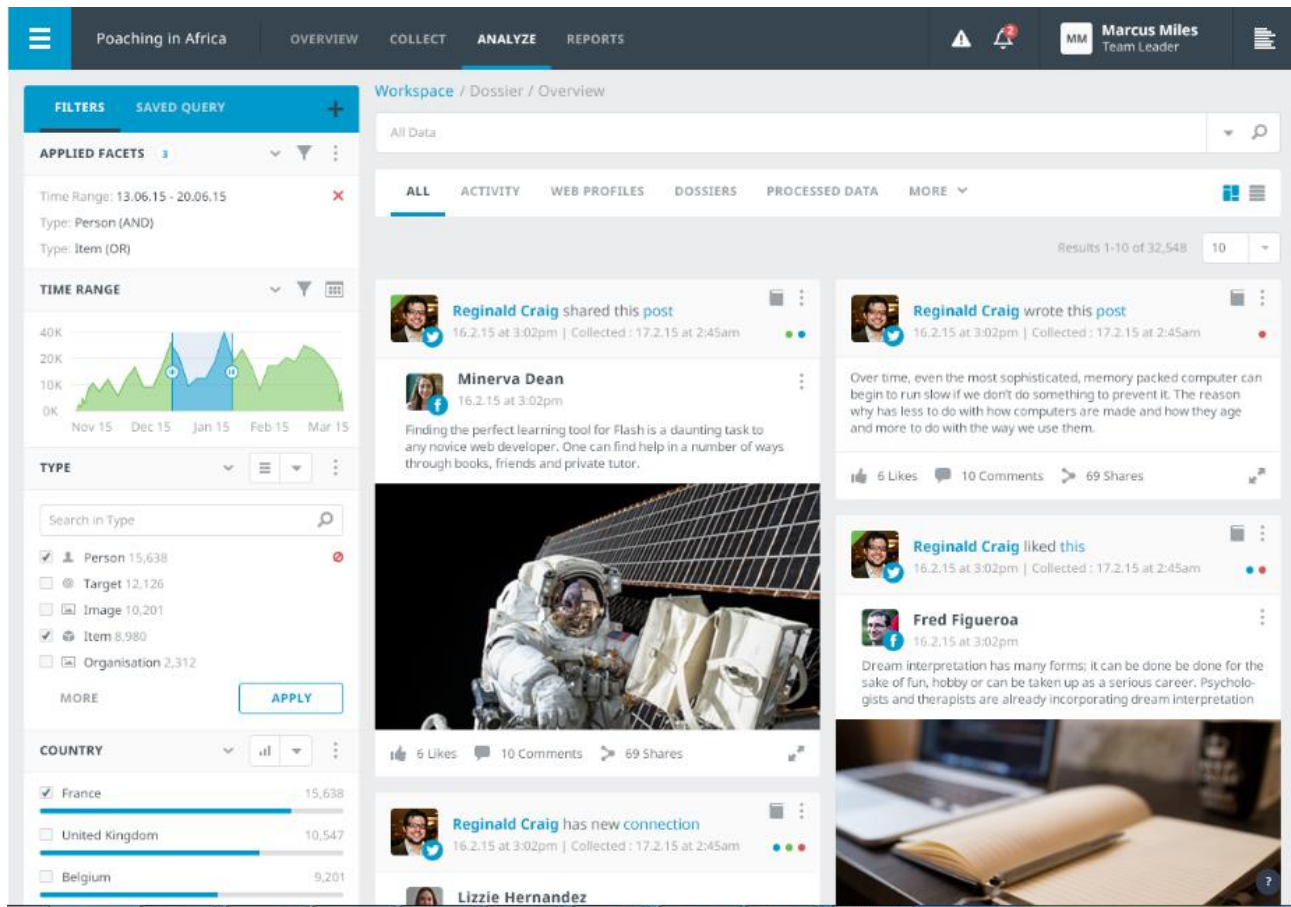


Figure 13 – WebInt-INVESTIGATE Discovery

2.7.1.1.1 Simple and Advanced Textual Searches

Verint WebInt provides simple and advanced search capabilities, considers all criteria, and supports Boolean search options (multiple selections, And/Or/Exclude operators), wildcards, fuzzy searches, and semantic search – all accessed through a simple search entry user interface.

2.7.1.1.2 Facet-based Discovery

Faceted navigation allows the user to refine and navigate the data collection using a set of discrete attributes such as time, activities relationships types, and websites.

Faceted navigation serves as a custom map that provides the analyst with insights into the content and its organization, and offers a variety of useful possible next steps to narrow the results to find the needle in the haystack, and understand the collected results as a whole by extracting entities from the textual content of the results, showing summarized information and charts.

WebInt-INVESTIGATE Facets include advanced content-sensitive filtering mechanisms, enabling analysts to quickly search through big data amassed in the system. Using WebInt-INVESTIGATE Facets, content is

automatically dissected and grouped according to values repeated in the data. For example, if multiple documents contain information about countries, a ‘Country’ facet is automatically created and the list of countries identified in the documents will be extracted and displayed along with the number of occurrences. Facets also allow analysts to filter search results in lists created by the system.

2.7.1.1.3 Geospatial Searches

Users generate search criteria according to all available entity criteria, and filter results according to geographic area parameters. Each search can be run either with or without the geographic filter.

2.7.1.2 Visual Link Analysis

Verint WebInt-INVESTIGATE incorporates powerful Visual Link Analysis (VLA) capabilities, which provide a visual display of an entity’s network of relations and associations.

The VLA visualizes the entity’s relationships and links, frequency, and types of association. It also indicates derived relations, such as which criminal groups they are associated with, and so on.

Relations may consist of human relationships, participation in events, communication links, derived connections and more. Investigators can also identify connections between seemingly independent entities, for example, two people may have a common contact that mediates between them.

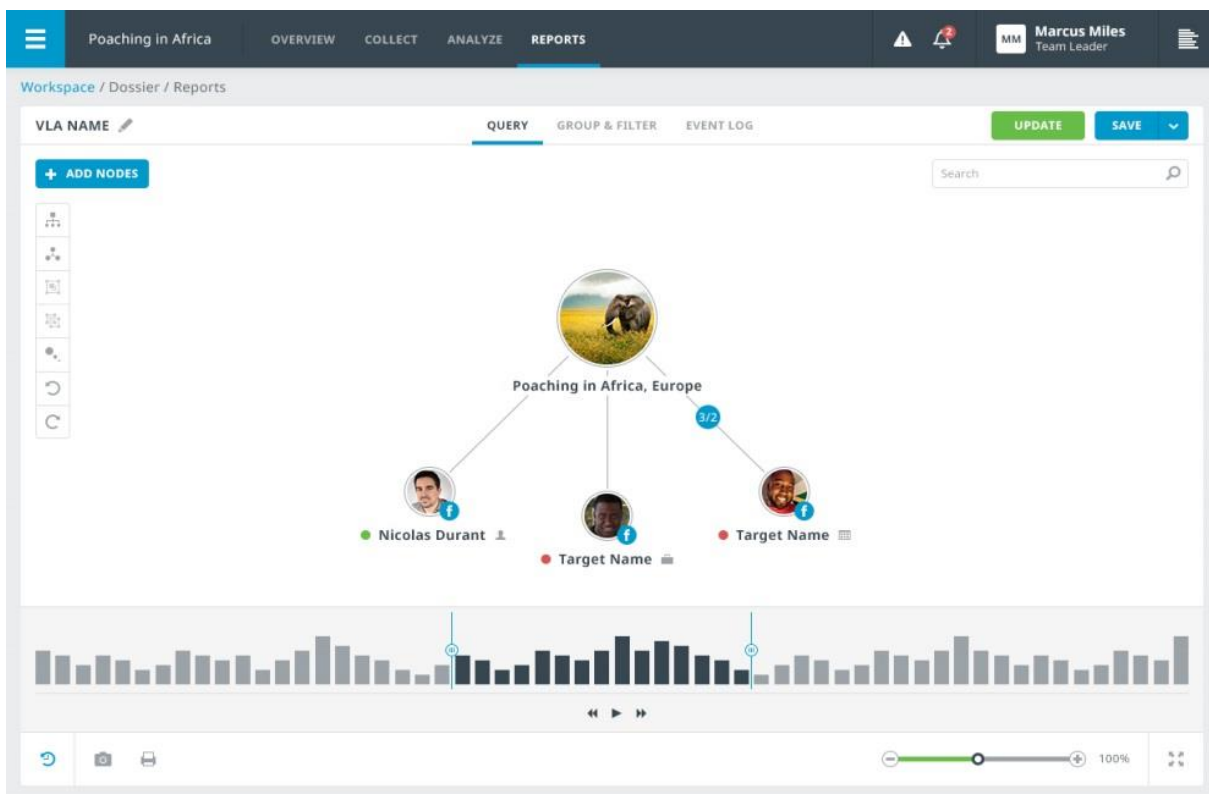


Figure 14 – WebInt-INVESTIGATE Link Analysis Display

2.7.1.3 Geospatial Analysis

Verint WebInt-INVESTIGATE includes GIS capability so that all geo-tagged entities are represented on the map, and manipulations to data (such as filtering) are synchronized in real-time with the active map display.

Geospatial information may be derived from a variety of sources: police log data, telephony and messaging metadata, social media interactions such as Facebook check-in, external GIS-GPS systems etc.

All location information is merged into a uniform geographic system by geocoding. The same geocoding process is applied when users search the system, so they can search for a street address or postal code and the search process automatically translates these into searchable coordinates.

Verint WebInt-INVESTIGATE geographical maps include a world-wide map that allows users to view and investigate location data within the investigation context.

Verint WebInt- INVESTIGATE offers various geospatial analysis tools. Geographical display enables investigators to view events, activities and data on the map, related information, such as type and time of event, is displayed to give users a complete intelligence picture. Geospatial display depicts the routes and routines of suspect entities to reveal location links between suspects or links to crimes or events that have taken place.

2.7.1.4 Social Analysis

Verint WebInt-INVESTIGATE enables the analysis of a group of web accounts as a single group, to find common elements and identifiers in order to understand the internal connection between the virtual group members. This is very useful when trying to understand a group of accounts, as well as for acquiring data regarding blocked profiles.

2.7.1.5 Text Analysis

Verint WebInt-INVESTIGATE enables the analysis of textual data including but not limited to:

- **Language Identification** – Examines all text data and determines the language of the text.
- **Named Entity Recognition** – Every text that enters the system is scanned to identify entities such as person, organization, location, phone, number credit card, number, date, vehicle, URL, facility, GPE, time, email, personal ID, number latitude/longitude, money, percentage, UTM, distance, religion, and nationality.

2.7.1.6 Entity Resolution Analysis

The matching and fusion of content belonging to the same entity is a critical step in the creation of logical entities, so that all the information about a specific person or organization is concentrated in one unified entity.

This is achieved using structured content to automatically match fields of content from different sources and by applying algorithms that identify and act on the similarities.

In most cases when dealing with unstructured content, manual intervention is required for accurate entity resolution, in which case users match the entities found in the entity extraction phase to existing or newly defined entities in the system.

2.7.2 Managing the Investigation Process

2.7.2.1 Investigation Management

The case framework is where investigations begin and where analysts are expected to provide the answers, using the power and functionality of the WebInt-INVESTIGATE. As such it is where analysts use all the resources and tools made available to them to gain the intelligence leads they need and fulfill their tasks.

Investigations in WebInt-INVESTIGATE are managed as a multi-resource work environment, with its own internal world of personnel (assigned analysts, data managers, etc.), access permissions, raw and vetted content, and analysts' insights. The system has been set up to support the investigative and knowledge needs of each case as a discrete 'universe' without compromising the security and intelligence needs of other cases.

Investigation progress reports allow senior analysts and/or administrators to track the progress and status of ongoing investigations.

The screenshot displays the WebInt-INVESTIGATE interface. At the top, there is a navigation bar with the 'WEBINT' logo, a search bar, and a user profile for 'Marcus Miles, Team Leader'. The main dashboard is divided into several sections:

- INVESTIGATIONS (12):** A list of active investigations. The top three items are:
 - ISIS in Europe:** By Marcus Miles | 26 Jul 2015 | Tomorrow, 12:00. Description: Counterterrorism officials said Saturday that the Islamic State is...
 - Poaching in Africa:** By Marcus Miles | 26 Jul 2015 | Today, 12:00 Past Due. Description: At current poaching rates, elephants, rhinos and other African wildlife may...
 - Ku Klux Klan on the rise:** By Marcus Miles | 26 Jul 2015 | Tomorrow, 12:00. Description: The Ku Klux Klan, with its long history of violence, is the most infamous...
- CALENDAR:** A weekly calendar view for June 2016. It shows four recurring events: 'Demonstration against Islam' on Thursdays from 09:30PM to 12:00PM.
- ACTIVITIES (8):** A log of user actions. Recent activities include:
 - Marcus Miles accessed 'Three heavily armed Britons arrested in Greece' (13h).
 - Marcus Miles logged out (13h).
 - Marcus Miles accessed 'Three heavily armed Britons arrested in Greece' (13h).
 - Marcus Miles logged out (13h).
 - Marcus Miles accessed 'Three heavily armed Britons arrested in Greece' (13h).
- INBOX (7):** A list of tasks and notifications. Recent items include:
 - 'Find Connection' (Completed) - Three heavily armed Britons... Workflow: Terrorist Event.
 - 'Find Suspect' (13h) - Three heavily armed Britons... Workflow: Terrorist Event.
 - 'Marcus Miles shared a document' (13h) - Three heavily armed Britons... (Open button).
 - 'Find Connection' (Completed) - Three heavily armed Britons...

Figure 15 – WebInt-INVESTIGATE Dashboard

2.7.2.2 Investigation Overview Dashboard

Verint WebInt-INVESTIGATE presents the investigator with a dashboard that displays case highlights focusing attention on recent activities of suspects, news updates, content highlights, recent searches, results of interest, alerts noted, and any recent inputs, analyst summaries, or leads provided.

As an investigator starts a new shift they can quickly identify recently added inputs, alerts of interest, insights made by colleagues, or awaited breakthroughs. The dashboard displays multiple widgets for presenting these summaries.

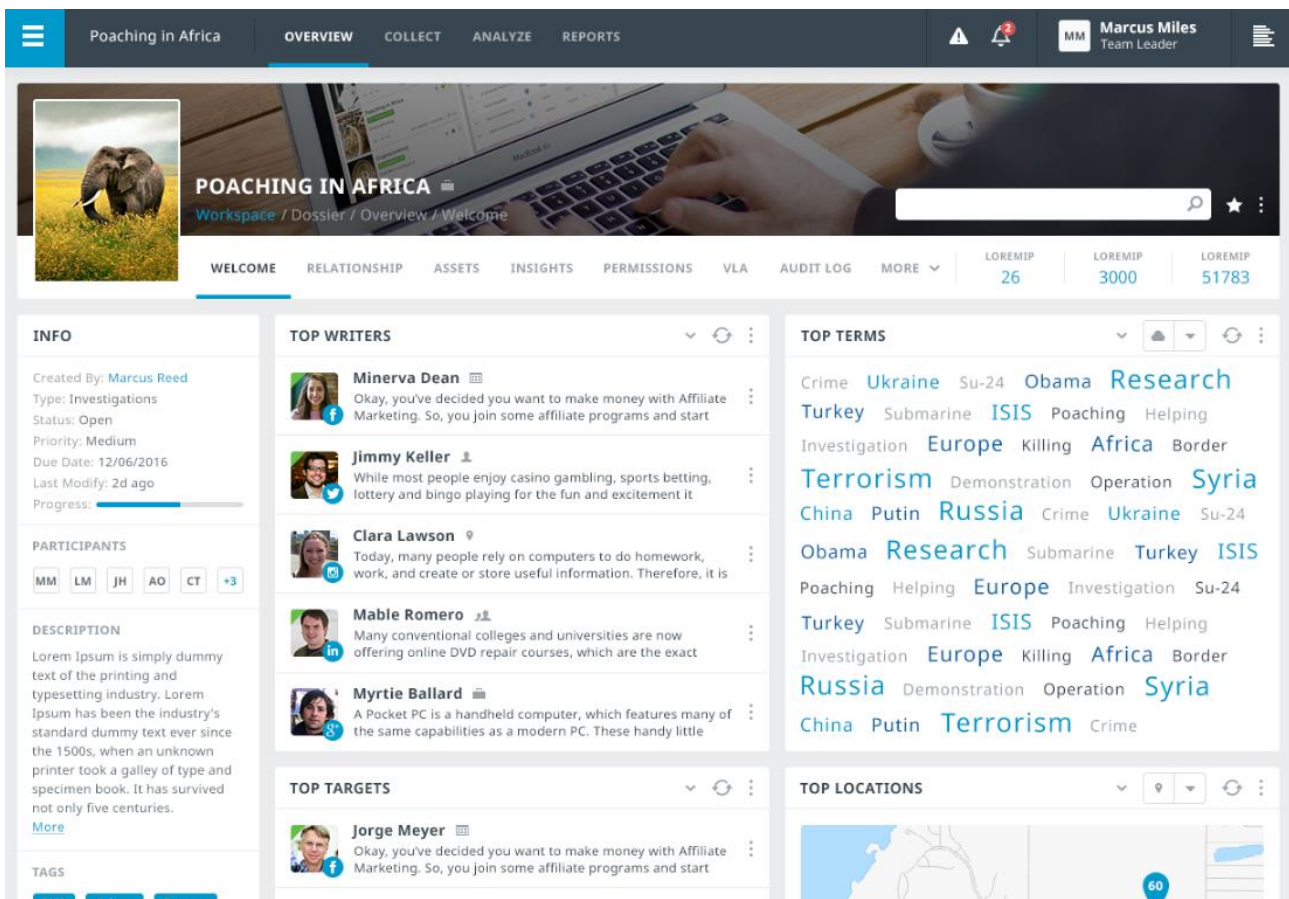


Figure 16 – WebInt-INVESTIGATE Investigation Dashboard

2.7.2.3 Target View

After defining a Target as an entity within the system, all automatically generated links and enrichment information are managed under that entity and are available for review.

The Target Information tab provides all the extracted and stored details about the Target, along with links to all raw data displayed in this tab. It also provides a statistics analysis of the target's web activities, including a list of usernames, social alerts, recent activities, main interests, and a graphic breakdown of his web activities and usernames.

Target cards include a set of aggregative views that create a complete picture of the person with focus on:

- **An indicative summary** about the person, directing the investigator's attention to the most relevant highlights, related investigation cases, and relations with other criminals.
- **Timeline display of actions, activities, locations** with enriched data about contacts and relations.
- **Related entities and links** are displayed using the VLA analysis tool.
- **Additional information** fused from the different databases the system integrates with, such as criminal records history and vehicles/weapons/real estate owned.

Using WebInt-INVESTIGATE, the analyst can consolidate web accounts that belong to the same target (person, organization, etc.) to get a comprehensive picture of that target's online presence.

There are two analytical options for unifying web accounts to targets: manually selecting the web accounts to be unified or using our proprietary recommendation engine.

By transferring the focus of the investigation from the identifiers to the entity, the analyst gains greater clarity and simplifies his investigation. Although this process is seemingly simple in the above example, relating multiple identifiers to their entities when investigating hundreds of identifiers may prove to be virtually impossible without advanced automatic tools.

2.7.2.4 Summary Reports

WebInt-INVESTIGATE provides template-based summary reports, enabling analysts to extract a comprehensive and aggregated overview of the investigation contents. The generated report includes a visualized output of the investigation, together with related content, summaries and insights. The report can then be disseminated to relevant departments or decision makers in a standard readable format.

Investigation reports are easily generated based on predefined templates that cover all the different aspects of the investigation. These reports can be configured or personalized as needed.

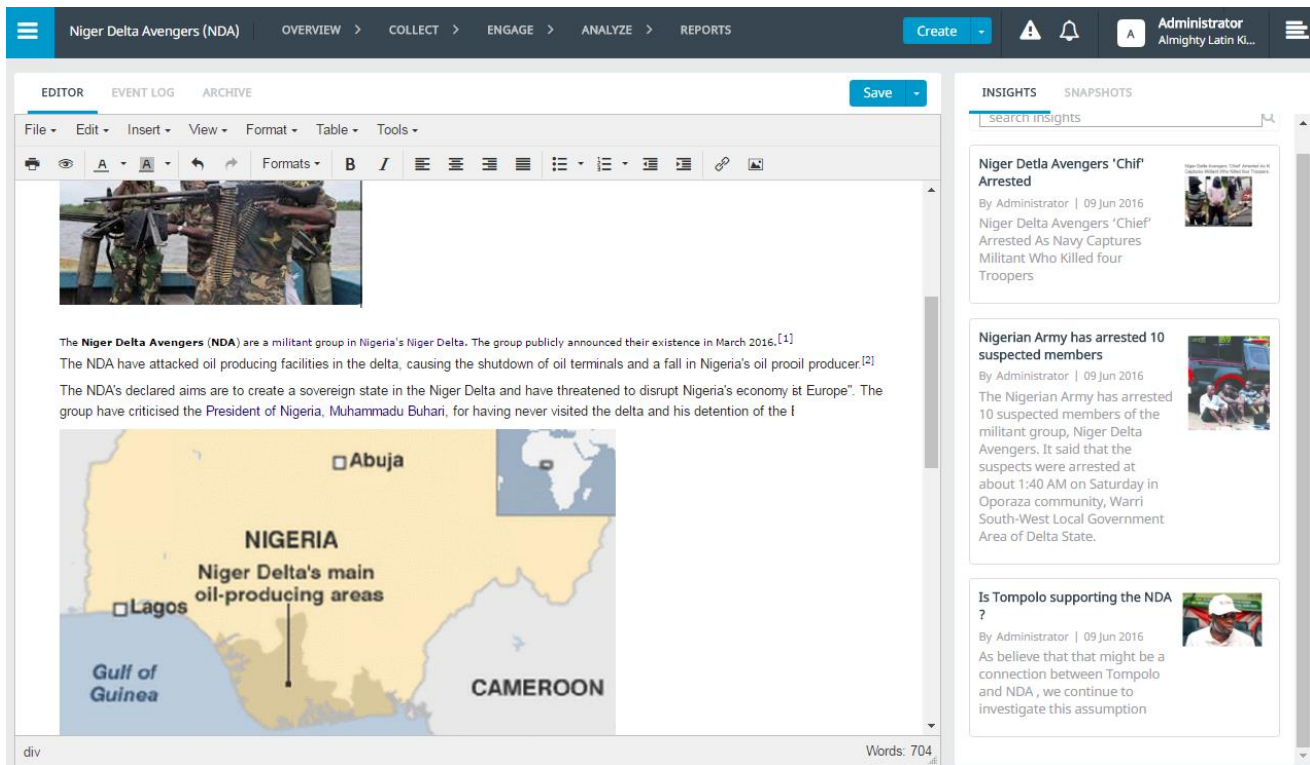


Figure 17 – WebInt-INVESTIGATE Report Dashboard

2.7.2.5 Search-Based Alerts

Users can prioritize specific searches and receive alerts when a predefined condition is matched and results are found. These searches can be scheduled to run periodically, based on time intervals, window of interest, time range of interest, and more.

2.7.2.6 Collaboration

For the team assigned to and working on a case, Verint WebInt-INVESTIGATE offers an efficient collaboration platform. Investigation management offers one type of information sharing for the investigation participants. In addition, the collaboration framework provides a means for analyst to send and receive messages, and share information while enforcing the predefined security policies for the content being shared.

2.7.2.7 Security and Compartmentalization

Verint WebInt-INVESTIGATE provides a strict yet adaptable control of data access management, user data access and auditing of user actions. In Verint WebInt-INVESTIGATE, stringent security controls manage each step of the data ingestion, user data access, and investigation and collaboration process, based on the understanding that the system’s security factor must comply with zero tolerance requirements.

Verint WebInt-INVESTIGATE safely delivers:

Secure source integration	Access authentication and security mechanisms enable multiple sources from different organizations to be securely integrated.
Secure classified content	Data is secured and managed at multiple levels, allowing for controlled and authorized user-access across multiple departments, teams and investigators.
Secure information sharing	Content and information can be securely shared while access permissions are enforced.

Acting upon these guidelines, Verint offers the following range of security mechanisms:

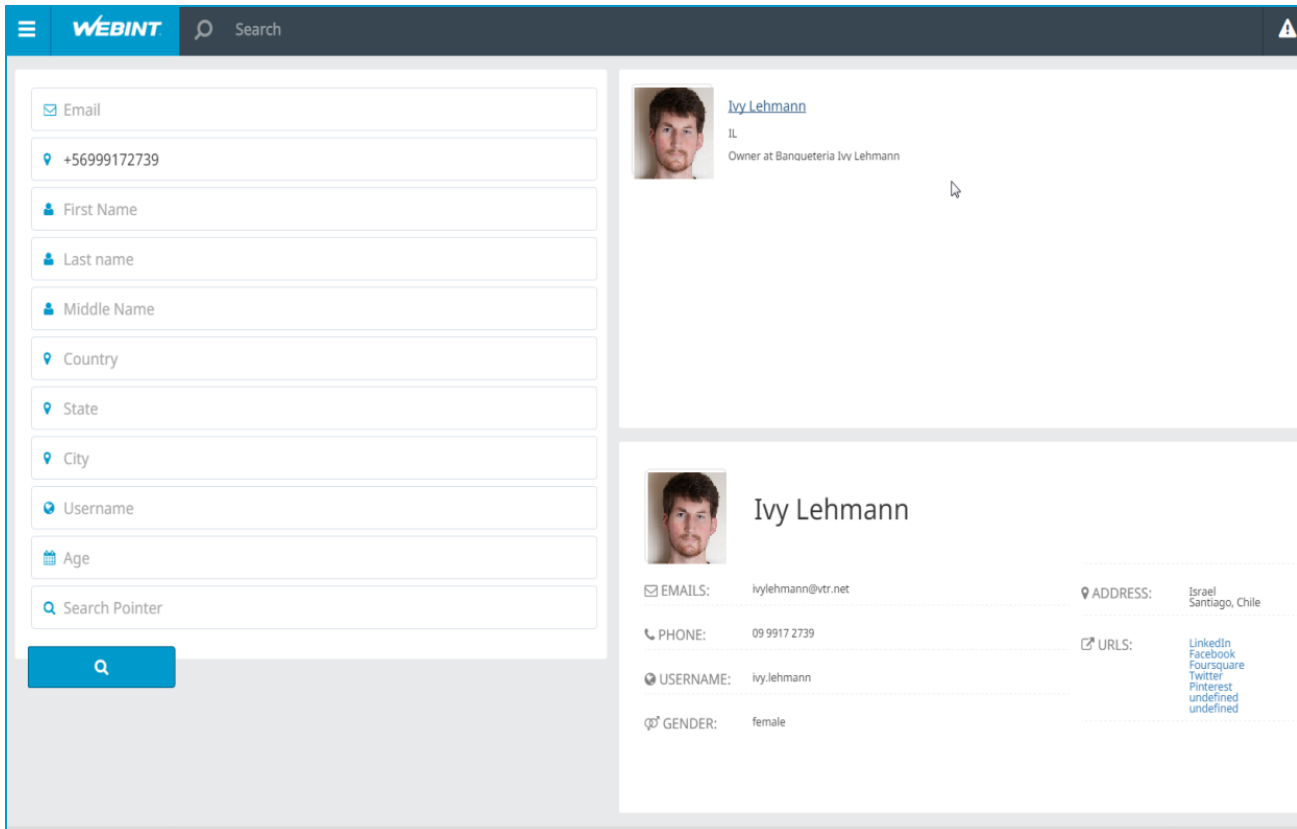
- **Content access control** – Data is controlled by user access permissions ensuring each item is accessed by authorized users only. Multi-level control mechanisms control access permissions at source levels that comply with a person-level and team-level requirements. This ensures data is used by approved personnel for authorized purposes only.
- **User level permissions** – User permissions determine which data items each user can access, and for what purposes
- **User authentication** – Different authentication sources can be implemented, including integration of enterprise LDAP. Organizations can retain existing enterprise authentication systems or use Verint WebInt-INVESTIGATE’s own authentication system.
- **User audit** – The system logs and stores each and every data access, search, investigation and analysis action performed by all users. Auditing allows the tracking of data usage – this is not limited only to actions of a specific user but also enables general tracking of how a data item has been used, by whom and for what purposes.
- **Active security model** – Regular security models often bind security permissions to content upon data ingestion, demanding heavy re-binding processes in the event of changes in the definition of permissions. Others use late binding techniques, where security permissions are bound upon content retrieval. In this case, content is retrieved wholly and only later filtered, which in case of error can result in a breach of security. The system implements a unique active security algorithm that supports a flexible and safe security model, with no performance reduction.

The platform active security mechanism uses a unique query-time join technique that binds security permissions during the initial retrieval action, which results in high flexibility for permission changes and no risk of retrieving unauthorized content.

2.7.3 Person Identify Search

The person identify search feature enable to quickly gain personal information on people from all over the world , the analyst can search the data by providing the person name ,phone number , email address or social account handle ,the system periodically scan the web and using harvesting technics and using advance entity

resolution algorithms , reveal the real identify of a person , the information returns can includes names, email address, phone numbers, social accounts ,images, ages, genders, workplaces, *related people* ,etc.



2.7.4 Fully Integrated with the Collection Platform

An investigation is an ongoing process, as new data is continuously discovered, and new leads are found. The analysis needs to have quick, easy and intuitive ways to extract new and relevant materials from the Web.

WebInt-INVESTIGATE is a holistic analytic and collection solution, therefore the analyst can request extraction of new data simply by pointing and clicking on the content he wants to extract.

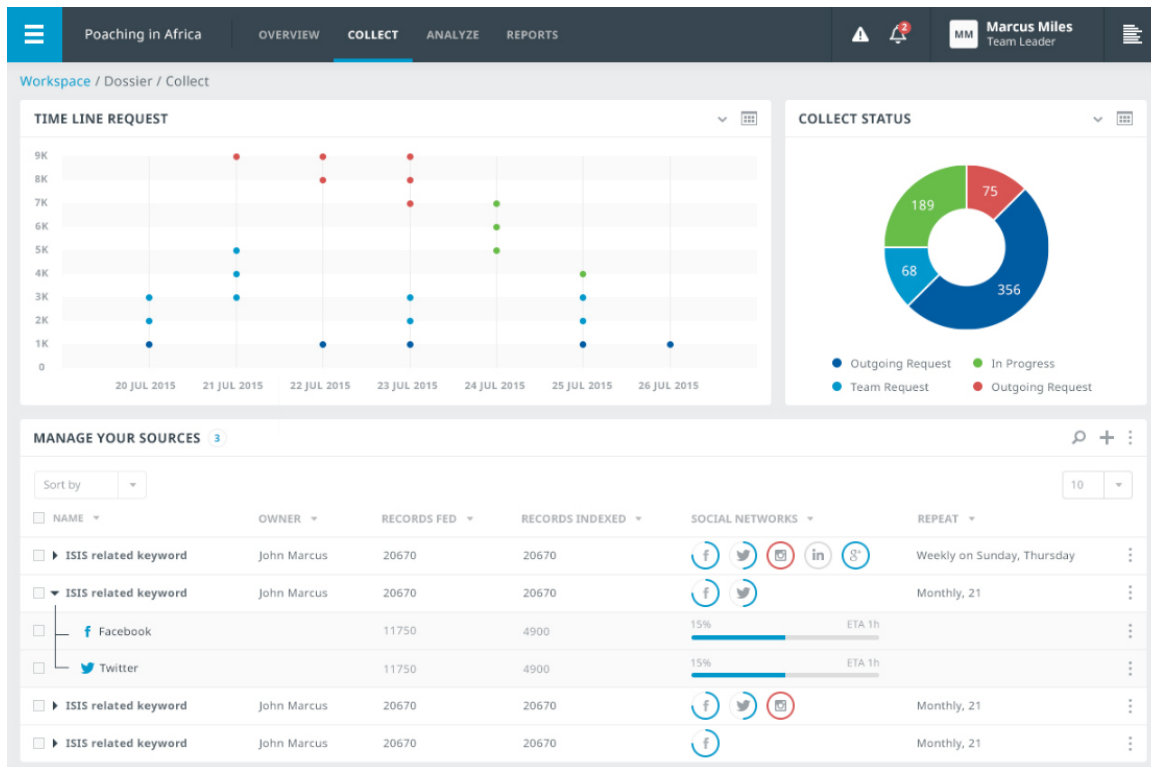


Figure 18 – WebInt-INVESTIGATE -ANALYTICS Collect integration

2.7.4.1 Reconstruction of a Web Profile

In cases where a Facebook account owner decides to limit access to his account (using privacy settings and restrictions), WebInt-INVESTIGATE allows analysts to run a reconstruction of the account’s lists of friends, and retrieve part of the shared information. If the analyst doesn't know in advance that the entity’s account is secured, WebInt-INVESTIGATE can help identify possible friends or groups as leads, which can then be defined in the WebInt-INVESTIGATE as entities, investigated separately, and lead back to the original target, thus enabling access to his activities.

By using leads that are approved friends of the account, such as close friends, related fan club or other group, WebInt-INVESTIGATE reconstruction engine exploits the account’s connections to open, non-secured friends or groups to recreate existing links, and locate friends/accounts that will finally lead to the required entity. That way, WebInt-INVESTIGATE recreates the entity’s list of friends, and enables access to the information that is shared with these friends, despite the restricted access to the entity's information.

2.8 WebInt BROWSER ADD-ON

The dedicated and secured WebInt browser is a complementary tool that enables the analyst to conduct online operations using a crafted virtual entity.

WebInt browser comes with various investigative tools that enable to conduct online investigation and special operations.

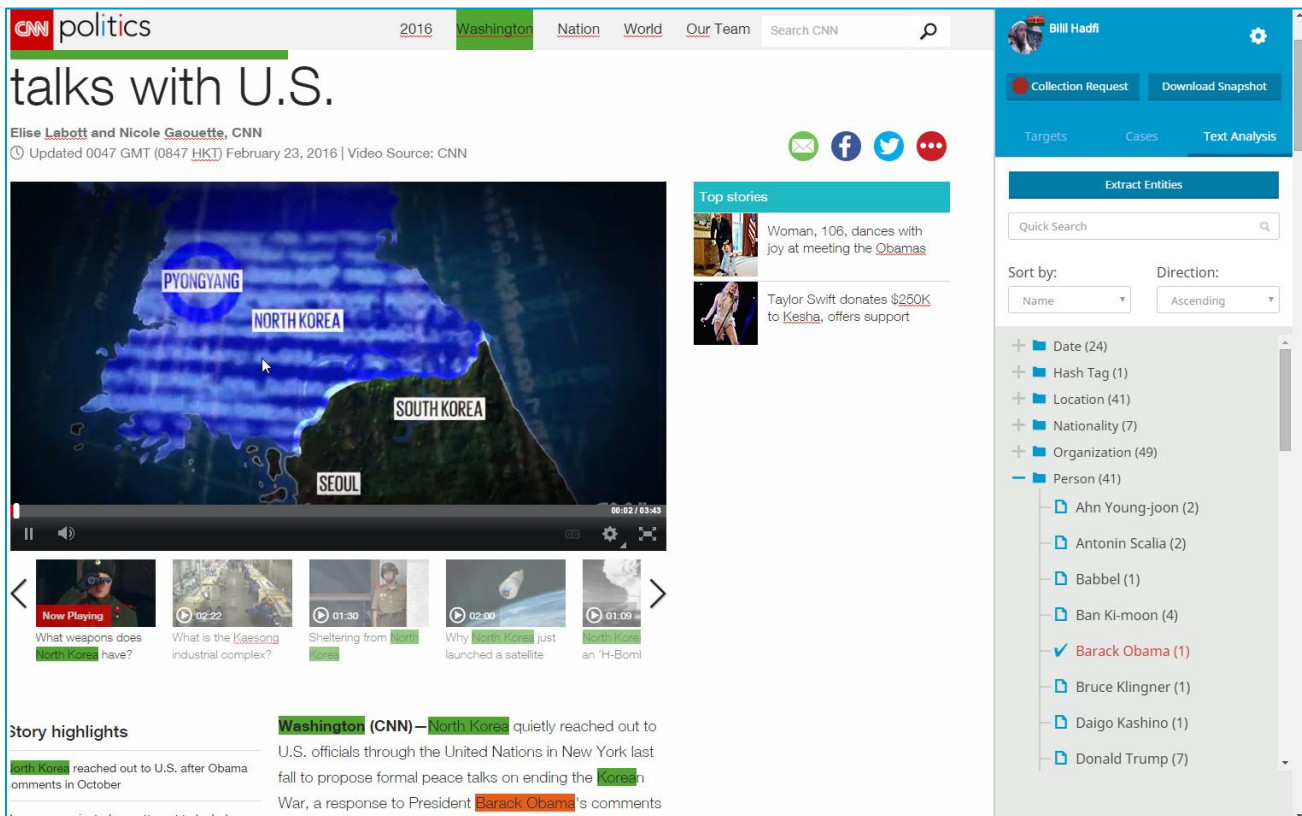


Figure 19 – WebInt–Secured Browser

2.8.1 Enhanced Security Environment

The WebInt secured browser technically ensures that online browsing is secure and anonymous; taking a holistic approach that enables the analyst to focus on the content while securing the investigation aims.

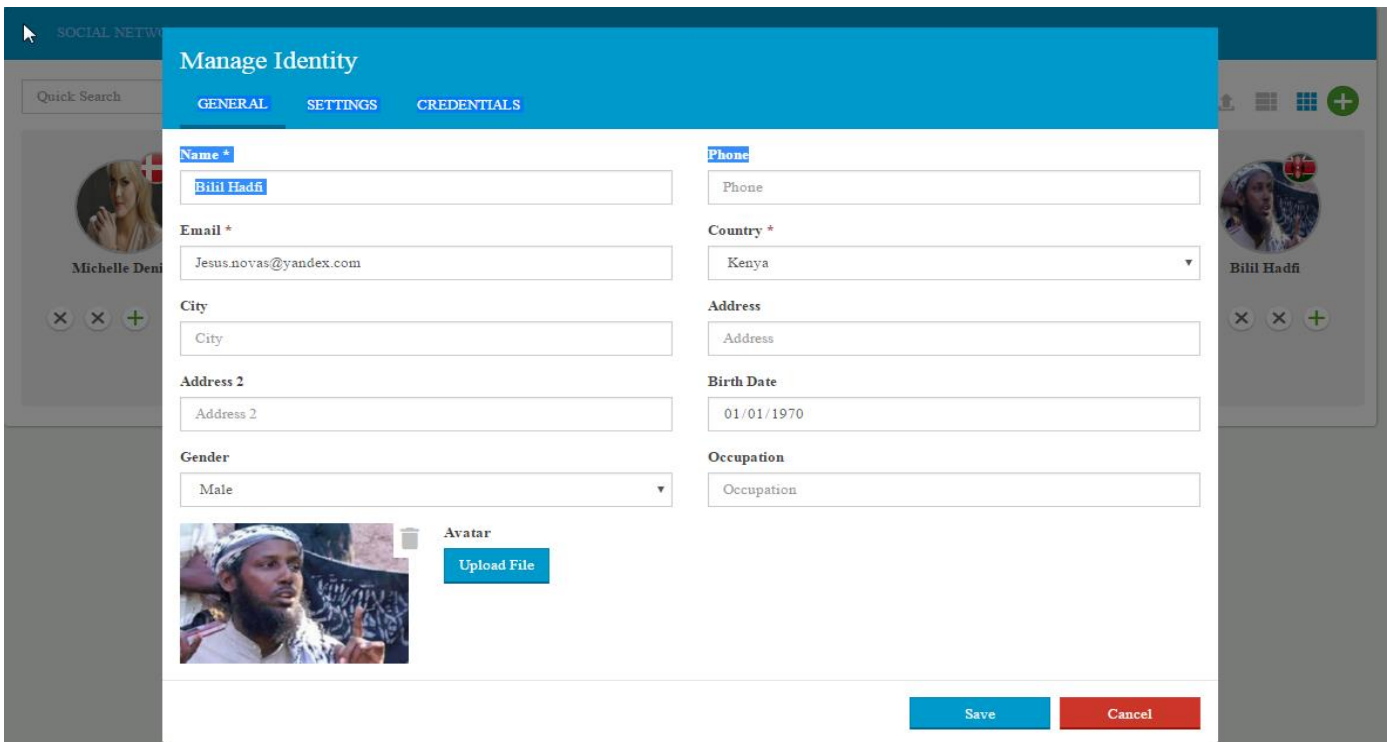
2.8.2 Avatar Management

A virtual entity is a fictitious entity (an online presence of a person) that is crafted to meet the investigation goals; using the virtual entity (avatar) the analyst can extract valuable content without compromising the investigation goals. The add-on browser enables the analyst to manage multiple crafted virtual entities over several investigations, multiple web-arenas and long periods of time.

The analyst can select which virtual entity will be used to surf the Web. The analyst can review the virtual entity detailed avatar card, learn about the avatar cover story, when needed, the analyst can seamlessly switch between avatars to meet the investigation objectives.


The secured browser ensures that the investigation is secure and anonymous by running the following security checks and locking procedures:

- Accessing the web using the avatar originating country IP address
- Verifying that the virtual entity will not be used concurrently



The screenshot shows a 'Manage Identity' form with the following fields and values:

Field	Value
Name *	Bilil Hadfi
Phone	Phone
Email *	Jesus.novas@yandex.com
Country *	Kenya
City	City
Address	Address
Address 2	Address 2
Birth Date	01/01/1970
Gender	Male
Occupation	Occupation

Avatar:  Upload File

Buttons: Save, Cancel

2.8.3 Added layers of information

The WebInt secured browser supercharges web browsing by displaying added layers of information on top of the browsed webpage. The secured browser automatically analyzes the web page and parses meaningful information without leaving the page.

2.8.4 Extracting Content While Browsing

The WebInt secured browser enables easy extraction of web data content on-the-fly while browsing the Web.

The analyst has two options:

- Manually capture specific items or a whole page and report it as insights
- Automatically issue a collection request for the relevant page data or the whole site using the WebInt-COLLECT platform

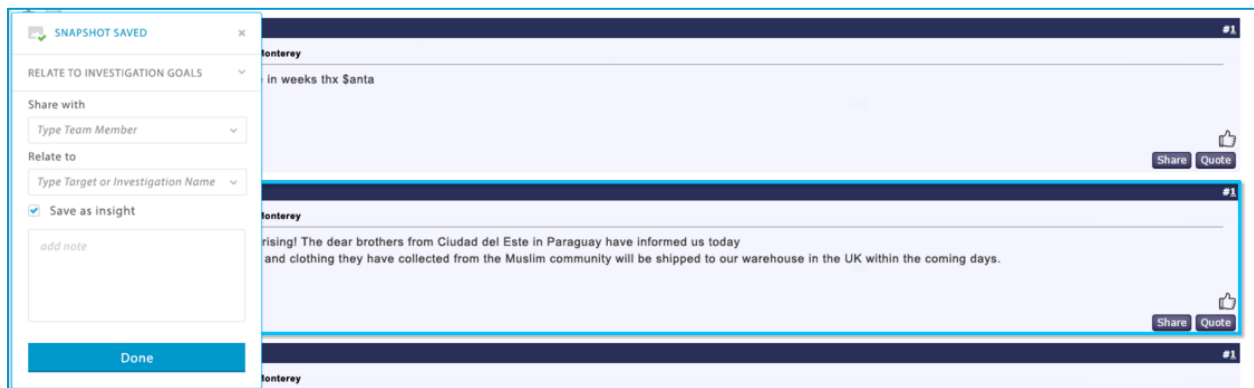


Figure 20 – Secured Manual Extract Web Content

2.9 WebInt-CONNECTIVITY LAYER

The WebInt-CONNECTIVITY LAYER is an integration layer between WebInt-COLLECT and other data sources and WebInt-INVESTIGATE.

Its main highlights include:

- **Distribution of collected data** – Manages and controls the distribution of the collected data on every stage, from WebInt-COLLECT to WebInt-INVESTIGATE or the customer's external information systems.
- **Security** – The WebInt-CONNECTIVITY LAYER functions as a security separation level between the external part of the system, WebInt-COLLECT, and the internal part, WebInt-INVESTIGATE system, which contains knowledge and investigation conclusions.
- **Cleaning Data** – Cleans up the collected data and scans for viruses.
- **Cleansing** – Cleanses the collected data, removes duplications, etc.
- **Enriching data** – Enriches the collected data using external engines.
- **Monitoring** – Monitors all tasks managed by the WebInt-CONNECTIVITY LAYER.

2.9.1 Manage and Control Collected Data Distribution

Data collected from the WebInt-COLLECT can be distributed to WebInt-INVESTIGATE, as well as to any other external information system, after appropriate authentication.

The WebInt-CONNECTIVITY LAYER distributes the collected data in XML format. The typical distribution is performed by copying a zip file (XML format) to the customer directory, but it also can be distributed using other methods, as agreed with the customer.

2.9.2 Security

The WebInt-CONNECTIVITY LAYER functions as a security separation level between the external side of the system that is connected to the web, and the internal part that contains knowledge and insights.

The data is transferred into the system through secure FTP (SFTP) protocol, and all the incoming data is scanned by the WebInt-CONNECTIVITY LAYER using antivirus applications.

2.9.3 Cleaning and Cleansing Data

In the process of moving the collected data into WebInt-INVESTIGATE, the WebInt-CONNECTIVITY LAYER cleans up the data and runs Norton Antivirus over all incoming data files. A suspicious file will be blocked from entering the analytic system.

After the data is cleaned, the WebInt-CONNECTIVITY LAYER checks the data and removes duplications in the new data, as well as between the new data and the existing data, and merges them together.

When collecting unstructured HTML data (by the “Unstructured Collection Engine”), the system analyzes the data to identify the main body of the page and remove advertising, “see also”, “More from...”, “Most popular...” etc. To help the analyst in focusing on the main subject of the page and to prevent false-positive results when searching for popular words and names, only the main content will be indexed.

2.9.4 Ingesting, Modeling and Enriching Loaded Data

Having incorporated external data into the system, the WebInt Data Ingestion and Processing layer is responsible for converting it into a uniform structure to create analysis-ready, meaningful information. Structured and un-structured content are transformed into logical entities that offer investigation-ready meaning, such as person, event, organization, and site.

Ingestion is a multi-step process configurable per data source and can include loops and concatenations.

2.9.4.1 Enriching Data

The WebInt-CONNECTIVITY LAYER provides ability to enrich the collected data before passing it on to the analytic system. During the enrichment process, the WebInt-CONNECTIVITY LAYER can integrate external engines that can generate added value to the analyst. External engines can provide add value, such as automatic translation of the content collected, extracting metadata of images collected, and more.

2.9.4.2 Distributing Data

The WebInt-CONNECTIVITY LAYER gets all collected data from the WebInt-COLLECT and distributes it to the required systems. On basic installation, the WebInt-CONNECTIVITY LAYER transforms all data to WebInt-INVESTIGATE only, but other customer's external systems can be connected to WebInt-CONNECTIVITY LAYER to receive the collected data.

2.9.5 WebInt-CENTER API

The WebInt API enables third-party systems to issue collection requests using the secure WebInt API and receive results using the WebInt export mechanism.

2.10 Introduction to Verint® WebAlert™

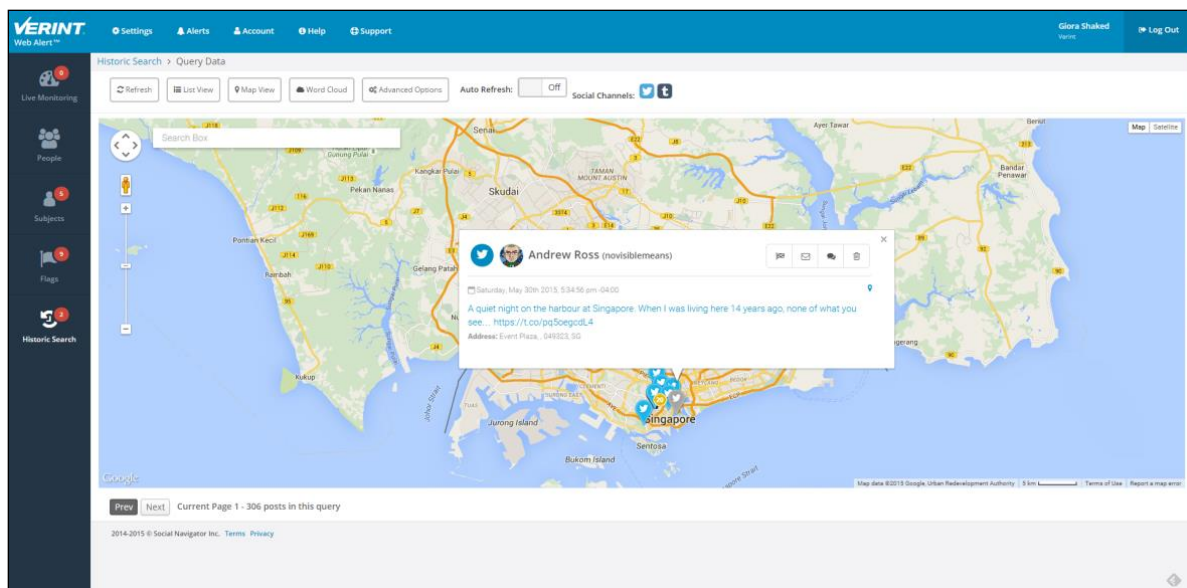
Web Alert is an SaaS web based application that interfaces with social media networks to collect and identify relevant communications in geolocations and for persons of interest. The system listens, monitors and extracts data from various social networks including Twitter, YouTube, and Instagram. It also collects aggregated information from the leading news outlets and blog platforms.

When social media communication occurs on the selected channels within the geolocation and with the specified keywords, the communication is saved for viewing in a live query. Similarly, when a person of interest posts on social media networks, Web Alert saves the communication making it available to Web Alert users for review. Web Alert saves text, photos and videos.

Web Alert detects high-risk posts and helps to identify potential threats and targets, preventing crime and terrorism before it happens. In addition to collecting relevant social media communications, Web Alert provides real-time notifications and analysis options for processing of these posts.

Web Alert builds an associate network that identifies the people closest to the person of interest, providing additional subjects for investigation and assessment, and the associate sub-groups identify clusters of connections who share common links.

Historic searching provides the capability to go back in time and retrieve all the social media content related to an event, enabling authorities to gather additional information for investigation and to locate witnesses and additional potential targets. A more detailed product description of Verint® WebAlert™ can be found in the attached Appendix.



2.10.1 Web Alert Functions

Web Alert performs the following main functions:

- **Live monitoring.** The system user defines the filter criteria, indicating which geolocation or area must be monitored, and what keywords should be used to include or exclude posts. Live monitoring is available globally.
- **People.** A person can be investigated by viewing their last posts, their risk score, and who follows them on Twitter, as well as via Facebook search, profile search, and uncovering, exploring and analyzing the person’s known associates and their group relationships on Twitter.
- **Subjects.** A person of interest can be monitored on an ongoing basis in real-time, via one or more of their social media accounts.
- **Historic search.** A search of historical data to identify and analyze what happened during a specific date range (up to two days of data).
- **Flags.** A list of bookmarked posts.
- **Alerts.** Creation of real-time alerts on live monitoring locations and on subjects available to mobile or email.




2.10.2 Web Alert Benefits







Web Alert provides the following benefits:

- Getting ahead of the threat and preventing tragedy. The system monitors and analyzes social media data in real-time to alert on potential imminent threats of shootings, stabbings, terror attacks, and so on.
- Creating actionable intelligence. The system filters available, unstructured social media data and delivers insightful and predictive modeling and analytics to create profiles and alerts. This analysis uses a combination of keywords, terms, location, geo-fencing metadata, and sentiment to identify conversations of interest. The uniqueness of the system includes, but is not limited to, the ability to better understand the specific context and nature of posts within a social community.
- Localized visual information. The geolocation-based data filters and history assist with dealing with public unrest, crisis management, and disaster response.

2.10.3 Data Channels

Web Alert monitors a broad range of social media channels.

Icon	Channel
	Twitter
	YouTube
	Instagram

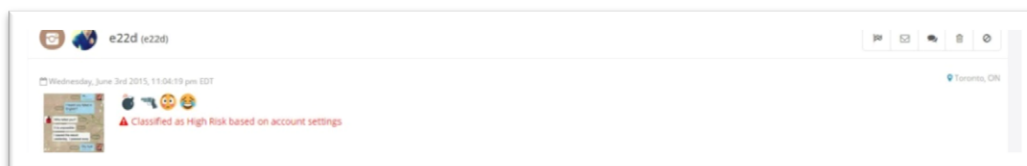
Icon	Channel
	Blog Web Alert supports over 27,000 news and blog sources from around the world. Note: This channel is potentially noisy and may return a large volume of irrelevant posts.
	Board Note: This channel is potentially noisy and may return a large volume of irrelevant posts.
	Tumblr
	YikYak
	News Note: This channel is potentially noisy and may return a large volume of irrelevant posts.
	Facebook
	VK

Additional social media platforms can be integrated.

2.10.4 Languages and Emojis

Web Alert parses keywords in 90 languages and supports multi-language searches. It also translates posts to and from these 90 languages including Spanish, English, Portuguese, and French.

Web Alert supports Emojis and automatically converts Emojis into their short-name. This enables users to search for posts containing Emojis. This is crucial as the use of Emojis in posts, particularly Instagram, is becoming more and more common. In some cases posts contain no ordinary text, just Emojis. A search for the word “gun” reveals posts that only contain emoticon references.



2.11 WebAlert System Features

This section describes the core system features.

2.11.1 Queries

Web Alert enables the definition of multiple live-monitoring queries using a geo-fence, complex keyword criteria (multiple keyword groups and exclude keywords), and geo keywords:

- Geo-fence comprising a circle, square or polygon.



- Boolean logic matching for keywords enables filtering for posts containing a specific keyword or combination of keywords.

Contain any of these words:

Add Keyword

You can click the High Risk icon to enable/disable High Risk

- Exclude keyword option enables pre-filtering for posts that contain a listed keyword, but not within the desired context. For example, the word “shot” may be in the keyword group, but is not worth mentioning when posted with the word basketball.

Contain any of these words:

Exclude keyword

- Geo-keywords facilitate the inclusion of posts without location services enabled, by using geographically relevant keywords, for example, “White House” or “JFK Airport”.

Geo keywords: Using region-specific keywords, what results do you want if there is no geolocation??

Geo Keyword

- Live query searching by top keywords as set in the initial query (available for the list view and map view, but not for the word cloud), author name, username, search terms, from date, to date, with geo, that is, referring to posts that have an actual geo tag as originally posted by the user on the channel, language, and channel type.

Live Query Details

BASIC INFORMATION

Name of query
South Carolina State House

Social Media Channels

LOCATION INFORMATION

Circle Radius in km: 50.00 | Current Location: lat 34.00040580000000 long -81.03282960000000

Geo Keywords - Region-specific keywords

imperial%wizard
kill%obama

KEYWORDS

Query results:

Contain any of these words:

acab
arrn%semitic
arrn%ban
charleston
confederacy
confederate%flag
dylann%roof
hider
imperial%wizard
kike
kill%obama
kill%president
kkk
klan

klux
naacp
nazi
nigger
nigro
protest
race
rally
shooting
supremacism
supremacist
supremacy
supremist
terror
weapons%ban

white%knights

Verint Systems Inc.

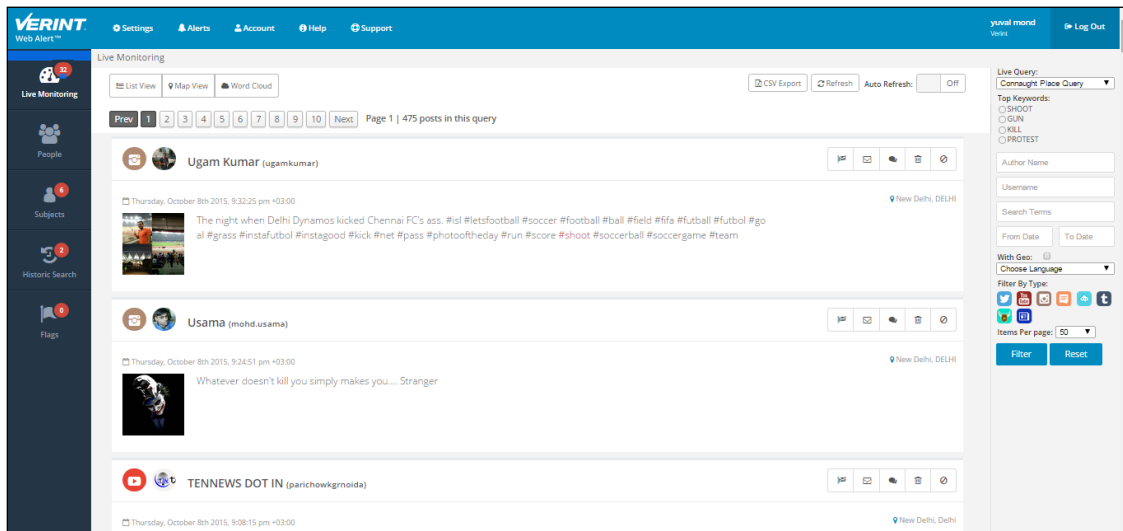
2.11.2 Live Monitoring

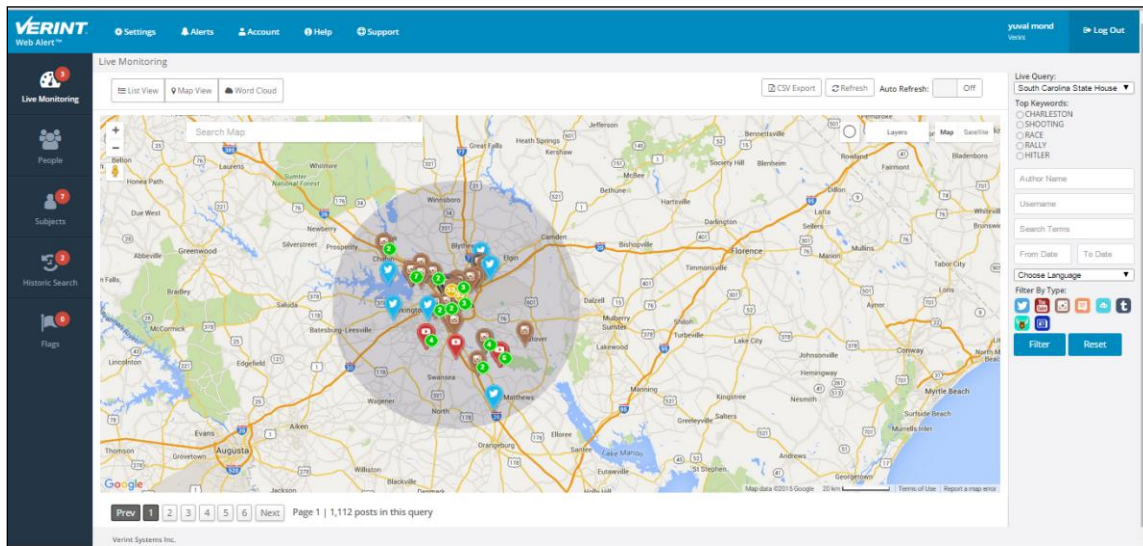
Live monitoring shows a list or map of the posts in the selected live query and is constantly updated with new results in real-time.



Posts are analyzed on an ongoing basis and a post containing a predefined high risk keyword is marked as:

⚠ Classified as High Risk based on account settings





Posts deemed to be threats based on predefined high risk keywords are marked as .

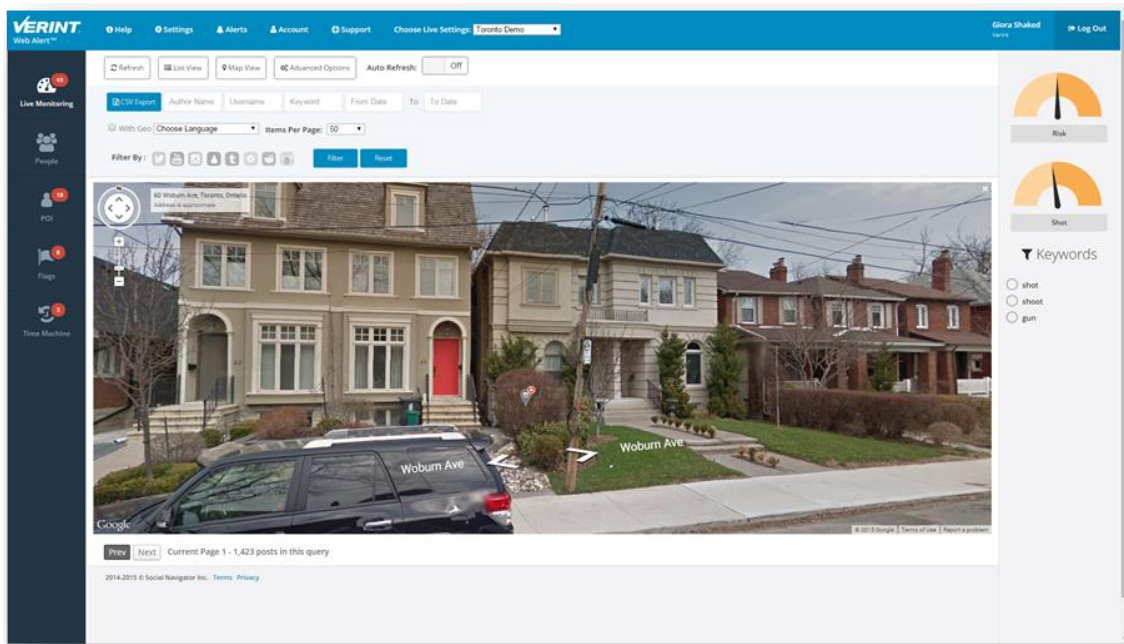


Posts can then be processed as follows:

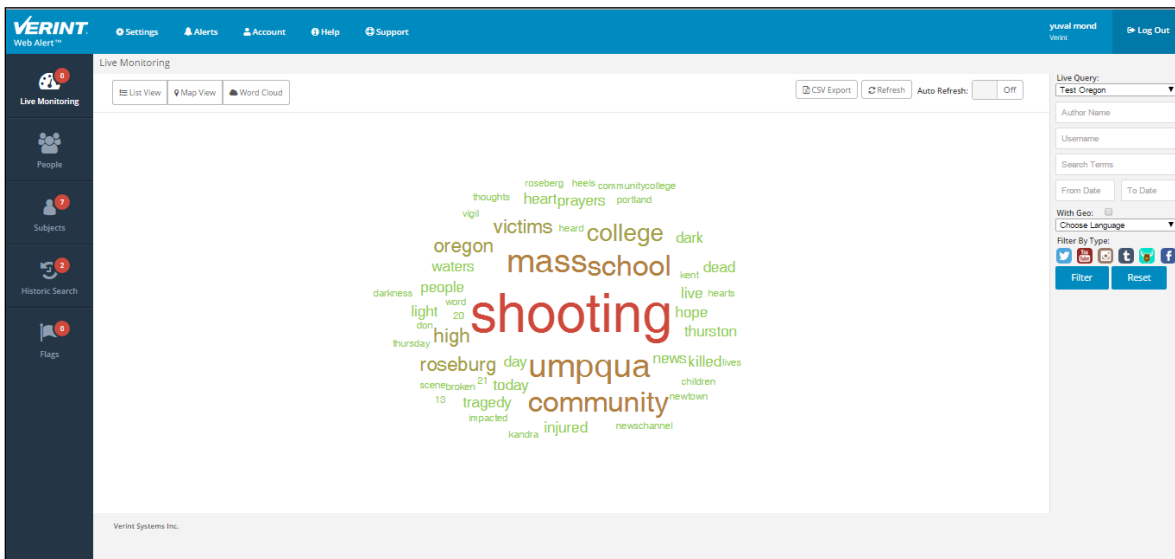
- Flagged for future action or analysis.
- Shared by email or text message (including the content of the post, the author and username, date and time of the post, address and street view images).
- Deleted to remove the post from the selected filter view.

In addition, the author of the post can be blocked, removing the posts for a specific user account from the data set. This user can be unblocked, restoring the data in the view. Web Alert users can also drill-down into the source platform to view the poster's profile.

Web Alert pinpoints the exact location of a post and can show the corresponding street view.



The word cloud shows a cloud view of the most frequent (top) words in the posts that meet the filter criteria, and enables users to drill down into a list view of the associated postings. This helps to determine common themes and provides a better understanding of which topics are most popular in the social media conversations.



2.11.3 Alerts

Web Alert enables users to set up and receive email and text alerts. Alert settings are defined by the user and can be based on customized keywords or when a subject makes a post, with the option to alert only when high risk keywords are used.

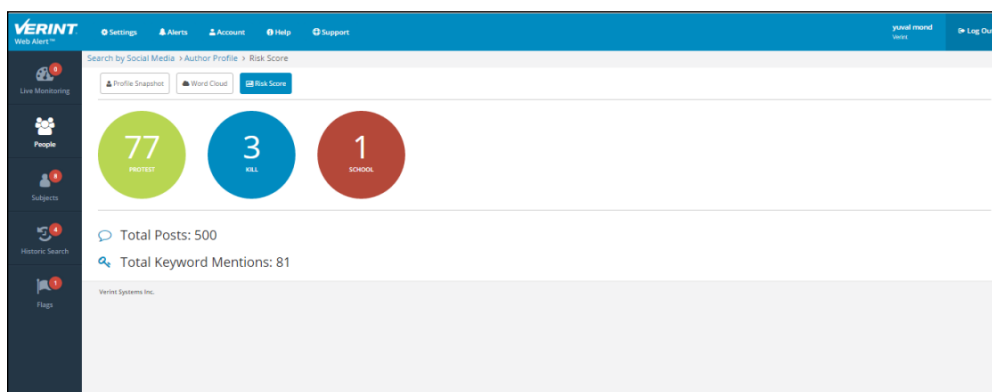
This enables the user to monitor subjects 24/7 as the system sends alerts as soon as it receives the post. The alert message contains the content of the post, any images contained in the post, the date and time the post was made, and street views of the location, if available. The alerts can be configured for any e-mail account or cell phone, and the recipient does not have to be a Web Alert user.

2.11.4 People

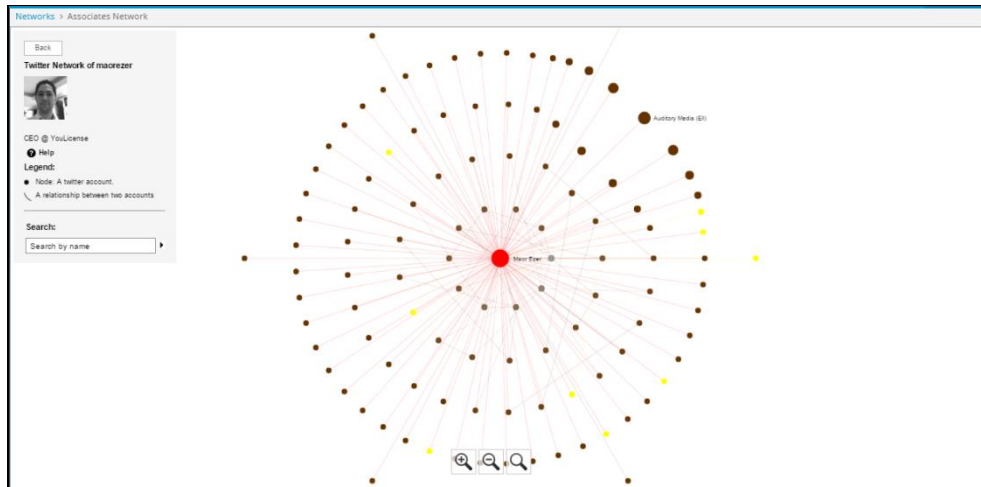
People can be investigated in the following ways.

- **User History.** Search for a person’s last 3200 posts on Twitter, Instagram, Tumblr and Facebook Pages 1000 and the last 500 posts on YouTube. Drilling down enables a user to view the person’s profile, word cloud, and risk score, as well as mark the person as a subject.

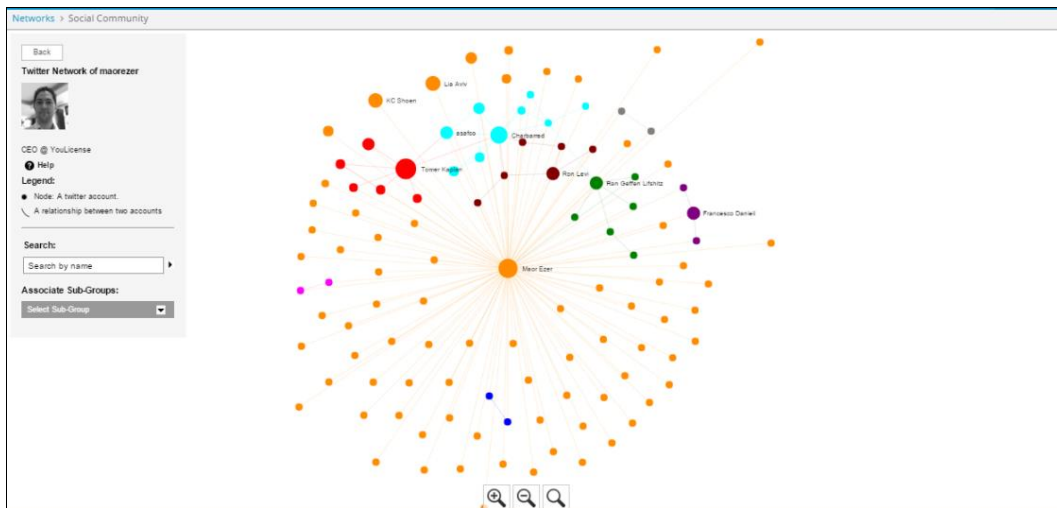
Web Alert also calculates the person’s risk score. This shows the number of times that the person has used each of the keywords in the active filter, as well as the total number of keyword mentions.



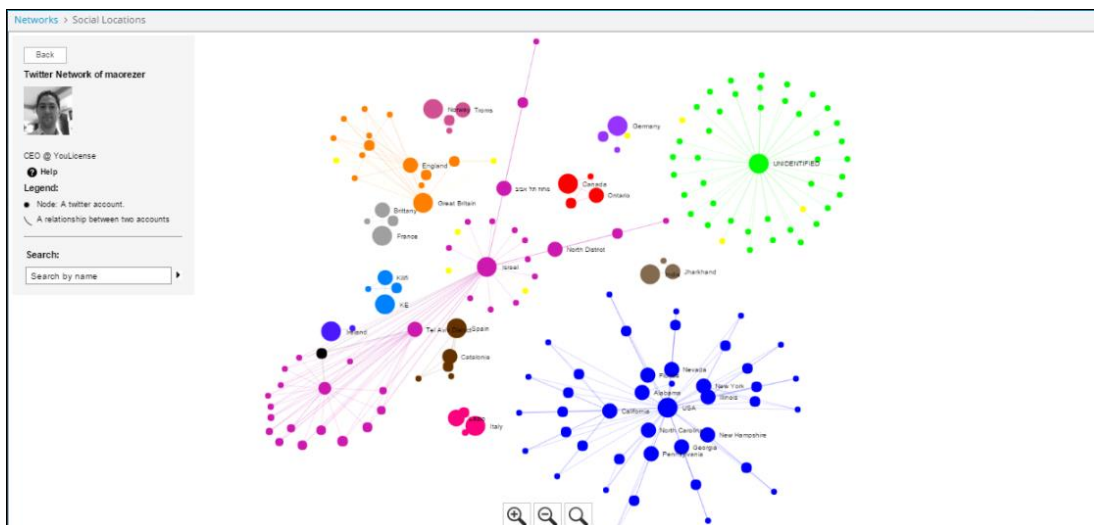
- **User Friends.** View who a person follows on Twitter.
- **Facebook Search.** Search Facebook for pages with relevant keywords (only pages and not personal profiles).
- **Profiles Search.** Search for profiles based on email address, Facebook username, Twitter username, and/or phone number (USA-only).
- **Social Networks.** Web Alert takes the analysis of a person’s posts further by uncovering, exploring, and analyzing the person’s known associates and their group relationships on Twitter. Web Alert enables the user to view an associates network and then drill-down to see the details for a connection. This feature identifies different groups that are more closely connected within the subject's social network. Many factors are taken into account including location, topics of interest, followers, and so on. All members of a group are assigned the same color. This enables law enforcement to drill-down into the groups and evaluate the users in order to determine how they are linked, for example, a gang, co-workers, or a sports team.



Web Alert enables users to view a person’s associated sub-groups and then drill-down to see the details for a connection. Web Alert identifies different sub-groups that are more closely connected within the subject's social network. Many factors are taken into account including location, topics of interest, followers, and so on. All members of a sub-group are assigned the same color.

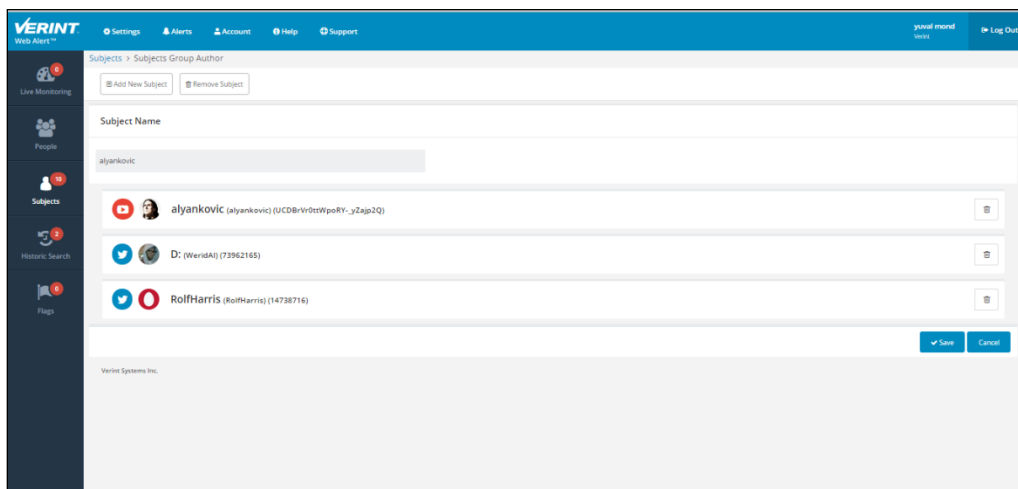


These groupings can represent nodes/people with similarities, for example, gangs, friends, family, colleagues, and teammates. This saves hundreds of hours of work by uncovering valuable intelligence about the relationships within a target group. The primary node within a group is also identified with a larger circle to help visualize who is important within the network. It is also possible to view the locations for the user’s associates.



2.11.5 Subjects

Web Alert enables monitoring of subjects (persons of interest) on an ongoing basis in real-time. Multiple social media accounts on Twitter, YouTube, Instagram, Tumblr or Facebook can be connected to a subject. Subjects are viewed in lists or maps in the same way as live monitoring of geolocations, and the same actions can be performed on these posts. Several social media accounts can be linked to a single subject.



2.11.6 Historic Search

The historic search enables the user to rewind and find out what happened in a specific date range (up to two days of data). This is especially useful for a post-event analysis to identify potential witnesses and suspects, view videos that were posted in relation to a particular event, and generally investigate the social media activity prior to and after an event.

2.11.7 Tags

The tags feature enables adding enhanced flexibility in managing and categorizing objects within the platform. Users can create as many tags as needed to either use them as folders for case management and/or to label elements with topics or categories. Elements that can be tagged are: Posts, Live Queries, Historic Queries, Profiles, Social Graphs, Subjects, Reports and Alerts. Each element can be assigned one or several tags.

2.11.8 Image Retention

The main image of each post is captured and stored for 30 days, providing the ability to view a full post even after it has been deleted. If a customer needs to retain the Image indefinitely, they can manually select that image for persistence.

2.11.9 Reports

The feature allows users to generate reports that display graphs of data volumes over time, channel distribution, language distribution, top authors, top keywords, top hashtags and top links.

2.11.10 Top Authors View

A capability which allows users to quickly identify influential authors and detect common authors.

2.11.11 Sentiment Analysis

All posts are analysed to determine average sentiment and those posts that have either positive or negative sentiment.

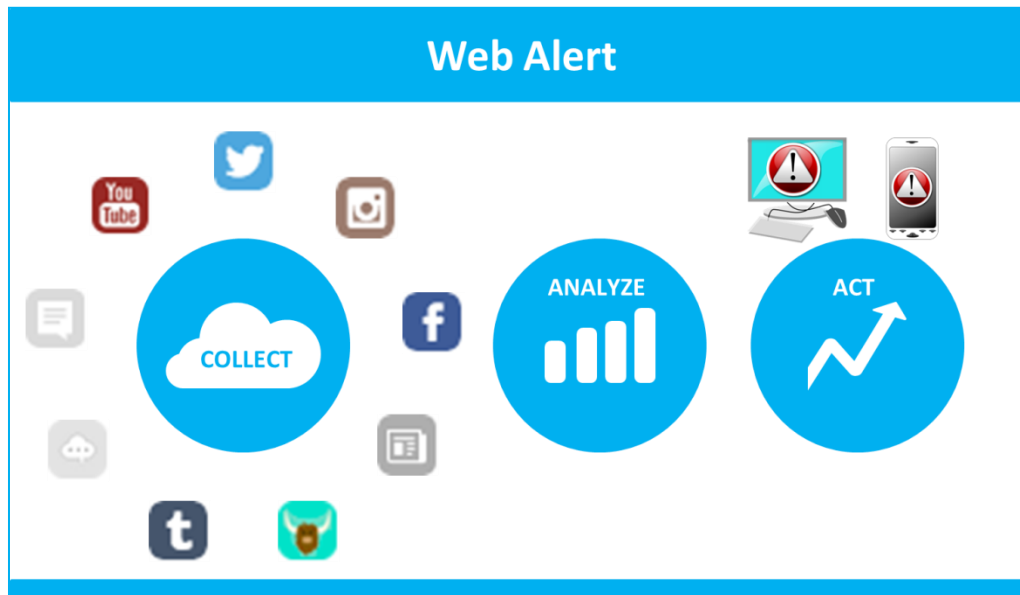
2.11.12 Capture Screenshot of Posts

Any Post can be exported to a pdf format. The exported post includes the post, the image (when available), the post location on a map and street view imagery of the location (when available).

2.12 WebAlert Technical Overview

Web Alert is deployed as a Web-based application hosted on the cloud in the USA that requires no installation. Web Alert can be accessed globally. The system is sold as a SaaS solution.

2.12.1 Architecture Flow



2.12.2 Technical Capabilities

The system:

- Supports a broad range of social media channels, Twitter, YouTube, Instagram, Blog, Board, Tumblr, YikYak, Sina Weibo, VK, News, and Facebook. Additional social media platforms can be integrated as required.
- Collects up to 1,500,000 posts every calendar month (can be expanded upon customer request).
- Saves social posts, images, and video.
- Runs up to 50 concurrent live queries (can be expanded upon customer request).
- Supports and translates up to 90 different languages. The complete list is detailed in https://translate.google.com/about/intl/en_ALL/languages.html.
- Converts Emojis into their short-name.
- Creates social networks for Twitter users with up to 10,000 followers.
- Performs historic searches on Twitter as far back as 2006 and 30 days on Instagram with each search up to 2 days in duration.
- Exports data via a CSV file.

2.12.3 Backfill & History

The backfill is the number of posts or days that the system retrieves from the past and presents in the result set when a query on location or subject or a peek query are performed.

	Twitter	Facebook Pages	Instagram	Tumblr
Backfill of new query	up to 500 recent posts up to 7 days back		up to 100 recent posts up to 7 days old	
Backfill of Subject	up to 3200 posts up to 1 month old	up to 1000 recent posts	up to 1000 posts up to 1 month old	up to 1000 posts up to 1 month old
Peek	up to 500 recent posts up to 7 days back		up to 500 recent posts up to 7 days back	
History for an individual account	up to 3200 recent posts	up to 1000 recent posts	up to 1000 recent posts	up to 1000 recent posts

2.12.4 Technical Requirements

Web Alert requires:

- The most recent version of Chrome is recommended.
- More than 2 Mbps of bandwidth for download per workstation.

2.12.5 Security

Security is an essential component of the overall design and use of Web Alert. The system contains security features that protect against external penetration and unauthorized internal usage. These security measures protect the data stored in the system and control access to that data. Data is isolated from other organizations at the application layer by organization ID and user ID.

2.12.6 Data Policy

Web Alert results are displayed in real time. For sources with fire hose agreements in place (Twitter, Tumblr, and commenting platforms for blogs and websites), there is a very low latency between when the post is made and when the platform displays it. For sources with API access, there may be a short delay between when the post is made and when the platform receives it from the API.

- **All results are archived.** All posts generated by predefined queries are saved in the database. In addition, when a person of interest (subject) is identified, all of the subject's posts are archived within the system regardless of the content or location. When a user deletes a query or a subject, the related data is deleted logically, that is, the relationship to the post is deleted. The physical data is retained. If the post forms part of another query, it remains available.

- **Throughput capability.** Our current infrastructure processes around one million posts per day. Scalability is determined by hardware resources. With appropriate planning, Web Alert can be scaled up and adjusted to any expected volume.
- **Historical performance statistics.** We monitor our servers and platform 24/7. To date, we have had 99.8% uptime of our platform, with the exception of the planned maintenance events. We notify our users well in advance of the scheduled downtimes. These periodic system maintenance events usually last from 30 to 120 minutes and on a monthly or bi-monthly basis.

2.12.7 User Levels

Web Alert allows admin users to create and share live queries, subjects, and historical searches in read-only mode with other authenticated users that belong to the same organization. All Web Alert users can share specific posts via email or text with others (including those outside of Web Alert).

There are two levels of users:

- **Admin user.** An admin user can create, edit, share or delete live queries, historical searches, and subjects, as well as create read-only users. They can also activate and deactivate the live queries and subjects.
- **Read-only user.** A read-only user can view and interact with the content collected by the various queries created and shared by an admin user. A read-only user can read, flag, share and export information but they cannot add or edit queries, historical searches or subjects.

There are two types of read-only users an administrative user can create:

- **Read-only.** This user will be able to see only the information specifically shared with him on a query by query basis.
- **Clone.** This user will be able to see all the queries and subjects under the admin user above him. A clone of all the content

2.13 Proposed Solution for Boston PD

Verint® Open Source Web Intelligence™ system is designed for scalability. Upon request, the system dimensioning can be easily scaled up. The following tables include the proposed configuration for a hybrid solution containing both Verint® WebInt™ as well as Verint® WebAlert™.

2.13.1 Verint® WebInt™ - Collect Configuration

	Description	Qty
Verint® Open Source Web Intelligence™ – Collect Components	Number of Crawlers	2
	Number of Admin User Licenses	1
Verint® Open Source Web Intelligence™ – Collect Features	Custom Actions	Yes
	User Mimicking	Yes
	Proxies management (ProxiEra)	Yes
	Collection via TOR	Yes
	De CAPTCHA* *This feature excludes on-going service by content	Yes
Hardware	Turnkey solution	Yes

2.13.2 Verint® WebInt™ - Analytics Configuration

	Description	Qty
Verint® Open Source Web Intelligence™ – Analytics Components	# of Concurrent User Licenses	10
Verint® Open Source Web Intelligence™ – Analytics Features	Text Entity Extraction <ul style="list-style-type: none"> Language: English support 	Yes
	Facebook Social Profile Reconstruction	Yes
	Same person automatic Identity matching suggestion	Yes
	Geographical Location Presentation Support	Yes
	Automatic Export of collected data	Yes
Hardware	Turnkey solution	Yes

2.13.3 Verint® WebInt™ - Web Flows

The Verint® Open Source Web Intelligence™ solution is delivered with the following pre-built generic Web flows for collection by Verint® Open Source Web Intelligence™ – Analysts:

- Facebook – User Profile, Event, Group, Page, Search
- Twitter – Target and Search
- YouTube – Target and Search
- LinkedIn – Target
- Google Search (cache data)
- Instagram.com
- Forum – Vbulletin

Additional specific web flows can be created by the system users using the Verint® Open Source Web Intelligence™ – Collect or provided by Verint at additional cost.

2.13.4 Verint® WebInt™ - Hardware

Verint® Open Source Web Intelligence™ suite including all modules will be installed on virtual machines. Servers will be optimized for HW and SW requirements.

The system will be installed on 5 physical servers:

- Collection Server
- Analytics Server
- Indexing Server
- Management Server
- Geo Server

The hardware which will be supplied for all servers is based on: Dell PowerEdge FC430/FC630 servers.

Please find below the specification of each server:

2.13.4.1 Collection Server

Physical machine	VM name	# Cores	Memory [GB]	Hard Disk [TB]	Hard Disk [TB]	Storage [TB]	OS
Collection	Hardware Specification:						
	PowerEdge FC430, 2 * CPU E5-2670v3 (2.3Ghz), 12 Core per CPU						
	128GB RAM, 6x1.2TB HD RAID 5 Capacity 5.46TB;						
	Network :						
	1. LAN – Gb Ethernet						
	2. WAN – DN/UP : 20Mbps/5Mbps * lines for failover						
	CollectDB1 MS SQL Standard	4	48	0.04	0.21	2	Win2012 Server
	CollectAdmin1	4	16	0.04	0.21		Win2012 Server
	CollectCU1	5	14	0.04	0.21		Win2012 Server
	CollectCU2	5	14	0.04	0.21		Win2012 Server
CollectExport1	6	24	0.04	0.21	1.5	Win2012 Server	

2.13.4.2 Analytics Server

Physical machine	VM name	# Cores	Memory [GB]	Hard Disk [TB]	Hard Disk [TB]	Storage [TB]	OS
Analytics	Hardware Specification:						
	PowerEdge FC430, 2 * CPU E5-2670v3 (2.3Ghz), 12 Core per CPU						
	128GB RAM, 6x1.2TB HD RAID 5 Capacity 5.46TB;						
	Network :						
	1. LAN – Gb Ethernet						
	MS SQL	8	32	0.04	0.21	1	Win2012 Server
	Load Balancer	2	18	0.04	0.21		Win2012 Server
	Node JS (PL), front end browser extension	4	18	0.04	0.21		Win2012 Server
	MPS1 - HM/SEP12/WSUS/AD	2	6	0.04	0.21	1	Win2012 Server
Basis, Analytics API	8	24	0.04	0.21		Win2012 Server	

2.13.4.3 Indexing Server

Physical machine	VM name	# Cores	Memory [GB]	Hard Disk [TB]	Hard Disk [TB]	Storage [TB]	OS
Indexing Server	Hardware Specification:						
	PowerEdge FC630 Server Node, 2xE5-2670 V3, 2 * CPU E5-2670v3 (2.3Ghz), 12 Core per CPU						
	512GB RAM, 4x1.2TB HD RAID 5 Capacity 5.46TB;						
	Network :						
	1. LAN – Gb Ethernet						
	Ingestion	8	128	0.04	0.21		Win2012 Server
	Indexer, searcher	12	356	0.04	0.21	3	Win2012 Server
Load Balancer	2	8	0.04	0.21		Win2012 Server	
SQL server	2	16	0.04	0.21	1	Win2012 Server	

2.13.4.4 Management Server

Physical machine	VM name	# Cores	Memory [GB]	Hard Disk [TB]	Hard Disk [TB]	Storage [TB]	OS
Management Server	Hardware Specification:						
	PowerEdge FC630 Server Node, 2xE5-2670 V3, 2 * CPU E5-2670v3 (2.3Ghz), 12 Core per CPU						
	512GB RAM, 4x1.2TB HD RAID 5 Capacity 5.46TB;						
	Network :						
	1. LAN – Gb Ethernet						
	Attivio Management	6	64	0.04	0.21		Win2012 Server
	Nuxeo 1	6	190	0.04	0.21	1	Win2012 Server
	Nuxeo 2	6	190	0.04	0.21		Win2012 Server
Pstgres SQL	6	64	0.04	0.21	1	Win2012 Server	

2.13.4.5 Geo Server

Physical machine	VM name	# Cores	Memory [GB]	Hard Disk [TB]	Hard Disk [TB]	Storage [TB]	OS
Geo Server	Hardware Specification:						
	PowerEdge FC430, 2 * CPU E5-2670v3 (2.3Ghz), 12 Core per CPU						
	128GB RAM, 6x1.2TB HD RAID 5 Capacity 5.46TB, 4*800SSD						
	Network :						
	1. LAN – Gb Ethernet						
	Geo Maps		12	64			

2.13.5 Verint[®] WebInt[™] - OS & Third Party Software

Description	QTY	Remarks
Windows 2012 R2 std	4	
Windows server 2012 R2 Telco	7	
Symantec Antivirus 1 User royalties	18	Per Server
SQL Server 2012 Standard 32/64	4	per DB server CPU
SQL 2012 Standard CAL 32/64 bit, Runtime license	25	Per User
Symantec AV For Network Attached Storage	25	Per User
Bitvise SSH Server	1	
Hyper-V	10	Per Server CPU
ubuntu 14.04.1 for 64bit AMD	1	
Attivio ANALYTICS Engine	1	
Basis Entity Extraction Engine	1	

Nuxeo content management Engine	1	
---------------------------------	---	--

2.13.6 Verint® WebAlert™ - SaaS Configuration

Verint® WebAlert™ is deployed as a Web-based application hosted on the cloud in the USA that requires no installation. Web Alert can be accessed globally. The system is sold as a SaaS solution and only user credentials are required for operation. The following system configuration is proposed:

No.	Item	GOLD
1.	Verint® Web Alert system package One year SaaS license	Included
2.	Training	Included
3.	Admin User Licenses <i>Admin users can create & modify query settings and create POI and time machine queries</i>	25
4.	Read Only User Licenses	125
5.	GEO Enabled Concurrent Queries <i>GEO enabled queries allow the user to monitor a location in real time based on GEO setting and keywords. These are concurrent live queries</i>	50
6.	Posts per Month <i>Aggregated posts pull from GEO queries, time machine and POI. Resets every month</i>	Up to 1,500,000
7.	Time Machine Units – Calendar Day <i>Historic queries of Twitter and Tumblr up to 3.5 years history. Resets every month</i>	Up to 260 days per month
8.	Data Storage	Unlimited
9.	Social Channels <i>Includes Twitter, YouTube, Instagram, YikYak, Board, Tumblr & news and blog aggregators</i>	All

10.	Annual Warranty	Included with annual license
-----	-----------------	------------------------------

2.14 Response to RFP Section 7A – Overview

Verint Systems is pleased to submit a proposal for a real-time open source and social media threat detection and analysis systems, software, and/or services for use by the Boston Regional Intelligence Center (BRIC) and select law enforcement personnel of the Metro Boston Homeland Security Region (MBHSR). Verint's proposal is based on the Verint® Web Intelligence Center product line consisting of both our Verint® WebInt™ as well as our Verint® WebAlert™ products.

This Verint offering will meet the condition to provide commercial off the shelf (COTS) desktop software applications, web-based software applications, and/or integrated services that will proactively alert personnel to threats communicated via social media and/or online open source platforms, allow for geospatial monitoring for threats via online open source and/or social media platforms, and provide capabilities designed specifically to support investigative processes and analysis of online open source and social media information.

The proposed solution will have the potential to greatly enhance the BRIC's and MBHSR's ability to identify, collect, aggregate, synthesize, evaluate, analyze, visualize and investigate criminal activity and threats to public safety via social media platforms and other online open source environments. Furthermore, these capabilities will leverage both real time and historic data sets from the aforementioned platforms and environments, and can be complemented and enhanced through their integration with existing structured and unstructured databases native to the Boston Police Department and Boston Regional Intelligence Center.

The solution leverages complementary "big data" and "fast data" architectural options to satisfy a variety of analytical and investigative requirements, to include considerations for optimizing "fast data", i.e., providing the BRIC with the enhanced capabilities of real-time stream processing and stream-based analysis to support public safety decision making related to emerging threat scenarios.

The end-to-end Verint® Web Intelligence Center solution collects and analyzes open-source Web content and transforms it into Actionable Intelligence®.

Verint® Web Intelligence Center applies the latest open-source Web intelligence methodologies to continuously access information from a multitude of open Web sources to extract and analyze the information contained therein.

Using the most advanced technologies available today, Verint® Web Intelligence Center streamlines the integration of the vast amounts of open-source Web data, generates new leads and tracks negative influencers, thus optimizing the investigation process. With the modular, scalable architecture and browser-based user interface of the solution, users do not have to install any applications when deploying the solution and therefore can keep IT involvement to a minimum.

Verint® Web Intelligence Center was especially designed with the unique requirements of the intelligence, law enforcement and security communities in mind. Verint® Web Intelligence Center places a focus on the confidentiality of the investigation's process. The system topology and the crawling algorithms are developed in such a manner that even if one of the crawler's tasks is exposed, the investigation's target still remains covert.

From the data collaboration and information sharing point of view, the open architecture of the system enables smooth connectivity to other intelligence systems in the organization, using standard and proprietary protocols.

Unlike many other open-source Web intelligence solutions in the market, Verint® Web Intelligence Center offers an end-to-end solution with a single unified user management interface – both for data collection and data analysis. The benefits of this comprehensive solution are far beyond the sum of its parts – instead of inefficient and prone-to-error data transformation processes between the system modules, the integrated approach provides continuous and automatic interaction between the different subsystems, ultimately resulting in more relevant leads, more data about the topics and persons of interest and faster time to intelligence.

2.14.1 Proactive Alert/ Warning Capabilities

Alerts and early warnings can be generated based on customizable triggers and adjustable thresholds. Trigger scenarios can be based on levels of activity, keyword combinations, etc. The definition of specific authors, sources, and levels of activity per keyword provides timely alerts on suspect behaviors. Further details on alerts can be found in [Section 2.11.3](#) above.

2.14.2 Analysis/ Crowdsourcing/ Social Threat Monitoring

WebInt Center enables investigative units to leverage Web, and open source data in order to identify insights and help accelerate investigations of fraud, criminal, terror, cyber and national security threats. It helps transform large volumes of content into meaningful intelligence and identify suspicious behavioral patterns including locations of suspects and links between suspects. Further details on analysis capabilities for WebInt can be found in [Section 2.7](#) and [Section 2.11.11](#) for sentiment analysis.

Verint Webint-INVESTIGATE continuously accesses defined websites and newly added sites/user forums to monitor them for newly added activity, recently confirmed users and new user forums.

2.14.3 Investigative Capabilities For Public Safety

WebInt-INVESTIGATE analyzes vast amounts of diverse, open-source content to enable rapid identification and tracking of events, targets, threats, and related activity.

Key benefits of WebInt-INVESTIGATE include:

- Topic Investigation - Emerging events analysis and general tracking of developments issues allow law enforcement organizations to track general and specific group activities. Keeping track of emerging events helps reduce surprise factors, and can help maintain public safety
- Target Investigation - Target characterization provides immense background information, automated alerts reveal investigation leads, and interactive links allow investigation drill-down. A target unification approach unifies the accounts of similar entities together, by actively proposing a relation between them, and possibly indicating the different accounts/names of the same person.
- Be Forewarned by Alerts - Alerts and early warnings can be generated based on customizable triggers and adjustable thresholds.
- Manage and Control Collection - This solution schedules the tasks, manages resources and logins to sites and follow-up on the collection until receiving the output data.

3 TECHNICAL DESCRIPTION

3.1 Response to RFP Sections 7B & Sections 8C-G

The following sections are direct responses to the technical requirements specifications as requested in RFP Section 7B

3.1.1 Summary Requirement 1 – Collection (RFP Section 7B1)

#	Detailed Technical Collection Requirements	Compliance	Comment
1.1	Solution shall be able to query content from any publicly available open source internet site including but not limited to blogs, news media websites, forums, chat rooms, social media such as Facebook, Twitter, Instagram, YouTube, Pinterest, Google Plus, Tumblr, LinkedIn, Reddit, VK, Flickr, Vine, Meetup, Ask.fm, Classmates, Periscope, Craigslist, Backpage, etc.	Comply	This platform supports web data extraction from virtually any HTML-based website, offering site-specialized robots, sophisticated crawling and harvesting capabilities.
1.2	Solution must allow user to save select content based on a query	Comply	
1.3	The solution will be able to query content from multiple types of sources, including internal structured and unstructured continually updating data sets, including but not limited to network file connectors, databases connectors, email connectors, API connectors, and SharePoint libraries	Comply	The solution supports querying data from various structured and unstructured data sources, including web sources, database connectors (JDBC supported), files connectors (support 500 file format) ,Emails, API connectors, AD, Documentum, SharePoint, Exchange and other
1.4	Solution shall allow query parameters to include the following: keywords, Boolean logic search strings, usernames, geo-fenced areas, emoticons	Comply	
1.5	Solution shall allow for metadata to be added to the query, including at least a name and notes field. (Ability to name the query)	Comply	When defining a query the user can save it for later use. Besides providing a name to the query the user can also add a description to a saved query.
1.6	Solution shall provide the ability to create additional queries as needed with independent search parameters, filters, and alerts	Comply	Refining and navigating the data is one of the day to day tasks of an analyst. The system supports defining various queries that can be saved , and executed in parallel
1.7	Solution shall provide the user the ability to group two or more	Comply	The user can combine several

#	Detailed Technical Collection Requirements	Compliance	Comment
	queries together and run them in a combined fashion using Boolean operators		queries together and run them in a combined fashion , each query can include various search operators and the user can decide which Boolean operators apply the combined queries
1.8	Solution shall be able to query content from the "surface of the web" (e.g. internet content indexed by most popular search engines), "deep web" (e.g. internet content that is not indexed by popular search engines, some of which may be found in closed forums), and "dark web" (e.g. internet content that is not indexed and is found within encrypted networks, such as TOR, requiring special web browsers and security protocols)	Comply	<p>The platform employs various collection strategies and mechanisms to reach data found in the Surface, Deep Web and Dark Web layers among them:</p> <ul style="list-style-type: none"> •pool of virtual agents (avatars) and their respective geographical origins (such as IP addresses) that are used to access the content on behalf of the customer •Browser-based and API-based crawling engines •Automatic bypass of CAPTCHAs
1.9	Solution allows parameters for each query to be unique	Comply	The user can define various parameters for each query. In addition the user can store a query and provide it a unique name for later use.
1.10	Solution shall have the ability to account for common misspellings of target search terms, as well as synonyms, related words, slang, synonyms, stemming, etc.	Comply	The solution textual analysis capabilities will account for common misspellings of the user search terms, as well as synonyms, related words, slang, lemmatization, etc.
1.11	Solution shall make use of machine learning and natural language processing to determine sentiment, hostile verbiage, slang, etc.	Comply	The solution has a built-in machine learning engine that is used to classify documents based on their sentiment and based on their subject , the customer can train the engine to meet specific business requirements or specific content requirements
1.12	Solution shall be able to filter queried content by the following parameters set by the end user: English Language Only, Re-Tweets vs. No Re-Tweets, Content with Pictures Only, Content with	Comply	The end user can filter the query content by various filters including but not limited to language , content

#	Detailed Technical Collection Requirements	Compliance	Comment
	external links only, Content source, etc.		type , content origin and many others
1.13	Solution shall have the ability to display queried content in real time in one or more columns	Comply	The data is ingested in near real time to the system.
1.14	System shall provide the user the ability to be alerted when a piece of content enters the system and meets certain user defined criteria. This includes volume thresholds over certain geographic areas	Comply	The user can setup automatic alerts based on various criteria, including volume thresholds, geo-fence, keywords, and other.
1.15	Solution shall provide the ability for alerts to be customizable by the end user allowing them to choose the method of alert from among the following: Email, SMS-text message, Sound, and/or Desktop Pop-up	Comply	
1.16	Solution shall allow for the ability to add, edit, and delete parameters from any query at any time on the fly	Comply	
1.17	Solution shall provide the ability to export and import parameters for inclusion in the query via a .CSV or other common file format	Comply	Queried data can be exported via different formats; by default the raw data is exported using Zip files which include the content and meta data in an XML format, and the linked binary data as file attachments.
1.18	The solution shall provide the ability to query and save data from SSL encrypted web sites	Comply	The platform is able to query and save data from SSL encrypted web sites (html based)
1.19	Solution shall provide the ability to apply non-detectable web crawlers to query for content	Comply	The platform provides a rich set of engines and strategies for covert web data extraction, including the ability to mimic genuine user browsing patterns, emulate web browser types, using proxies and TOR to disguises the organization identity, meeting web site polices and more.
1.20	Solution shall update content in queries automatically at short regular intervals without any user interaction needed, when desired by the user	Comply	
1.21	Solution shall provide the ability to pause auto-updates when looking at specific content in more detail so as not to lose it in the stream	Comply	

#	Detailed Technical Collection Requirements	Compliance	Comment
1.22	Solution shall provide the ability for queries to return all historical content from any provider that meet the search parameters of the user	Comply	The solution queries historical content from various web providers that support this option, new queries can be defined by crawling unstructured web sites and/or by customizing a dedicated robot (web flow) by the customer or by Verint Professional services team
1.23	Solution shall not be limited in its ability to query content available from any particular open source/social media platform that is not protected by privacy settings	Comply	New queries can be defined by crawling unstructured web content and/or by customizing a dedicated robot (web flow) by the customer or by Verint Professional services team
1.24	Solution shall provide ability for users to add/customize RSS feeds that are available for querying	Comply	The platform offers RSS collection engines that transform streams of RSS links into structured web data that fit the platform data models.
1.25	Solution shall have ability to schedule queries to begin in advance including allowing users to set start and end date/time periods for data querying. This should also include ability to schedule all other features of the query including location, keywords, alerts, etc.	Comply	WebInt-Analytics is fully integrated with the collection platform. The end user can schedule queries, define the query criteria, setup thresholds and other configuration settings needed.
1.26	Solution shall have the ability for users to identify specific named users on specific websites to restrict from inclusion in the query results	Comply	
1.27	Solution shall have the ability to query content based on industry standard emoticons	Comply	
1.28	The solution shall have the ability to allow users to duplicate queries, creating a new query based on the same starting parameters	Comply	
1.29	The solution shall have the ability to query data from websites that support displaying html content	Comply	The platform supports web data extraction from virtually any HTML-based website
1.30	The solution shall have the ability to query and save all content presented in the page including but not limited to user comments and reply to a comment, attachments, etc.	Comply	
1.31	The solution shall be able to overcome challenge-response type tests from websites	Comply	The platform supplies an easy-to-define event handler to preconfigure the appropriate behavior to

#	Detailed Technical Collection Requirements	Compliance	Comment
			overcome error messages, buttons that no longer exist, CAPTCHAs, and other unexpected events
1.32	The solution shall support saving content from multiple, disparate queries running simultaneously	Comply	
1.33	The solution shall provide options for saving content in a structured format to facilitate further analysis and investigative requirements (e.g. Discovery)	Comply	The solution provides options for saving content in a structured format
1.34	The solution shall be scalable allowing for growth in queries and resultant content volume over time	Comply	<p>The platform offers a highly scalable solution, capable of adapting to changes in requirements, traffic loads, and types of engines, content coverage, storage, and more. Scalability is achieved by:</p> <ul style="list-style-type: none"> • Incorporating additional crawler units • Incorporating additional proxy machines • Incorporating additional index and ingestion servers.
1.35	The solution shall provide a secure method for saving web content on- the-fly while users are browsing the web	Comply	<p>WebInt secured browser (one of the tools that the analyst has in his arsenal) enables easy extraction of web data content on-the-fly while browsing the Web.</p> <p>The analyst has two options:</p> <ul style="list-style-type: none"> • Manually capture specific items or a whole page and report it as insights • Automatically issue a collection request for the relevant page data or the whole site using the WebInt-COLLECT platform
1.36	Solution shall allow users to create and store libraries of search terms, search parameters, query logic, query algorithms, etc. for future use and for knowledge management amongst local user community (organization)	Comply	The end users can create, update, delete taxonomies (e.g. search terms libraries) and store queries. In addition they have many tools for knowledge management including

#	Detailed Technical Collection Requirements	Compliance	Comment
			<p>annotate query data , write reports , dossier management , uploading attachments , sending message between users and other collaborative and knowledge management tools .</p>
1.37	<p>Solution shall allow for executing program languages such as C#, Java, JavaScript, .Net, Python, C++, PHP, etc. during query in order to call external services, etc.</p>	Comply	<p>The user can write scripting code (using the built-in JavaScript editor, part of the web flow studio), the web flow (robot) will later be able to execute this code enabling to run custom transformation, calling external services, etc.</p>
1.38	<p>Solution shall be able to access dark websites securely using TOR while hiding the user's IP address and identifiable information using methods such as automated proxy detention and scoring, anonymizers, and virtual identities</p>	Comply	<p>The solution support access to dark websites securely using a built-in TOR gateway while hiding the user's IP address and identifiable information</p>

3.1.1.1 Plan of Services – Collection (RFP Section 8C)

1. **Describe the technical method by which the solution will query data on the surface web, deep web, and dark web.**

Verint WebInt-COLLECT is an advanced data extraction and collection solution, capable of extracting data from vast amounts of web sites, by using one of the following techniques:

- a. **Fire hose/API:** Supports a broad range of social media channels, Twitter, YouTube, Instagram, Blog, Board, Tumblr, YikYak, Sina Weibo, VK, News, and Facebook. For sources with fire hose agreements in place (Twitter, Tumblr, and commenting platforms for blogs and websites), there is a very low latency between when the post is made and when the platform displays it. For sources with API access, there may be a short delay between when the post is made and when the platform receives it from the API
- b. **Crawlers** - This solution supports web data extraction from virtually any HTML-based Web source, including social network sites, portals, forums, blogs, news, and more. Handles simple static HTML-based sites, rich dynamic Web pages, and even password-protected and dark websites.

Deep and Dark Web Support: The platform employs various strategies and mechanisms to reach data found in Deep Web and Dark Web layers, which is much larger in scale than the “standard” Web data. Deep Web includes dynamic pages that require domain knowledge, unlinked content that is difficult to reach (for example, data secured by user-password login or access blocked by CAPTCHAS). Dark Website collection enables collecting data from the web layers that are inaccessible from regular Web browsers.

Visual Robot (Webflow) Definition: Designing web scraping projects is easy with the visual Robot (Webflow) editor. Simply load the website in the built-in Web browser and click on the content you wish to extract. The Robot (Webflow) editor contains tools that assist in developing the collection, breaking down the collection into sub-Robot (Webflows) for reuse, and simplifying data extraction patterns. This is all possible using simple point-and-click operations.

Dark Web Access: In order to collect from the Dark Web, the system accesses the sites using TOR and utilizes multiple tools to attain access to such sites:

- Pool of virtual agents and their respective geographical origins (such as IP addresses) that are used to access the content on behalf of the customer
- Browser-based and API-based crawling engines
- Automatic bypass of CAPTCHAs

All these collection strategies work while running automated engines to remain below the radar of bot detectors.

2. Please describe if and how the solution will incorporate machine learning, natural language processing, semantics, and related techniques into its query tools?

Verint WebInt enables search on all textual content in the system, including raw source content and metadata, entities' content, and vetted content such as analyst insights and summaries. Textual indexing based on Unicode allows it to support simple textual searches for all character sets, and therefore all languages.

Simple, advanced, and structured search modes offer users a series of options to combine different search criteria and filtering options across all data, ensuring that all relevant entities, patterns, or links are identified as quickly as possible.

Simple and Advanced Textual Searches - Verint WebInt provides simple and advanced search capabilities, considers all criteria, and supports Boolean search options (multiple selections, And/Or/Exclude operators), wildcards, fuzzy searches, and semantic search – all accessed through a simple search entry user interface.

Structured Guided Search - Investigators can perform structured searches based on entity types and properties.

Facet-based Discovery - Faceted navigation allows the user to refine and navigate the data collection using a set of discrete attributes such as time, activities relationships types, and websites.

Faceted navigation serves as a custom map that provides the analyst with insights into the content and its organization, and offers a variety of useful possible next steps to narrow the results to find the needle in the haystack, and understand the collected results as a whole by extracting entities from the textual content of the results, showing summarized information and charts.

WebInt Facets include advanced content-sensitive filtering mechanisms, enabling analysts to quickly search through big data amassed in the system. Using WebInt Facets, content is automatically dissected and grouped according to values repeated in the data. For example, if multiple documents contain information about countries, a 'Country' facet is automatically created and the list of countries identified in the documents will be extracted and displayed along with the number of occurrences. Facets also allow analysts to filter search results in lists created by the system.

Geospatial Searches - Users generate search criteria according to all available entity criteria, and filter results according to geographic area parameters. Each search can be run either with or without the geographic filter.

Text Analysis - Verint WebInt enables the analysis of textual data including but not limited to:

- Language Identification – Examines all text data and determines the language of the text.

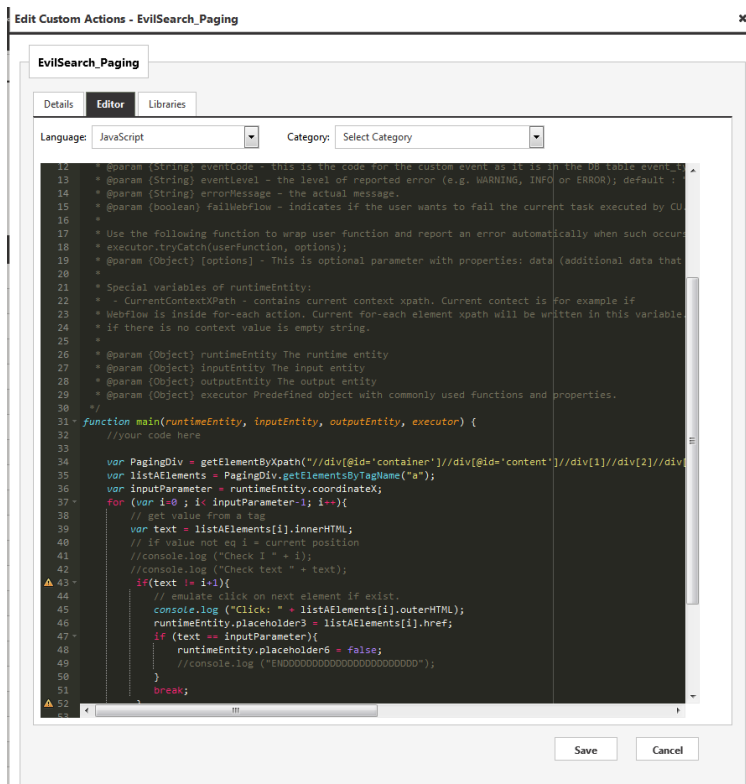
Named Entity Recognition – Every text that enters the system is scanned to identify entities such as person, organization, location, phone, number credit card, number, date, URL, time, email, number latitude/longitude, money, religion, and nationality.

3. Please describe how the solution will allow for executing programming languages to facilitate queries calling external resources?

APIs usually exist on big sites, and allow collecting a large amount of data quickly, with low web traffic and low maintenance. Web API is usually executed after authentication by sending an HTTP request to the Website asking for data, and getting a response in JSON or XML format with the requested data from the Website. Working with the website's API is more stable, as modifications in the Website GUI do not affect the collection process, and transformed data is clean without graphics or formatting. As a result, this data is less prone to change and is collected much faster than other types of data.

The end user can use scripting language to extract content from websites that support this method.

Having incorporated external data into the system, the WebInt Data Ingestion and Processing layer is responsible for converting it into a uniform structure to create analysis-ready, meaningful information. Structured and un-structured content are transformed into logical entities that offer investigation-ready meaning, such as person, event, organization, etc.



4. Please describe how the solution will handle alerting users to new content that' meets their query parameters?

The system enables users to set up and receive email and text alerts. Alert settings are defined by the user and can be based on customized keywords or when a subject makes a post, with the option to alert only when high risk keywords are used.

This enables the user to monitor subjects 24/7 as the system sends alerts as soon as it receives the post. The alert message contains the content of the post, any images contained in the post, the date and time the post was made, and street views of the location, if available. The alerts can be configured for any e-mail account or cell phone, and the recipient does not have to be a WebInt user.

Alerts and early warnings can also be generated based on customizable triggers and adjustable thresholds. Trigger scenarios can be based on suspect behavioral patterns, keyword combinations, etc.

Search based alerts - Users can prioritize specific searches and receive alerts when a predefined condition is matched and results are found. These searches can be scheduled to run periodically, based on time intervals, window of interest, time range of interest, and more.

5. Please describe the technical method by which the solution will save select data from the surface web, deep web, and dark web.

In the process of moving the collected data into WebInt-ANALYTICS, the WebInt-CONNECTIVITY LAYER cleans up the data and runs Antivirus over all incoming data files. A suspicious file will be blocked from entering the analytic system.

After the data is cleaned, the WebInt-CONNECTIVITY LAYER checks the data and removes duplications in the new data, as well as between the new data and the existing data, and merges them together.

When collecting unstructured HTML data (by the "Unstructured Collection Engine"), the system analyzes the data to identify the main body of the page and remove irrelevant content such as advertising. A method which helps the analyst in focusing on the main subject of the page and to prevent false-positive results when searching for popular words and names.

6. Please describe how the solution will ensure a secure and anonymous environment for executing queries and saving select data?

The platform provides a rich set of engines and strategies for extracting vast amounts of Web data without detection.

The Webflow (robot) defines the navigation and extraction of data. The platform then wraps the Webflow, using built-in tools with the required security, covertness, and stability to allow covert

collection. This enables the user to focus on extracting the relevant content, requiring only minimal user involvement to maintain a covert collection process. The main methods are:

- **User Behavior Emulation** - Unlike humans, automatic collection scrapers pass through all the links on route to the required information one by one, in order, with no delay. There are no “wasted” steps and no routine of steps in a loop. Humans, on the other hand, behave differently, and that difference can be utilized by website protection tools to identify and limit the automatic collection process. The platform provides easy to define, user behavior emulation, which can be defined once and then reused by any Webflow for data collection.
- **Browser Type Emulation** - The user can define what browser type and browser version should be used by the system for each specific site (e.g., Firefox, Internet Explorer, or Chrome).
- **Overcome Error Messages and CAPTCHA** - While surfing the Web, many error messages and CAPTCHA challenges may be presented to the user. The platform supplies an easy-to-define event handler to preconfigure the appropriate behavior to overcome error messages, buttons that no longer exist, CAPTCHAs, and other unexpected events. The event handler can be defined once and applied over multiple Webflows.
- **Meet Website Policy and Limitations** - Users do not have to be concerned by limitations such as geographical location, number of parallel logins for the same account, or rate limitation flows. The platform envelops the Webflow with constraints that allow the user to define the limitations to be applied on run-time; for example, select randomly available logins fit to that site, use each login no more than twice in parallel, and make sure that the website login is consistent in terms of geographic location.
- **Proxy Management** - The Proxy Management mechanism enables management of the proxy pool, checks each proxy validation, and verifies that they are used in an optimal way, adhering to security measures to stay below the radar of websites and anti-bot tools.
- **Pooling System Resources to Support Enhanced Collection Strategies** - This strategy reduces the risk of exposure and reduces the collection time. Used in parallel on multiple virtual agents and multiple different proxies, this strategy enables spreading the work between the different virtual agents (e.g., one virtual agent originated from a specific proxy collects some of the target profile posts, while another virtual agent originated from a different proxy collects some of the albums). Such a strategy reduces the blockage rate and introduces a more robust collection process.

7. *Please describe if the solution will be scalable to allow for increasing volume of content over time, particularly as queries gain complexity, and both frequency and overlap of use (simultaneous use) expand? How will the ability to save/export select content be affected?*

The platform offers a highly scalable solution, capable of adapting to virtually any changes in requirements, traffic loads, and types of engines, content coverage, storage, and more.

- Scalable Collection Support by adding additional crawler units – The platform automatically incorporates newly added crawlers units. Each crawler unit can run several concurrent collection tasks (e.g., crawler engines). Adding crawler units enables the support of additional collection resources.
- Scalable proxy support by adding additional proxy machines – The platform automatically incorporates newly added proxies to utilize additional IP addresses to access the data without being hit by site policies, to stay below bot radars, and to limit the exposure rate.
- Scalable proxy support by adding additional virtual agents – The platform automatically incorporates newly added virtual agents to consume more content in less time.
- Scalable ETL process by adding additional servers – To meet future needs for content analysis to highlight the changes and transform content into the customer data model, the system can scale out by incorporating additional index and ingestion servers

The system is designed for scalability. Upon request the system dimensioning can be easily scaled up, as follows:

- Additional crawler units to increase collection capacity
- Additional User licenses

Additional storage - Includes the site database and data storage. Depending on the data collection scope, this can be implemented in a single database server, or in separate databases, depending on capacity requirements.

The database servers can be configured in high availability.

3.1.2 Summary Requirement 2 – Analysis (RFP Section 7B2)

#	Detailed Technical Collection Requirements	Compliance	Comment
2.1	Solution shall have the ability to develop various threat models consisting of algorithms of keywords, Boolean operators, and weighting measures that will cause content queried by the solution to be prioritized above other content when brought to the attention of the user via the GUI	Comply	The end user can define a query using wide set of operators including: <ul style="list-style-type: none"> • Boolean search • Proximity search • Fuzzy search based on spelling variations • Spell checking and suggestions (corpus-built)
2.2	Solution shall allow for threat models to be the basis of collecting data for further evaluation, analysis, and investigation	Comply	
2.3	Ability for end users to manipulate weights and terms on threat model easily on the fly based on user roles	Comply	
2.4	Ability for users to set alerts based on threat model thresholds or terms	Comply	
2.5	Solution shall provide ability for users to perform quick and general searches of content	Comply	The solution has an advance slice & dice mechanism which includes textual searches, faceted search, geo-spatial searches and linked content searches.
2.6	Solution shall provide user interface allowing user to explore queried and saved data via filters and subqueries	Comply	
2.7	Solution shall have the ability to share content of interest with non-users of the system via email directly from the user interface	Comply	The system enables data collaboration between the users using the inbox widget and via emails that enables sharing the data to external users.
2.8	Solution shall provide the ability to view interaction between subjects in a link/network analysis chart and display in a timeline	Comply	The Visual Link Analysis (VLA) provides various ways to visualize interactions, among them a timeline and geographical view.
2.9	Solution shall include language translation service (other language to English translation)	Comply	The platform has an embedded translation service that supports various languages
2.10	Solution shall have the ability to automatically identify and extract	Comply	Collected textual content that enters

#	Detailed Technical Collection Requirements	Compliance	Comment
	well known common numerical and alphabetical structures contained in content including but not limited to phone numbers, social security numbers, URLs, emails, people, locations, addresses, license plates		the system is scanned to identify entities such as person, organization, location, phone, number credit card, number, etc.
2.11	System shall provide ability to add background meta-data to extracted entities, such as the real life name, date of birth, address, and aliases	Comply	The end user can add and view annotations (insights) which were added to the investigation data
2.12	System shall allow users to easily extract these entities from structured and unstructured content via color coding and other labeling methodologies	Comply	The system highlights in different colors identified named entities such as people names , emails, phone numbers ,etc. in addition the system annotate pieces of information which includes background meta-data that was added by the analysts
2.13	Content saved using the solution must be easily integratable into commonly available external analysis software tools. These tools shall include but not be limited to i2 Analyst Notebook, ESRI GIS solutions, Microsoft Excel, Word	Comply	The system supports exporting the collected and analyzed data using various common formats including XML, CSV and PDF. If needed, the data can be customized by the customer or by Verint to meet specific 3party import specifications
2.14	Solution shall have ability to export formatted reports for dissemination to non-users of the solution	Comply	The Solution can export data such as reports and alerts for dissemination to non-users of the solution
2.15	Solution shall allow reports to be customizable to include open source content selected by the user in the solution and/or also analytical charts and graphs created by the user in the solution	Comply	The platform supports customized reports to include open source content selected by the user , and analyzed content such as insights visual analysis maps and other snapshot of content with value to the investigation
2.16	Solution shall allow reports to be exported in PDF or Microsoft Word format	Comply	Reports can be exported in PDF format
2.17	Solution shall facilitate relationship analysis between two or more web identities showing common shared attributes between them including the use of statistical algorithms to determine relationship strength and other factors	Comply	The platform supports various analytics tools including social analysis capabilities which support graph based and statistical algorithms to determine relationship strength, detecting mediators, applying SNA algorithms such as

#	Detailed Technical Collection Requirements	Compliance	Comment
			closeness, detecting communities, finding shared attributes and more.
2.18	Solution shall support analysis of content aggregated into charts and graphs	Comply	The platform presents aggregated data using charts and graphs.
2.19	Solution shall facilitate the identification and unification of disparate online entities to present the complete picture of an individual online identity	Comply	The platform supports identification and unification of disparate online entities to present a complete picture of an individual online identity. It is done by applying entity resolution algorithms. This unification can also be done manually
2.20	The solution shall reveal data about private web-profiles from scattered public content and provide the users with insights into those virtually invisible entities	Comply	The platform has built-in tools which enable to automatically reconstruct private web-profiles from scattered public content.

3.1.2.1 Plan of Services – Analysis (RFP Section 8D)

1. ***Where does data analysis occur: Please describe the platform(s) and methodology(s) used for processing and analyzing data? Does the solution harness streaming processing and/or complex event processing to enable the analysis of data in motion; aggregation of data in memory and use of "live data marts"; hosted, virtual or local data storage and indexing, and subsequent processing by queries and analytic tools native to the solution and/or owned by the operator, etc.?***

Data processing and analysis is done on Verint WebInt – Analytics, which is specially designed to facilitate the intelligence investigators' workflow. It provides users with an extensive suite of analytical tools to visualize and analyze information from multiple angles. These include a combination of quick and easy tools for general questions, dedicated tools to drill down into investigations of relational, geospatial, statistical, and behavioral links and associations, timeline-based research, and report and summary tools to disseminate information to colleagues and other departments.

This rich combination of purpose-built tools helps users navigate the investigation. Once they find a clue or lead, users can choose from a multitude of steps using different physical, deductive, and conceptual links between types of views. This facilitates a "dialogue" between the user and the data, allowing them to simulate different investigatory options by trial-and-error, the very essence of their daily work.

- Textual Analysis - enables search on all textual content in the system, including raw source content, enriched content (such as Named entities extraction content), metadata, entities' content, and vetted content such as analyst insights and summaries. Textual indexing based on Unicode allows it to support simple textual searches for all character sets, and therefore all languages, while linguistic analysis (which is language dependent that supports stemming and synonyms expansions) enable more refined searches
- Geospatial Searches - Users generate search criteria according to all available entity criteria, and filter results according to geographic area parameters. Each search can be run either with or without the geographic filter.

Entity Resolution Analysis - The matching and fusion of content belonging to the same entity is a critical step in the creation of logical entities, so that all the information about a specific person or organization is concentrated in one unified entity.

This is achieved using structured content to automatically match fields of content from different sources and by applying algorithms that identify and act on the similarities.

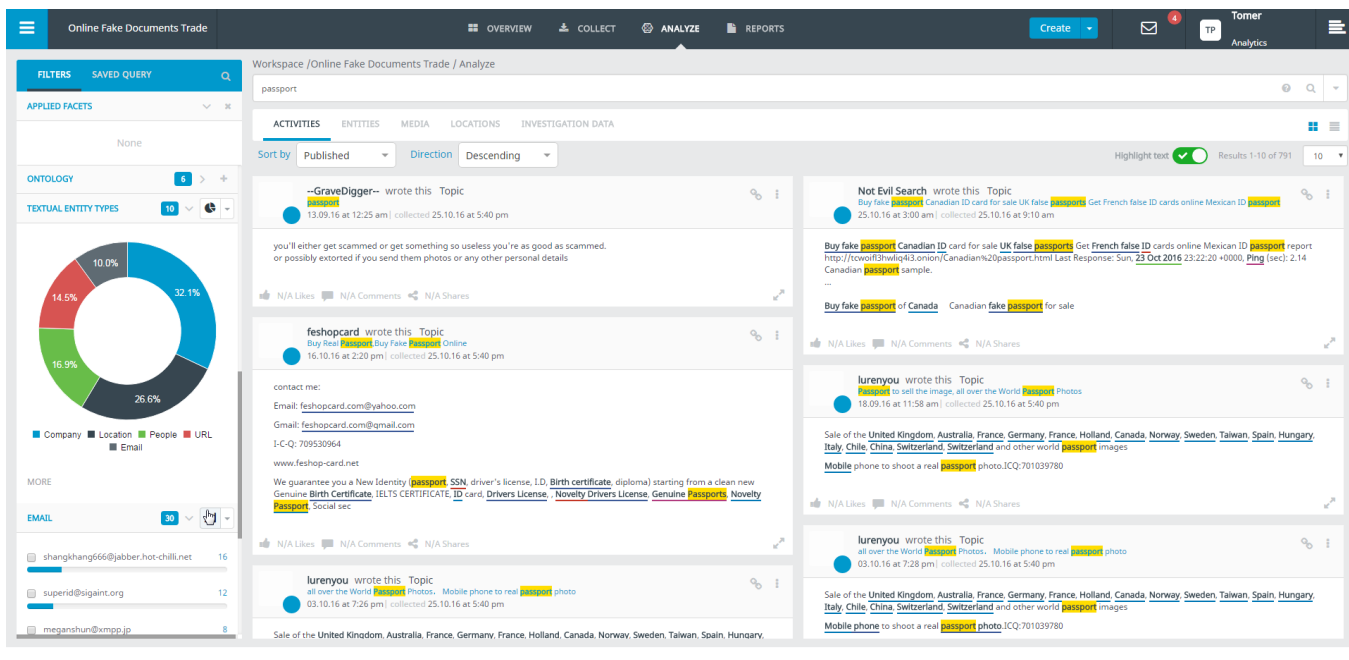
In most cases when dealing with unstructured content, manual intervention is required for accurate

entity resolution, in which case users match the entities found in the entity extraction phase to existing or newly defined entities in the system.

2. Please describe how the solution will handle entity extraction to enhance natural language processing techniques? How will the user explore and analyze those distinct entities?

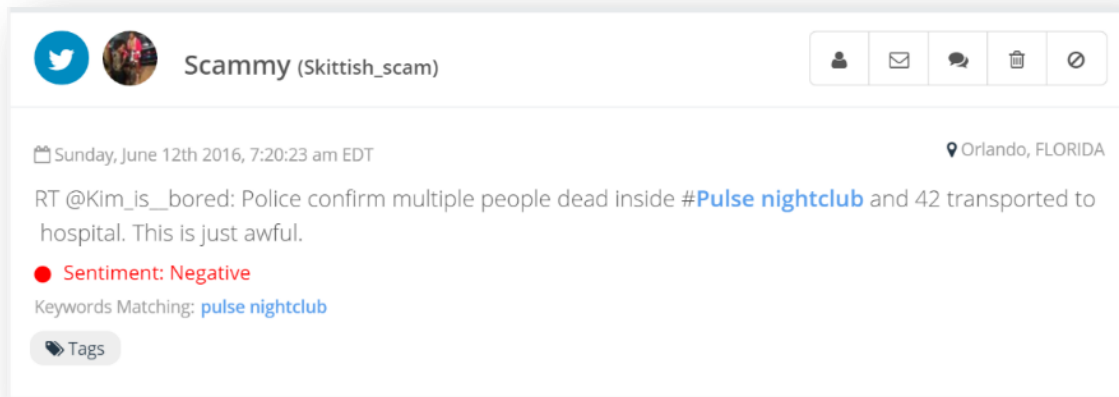
Every text entering the system is scanned to identify entities such as person, organization, location, phone, number credit card, date, URL, time, email, , religion, nationality.

When an entity is found, the system enables searching and filtering results using facets over entities and entity types, and provides an additional list of entities as found in order to summarize the text.



3. Does the solution use a lexicon-based sentiment engine? If so, what languages are included in the lexicon? Is the lexicon customizable to the user's areas of interest? Are tools provided to filter between positive and negative words in order to screen for false positives?

Each post is analyzed to determine the average sentiment and those posts that have either positive or negative sentiment and are marked accordingly (Sentiment: Positive ● or ● Sentiment: Negative). There is also a sentiment filter. Posts can also be tagged.



The platform supports sentiment analysis using a statistical classification engine, based on machine learning algorithm. A sentiment engine supports classifying the polarity (e.g. positive, negative, and neutral) for a given text at a document level and entity level.

Supported languages in WebInt:

Albanian, Arabic, Bosnian, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian, Urdu, Vietnamese.

4. Will the solution include options to seamlessly integrate COTS language translation services software?

The system parses keywords in various languages and supports multi-language searches. It also translates posts to and from various languages including Spanish, English, Portuguese, and French.

Other COTS language translation services can be integrated upon request.

5. Please describe how the solution will allow users the ability to implement and adjust a threat model for use in querying and analyzing prioritized content. Is this driven by pre-configured engineering and subsequently "tuned" by experts within the company, configured by local administrators of the solution, configured by users of the solution, some combination of the three? Please explain.

Users can prioritize specific searches and receive alerts when a predefined condition is matched and results are found. These searches can be scheduled to run periodically, based on time intervals, window of interest, time range of interest, and more.

Automated target characterization is based on the following flows and mechanisms:

- **Web Profile Recommendation and Unification**

Correlation of several web profiles to automatically generate proposed users for a defined entity. This helps analysts identify additional users in different websites that are used by the same entity.

- **Rule-Based Behavior Alerts**

When investigating website activity or user forums, behavior patterns are significantly more important than the simple content of a post or communication. The greater interest is in the user actions, such as which URL was mentioned by multiple web accounts or, which mediator was found. Additional alerts can be added per customer request by Verint professional services.

- **Historical Data Characterization**

Verint Webint-Analytics can download not only the current activity of the target, but also retrieve his historical data. In fact, Collection web flow can be run on a target's historical actions at any time, without any requirements for special warrants. As a result, alerts are displayed regarding actions of interest or suspicious behaviors performed by the target in the months preceding the definition of the user as a target. Rules run on historical data can reveal not only retrospective alerts, but also expose patterns of behavior, routines, or breaks in routine that can be extremely useful.

- **Continuous Website Monitoring**

Verint Webint-Analytics continuously accesses defined websites and newly added sites/user forums to monitor them for newly added activity, recently confirmed users and new user forums.

6. *Please describe the embedded visual data analysis features of the proposed solution, to include link/network charts, timelines, trend analyzers, graphs, etc. and the interaction between such analytic tools and both historic and live content.*

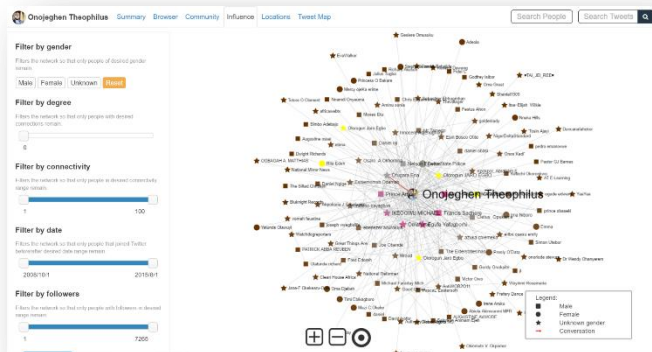
The system enables users to view a person's associated sub-groups and then drill-down to see the details for a connection. Web Alert identifies different sub-groups that are more closely connected within the subject's social network. Many factors are taken into account including location, topics of interest, followers, and so on. All members of a sub-group are assigned the same color.

These groupings can represent nodes/people with similarities, for example, gangs, friends, family, colleagues, and teammates. This saves hundreds of hours of work by uncovering valuable intelligence about the relationships within a target group. The primary node within a group is also identified with a

larger circle to help visualize who is important within the network. It is also possible to view the locations for the user's associates.



An influence graph displays the sphere of influence visualized in a concentric layout around the subject. It represents the strength of connections between all the members of the network, as they interact with the Subject. This is measured by calculating the number of links for each node of the graph. Each node's connectivity is highlighted by three features: size, color and distance from the subject of the node.

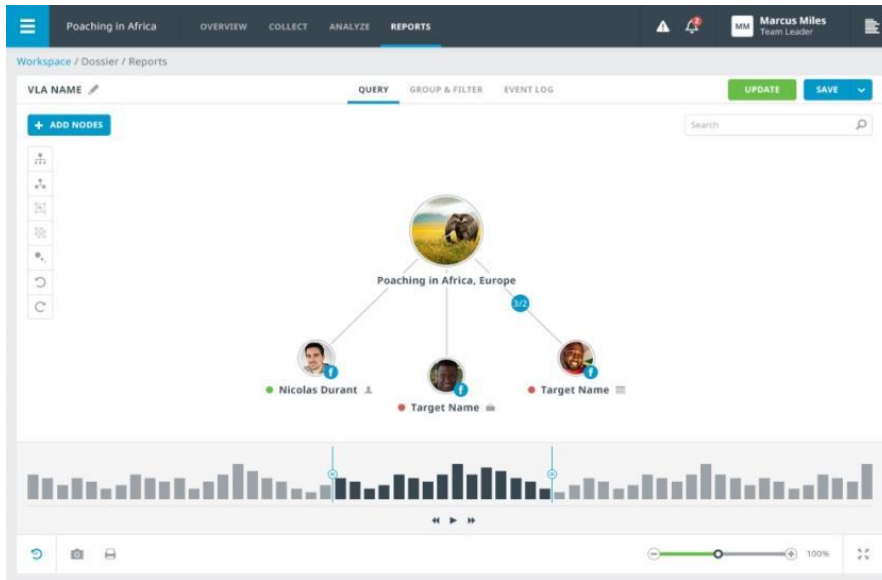


7. Please describe how the solution facilitates relationship analysis between two or more web identities showing common shared attributes, as well as communication frequencies between them.

Verint WebInt incorporates powerful Visual Link Analysis (VLA) capabilities, which provide a visual display of an entity's network of relations and associations.

The VLA visualizes the entity’s relationships and links, frequency, and types of association. It also indicates derived relations, such as which criminal groups they are associated with, and so on.

Relations may consist of human relationships, participation in events, communication links, derived connections and more. Investigators can also identify connections between seemingly independent entities, for example, two people may have a common contact that mediates between them.



8. ***Please describe if and how the solution categorizes web entities according to types, based on their activity, the attention their comments received, their number of followers and the number they follow, among other factors.***

The solution is categorizing web entities based on their properties, activities, relations and based on influence on a given set. For example the system characterizes Web entities using social network algorithms such as centrality and closeness.

One of the other methods supported by the system is categorization based on ranking; for example, the system supports ranking Web entities based on content they generated and based on other properties the Web entities support.

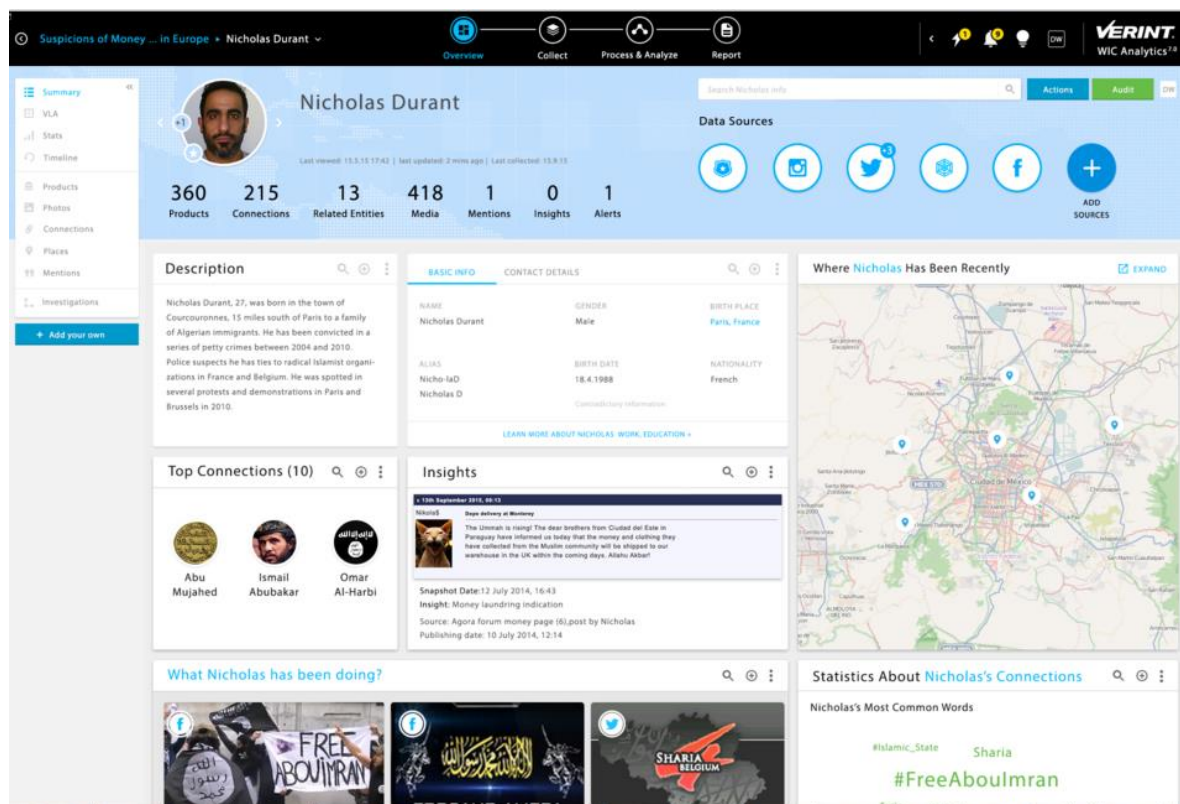
9. ***How will the solution facilitate the identification and unification of disparate online entities, presenting the user with a complete picture of the identity?***

Using WebInt-ANALYTICS, the analyst can consolidate web accounts that belong to the same target (person, organization, etc.) to get a comprehensive picture of that target's online presence.

There are two analytical options for unifying web accounts to targets: manually selecting the web accounts to be unified or using our proprietary recommendation engine.

By transferring the focus of the investigation from the identifiers to the entity, the analyst gains greater clarity and simplifies his investigation. Although this process is seemingly simple in the above example, relating multiple identifiers to their entities when investigating hundreds of identifiers may prove to be virtually impossible without advanced automatic tools.

The Target Information tab provides all the extracted and stored details about the Target, along with links to all raw data displayed in this tab. It also provides a statistics analysis of the target's web activities, including a list of usernames, social alerts, recent activities, main interests, and a graphic breakdown of his web activities and usernames.



10. In what file formats can the solution import/export content for use within 3rd party COTs analytic solutions?

Export

Data collected from the WebInt-COLLECT can be distributed to WebInt-ANALYTICS, as well as to any other external information system, after appropriate authentication.

The WebInt-CONNECTIVITY LAYER distributes the collected data in XML format. The typical distribution is performed by copying a zip file to the customer directory, but it also can be distributed using other methods, as agreed with the customer.

Import

Raw Data can be imported to the system using an XML files or other methods, as agreed with the customer.

The WebInt-CONNECTIVITY LAYER functions as a security separation level between the external side of the system that is connected to the web, and the internal part that contains knowledge and insights.

In the process of moving the collected data into WebInt-ANALYTICS, the WebInt-CONNECTIVITY LAYER cleans up the data and runs Antivirus over all incoming data files. A suspicious file will be blocked from entering the analytic system.

After the data is cleaned, the WebInt-CONNECTIVITY LAYER checks the data and removes duplications in the new data, as well as between the new data and the existing data, and merges them together.


11. Please describe the capabilities of the solution involved in producing information products and reports for export to non-users of the system?

Verint WebInt - Analytics, summarized and analyzed Intelligence is easily reportable. With an automatic report generator; the analyst can generate summary reports on cases, target entities and web accounts monitored. The reports include a wide variety of details, such as geo-data, link-analysis maps, statistics about the target's activities and much more. These reports draw their information from Verint WebInt's databases and analyzed data, and present them in a highly understandable format which any Intelligence client can easily work with. The reports also allow quick and easy editing by the analyst, which may add his own analysis and edit automatically generated content according to his needs.


Niger Delta Avengers (NDA) OVERVIEW > COLLECT > ENGAGE > ANALYZE > REPORTS Create Administrator Almighty Latin K...

EDITOR EVENT LOG ARCHIVE Save

File Edit Insert View Format Table Tools




The **Niger Delta Avengers (NDA)** are a militant group in Nigeria's Niger Delta. The group publicly announced their existence in March 2016.^[1] The NDA have attacked oil producing facilities in the delta, causing the shutdown of oil terminals and a fall in Nigeria's oil prooil producer.^[2] The NDA's declared aims are to create a sovereign state in the Niger Delta and have threatened to disrupt Nigeria's economy at Europe³. The group have criticised the President of Nigeria, Muhammadu Buhari, for having never visited the delta and his detention of the I




INSIGHTS SNAPSHOTS

SEARCH INSIGHTS


Niger Delta Avengers 'Chief' Arrested
By Administrator | 09 Jun 2016
Niger Delta Avengers 'Chief' Arrested As Navy Captures Militant Who Killed four Troopers



Nigerian Army has arrested 10 suspected members
By Administrator | 09 Jun 2016
The Nigerian Army has arrested 10 suspected members of the militant group, Niger Delta Avengers. It said that the suspects were arrested at about 1:40 AM on Saturday in Oporaza community, Warri South-West Local Government Area of Delta State.



Is Tompolo supporting the NDA ?
By Administrator | 09 Jun 2016
As believe that that might be a connection between Tompolo and NDA, we continue to investigate this assumption



div Words: 704

3.1.3 Summary Requirement 3 – Investigative (RFP Section 7B3)

#	Detailed Technical Collection Requirements	Compliance	Comment
3.1	Ability to preserve content in its entirety for evidentiary purposes	Comply	The platform preserves content in its entirety for evidentiary purposes
3.2	Ability to link/jump back to original source website of the document	Comply	The user can ask the system to navigate to the original content that was collected
3.3	Solution shall provide the ability to maintain user defined containers to organize and manage different investigations	Comply	Investigations are managed as a multi-resource work environment, with access permissions, raw and vetted content, such dossiers , analysts' insights, saved searches, link analysis maps, ,attachments and reports
3.4	Solution shall allow users to link queries to case containers	Comply	The platform allows end users to link queries to the case (a case container)
3.5	The solution shall have the ability for users to share cases with all or specified users	Comply	The platform support sharing cases between users and group of users
3.6	The Solution shall have the ability for users to add metadata to the case	Comply	The end users can add metadata to cases via the insight mechanism
3.7	A simple user interface shall be provided to create, edit, manage and access these case containers	Comply	
3.8	System shall allow users to attach files to a case	Comply	The end users can attached files to a case
3.9	Users should have the ability to duplicate cases and create new cases based on the same starting parameters	Comply	The end user can duplicate existing cases. The user can later modify the starting parameters to meet the new investigation agenda.
3.10	Solution shall support the creation and management of virtual identifies	Comply	In order to access restricted web content (e.g. websites that require login), the platform maintains a managed virtual agent pool. The system verifies that each virtual agent is assigned with a preferred IP address; verify that the virtual identity is being used according to

#	Detailed Technical Collection Requirements	Compliance	Comment
			the policy of the targeted web source and more.
3.11	Virtual Identity configuration supports a minimum of login, password, proxy, and description settings	Comply	The platform supports managing virtual identities. The administrator can configure the Virtual Identity password, proxy, description and other settings
3.12	The creation of virtual identities shall be managed via role based access controls	Comply	
3.13	Virtual Identities shall be able to be used to query and save content for investigative purposes	Comply	
3.14	Solution shall support the duplication of virtual identities	Comply	The solution enables comprehensive virtual identities management including the ability to duplicate virtual identities
3.15	The solution should include a secured browser as a complementary tool that enables the user to interact with online content using virtual identities	Comply	The platform support a secured browser add-on as a complementary tool that enables the user to interact with online content using virtual identities while supporting secured browsing capabilities
3.16	The secured browser ensures the protection of the local network from malicious code (cyber security threats) and allows for anonymous browsing	Comply	The platform secured browser ensures the protection of the local network from malicious code by applying threat protecting and firewall configuration , along with using proxies and applying strict web-browser browsing policies that enhance anonymous browsing
3.17	The secured browser is able to access the web using IP addresses designated for specific virtual identities	Comply	The platform secured browser support access the web using IP addresses designated for specific virtual identities
3.18	The solution shall provide visual analytic tools to aid investigators, to include, but not limited to, link analysis, geospatial, and timeline tools	Comply	The system supports visual analytic tools which includes link analysis , geospatial , charts and timeline tools
3.19	The solution shall provide a secure means for local system audits of its investigative components	Comply	

3.1.3.1 Plan of Services – Investigative (RFP Section 8E)

1. Please describe how the solution will handle the concept of a "case file"?

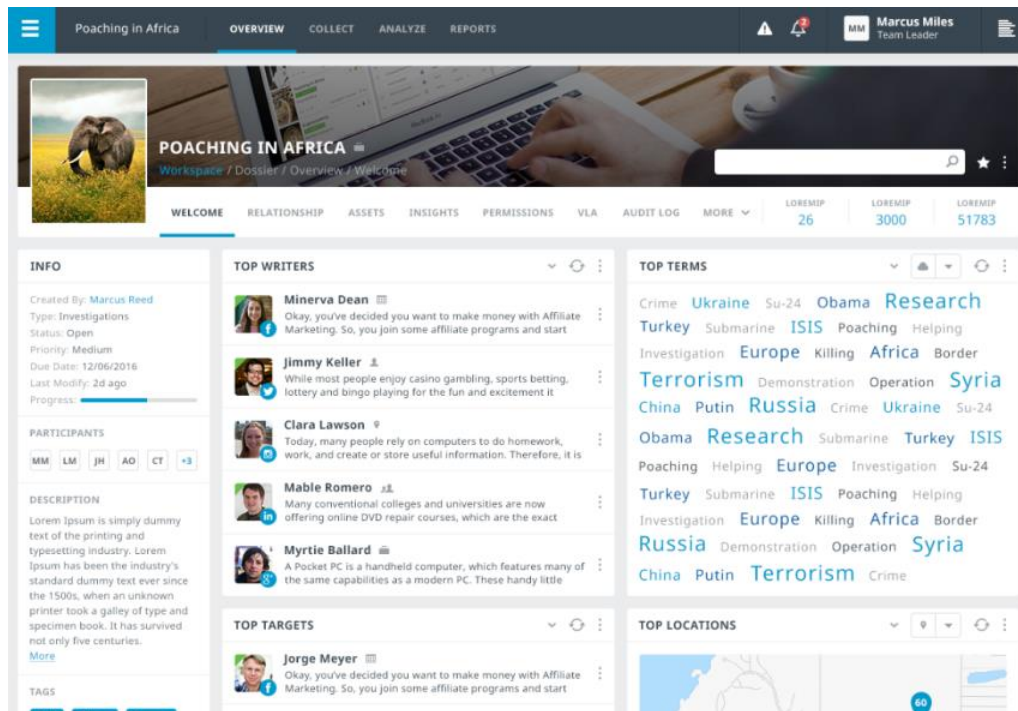
The case (Investigation) framework is where investigations begin and where analysts are expected to provide the answers, using the power and functionality of the WebInt. As such it is where analysts use all the resources and tools made available to them to gain the intelligence leads they need and fulfill their tasks.

Cases (Investigations) in WebInt are managed as a multi-resource work environment, with its own internal world of personnel (assigned analysts, data managers, etc.), access permissions, raw and vetted content, and analysts' insights. The system has been set up to support the investigative and knowledge needs of each case as a discrete 'universe' without compromising the security and intelligence needs of other cases.

Investigation progress reports allow senior analysts and/or administrators to track the progress and status of ongoing cases.

Verint WebInt presents the investigator with a dashboard that displays the case (investigation) highlights focusing attention on recent activities of suspects, news updates, content highlights, recent searches, results of interest, alerts noted, and any recent inputs, analyst summaries, or leads provided.

As an investigator starts a new shift they can quickly identify recently added inputs, alerts of interest, insights made by colleagues, or awaited breakthroughs. The dashboard displays multiple widgets for presenting these summaries.



WebInt-ANALYTICS Case Dashboard

2. Please describe how the solution facilitates the retention of content for evidentiary purposes?

The WebInt dedicated and secured browser is a complementary tool that enables the analyst to conduct online operations using a crafted virtual entity.

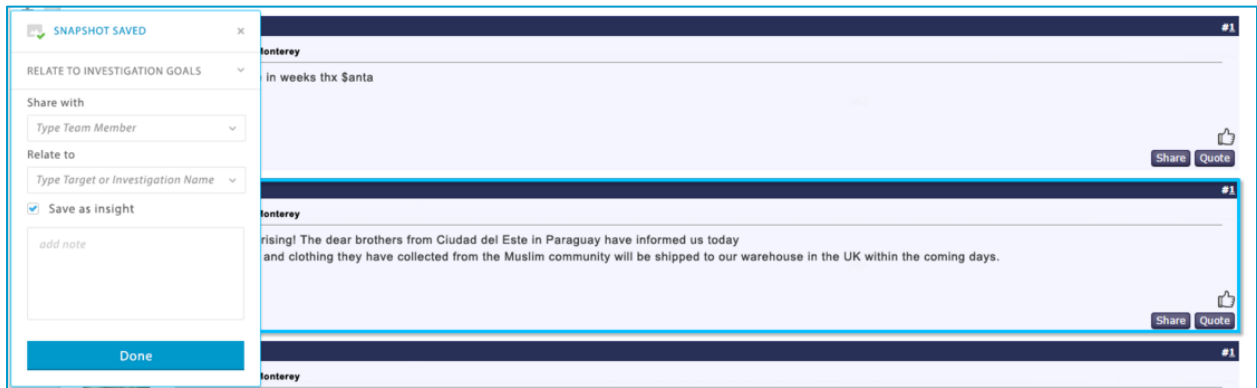
The secured browser comes with various investigative tools that enable to conduct online investigation and special operations.

The WebInt secured browser technically ensures that online browsing is secure and anonymous, taking a holistic approach that enables the analyst to focus on the content while securing the investigation aims.

Extracting Content While Browsing

The WebInt secured browser enables easy extraction of web data content on-the-fly while browsing the Web.

The analyst can manually capture specific items or a whole page and report it as insights. The insight is kept as retained for evidentiary purposes.



Secured Manual Extract Web Content

3. Please describe how the solution will facilitate the maintenance of virtual identities?

Virtual Agent

In order to access restricted web content (e.g., websites that require login), the system maintains a managed virtual agent pool. The virtual pool maintains the virtual agent’s identifiers: user name, password, and IP address for use with the virtual agent.

	Name	Password	Consumer Name	Web Platform	Status	Status change date	Network Strategy
1	breda.graja	mishuta27	System Default Cons	instagram	OK	2015-11-06T18:13:07	Proxiera
2	Ron.Levin7	RonLevin123	System Default Cons	instagram	OK	2015-11-06T18:11:45	Direct ip
3	justin.swift860@gme	justinswift860	System Default Cons	fb2	OK	2015-11-06T18:13:28	TOR
4	justin.swift860@gme	justinswift860	System Default Cons	FBMergeWP	OK	2015-11-06T18:14:03	Specific Proxy
5	va1many	123	System Default Cons	mymanywf	OK	2015-11-05T18:57:14	Direct ip
6	mymany	1	System Default Cons	mymanywf	OK	2015-11-05T18:57:22	Direct ip

Virtual Agent Management

Avatar Management

A virtual entity is a fictitious entity (an online presence of a person) that is crafted to meet the investigation goals, using the virtual entity (avatar) the analyst can extract valuable content without compromising the investigation goals. The WebInt secured browser enables the analyst to manage

multiple crafted virtual entities over several investigations, multiple web-arenas and long periods of time.

The analyst can select which virtual entity will be used to surf the Web. The analyst can review the virtual entity detailed avatar card, learn about the avatar cover story, review its history, and more, when needed, the analyst can seamlessly switch between avatars to meet the investigation objectives.

The secured browser ensures that the investigation is secure and anonymous by running the following security checks and locking procedures:

- Accessing the web using the avatar originating country IP address
- Emulating a browser configuration which meet the cover story of the avatar
- Verifying that the virtual entity will not be used concurrently

4. *Please describe how the solution will ensure these virtual identities are managed securely and anonymously?*

To ensure these virtual identities are managed securely and anonymously the following security checks and locking procedures are done:

- Accessing the web using the avatar originating country IP address
- Emulating a browser configuration which meet the cover story of the avatar
- Verifying that the virtual entity will not be used concurrently

5. *How will the solution facilitate security and anonymity for accessing, browsing, analyzing and investigating content within the Dark Web?*

The platform provides a rich set of engines and strategies for extracting vast amounts of Web data without detection.

The Webflow (robot) defines the navigation and extraction of data. The platform then wraps the Webflow, using built-in tools with the required security, covertness, and stability to allow covert collection. This enables the user to focus on extracting the relevant content, requiring only minimal user involvement to maintain a covert collection process.

User Behavior Emulation - Unlike humans, automatic collection scrapers pass through all the links on route to the required information one by one, in order, with no delay. There are no “wasted” steps and no routine of steps in a loop. Humans, on the other hand, behave differently, and that difference can be utilized by website protection tools to identify and limit the automatic collection process. The platform provides easy to define, user behavior emulation, which can be defined once and then reused by any Webflow for data collection.

Browser Type Emulation - The user can define what browser type and browser version should be used by the system for each specific site (e.g., Firefox, Internet Explorer, or Chrome).

Overcome Error Messages and CAPTCHA - While surfing the Web, many error messages and CAPTCHA challenges (scribble letters the user needs to identify) may be presented to the user. While a human user easily manages to overcome the Web server errors and CAPTCHAs, automatic collection machines tend to get stuck on those unexpected events.

The platform supplies an easy-to-define event handler to preconfigure the appropriate behavior to overcome error messages, buttons that no longer exist, CAPTCHAs, and other unexpected events. The event handler can be defined once and applied over multiple Webflows.

Meet Website Policy and Limitations - Users do not have to be concerned by limitations such as geographical location, number of parallel logins for the same account, or rate limitation flows. The platform envelops the Webflow with constraints that allow the user to define the limitations to be applied on run-time; for example, select randomly available logins fit to that site, use each login no more than twice in parallel, and make sure that the website login is consistent in terms of geographic location.

Web Strategy - When defining a collection task using an existing Webflow, the user can define what web strategy to use to meet the specific needs of the collection task. That Webflow can be freely switched between web surfing strategies as needed.

- Proxy - is a built-in mechanism used to hide the customer IP address. Proxies can be installed on any cloud service like Amazon Web Services.
- TOR is a system that directs internet traffic through a worldwide volunteer network of servers. To enable anonymity while surfing, TOR hides the collection system and enables it to access websites available only through TOR (parts of the Dark web). To get the Webflow to work through TOR, the user needs only to define the network strategy.

3.1.4 Summary Requirement 4 – Geospatial (RFP Section 7B4)

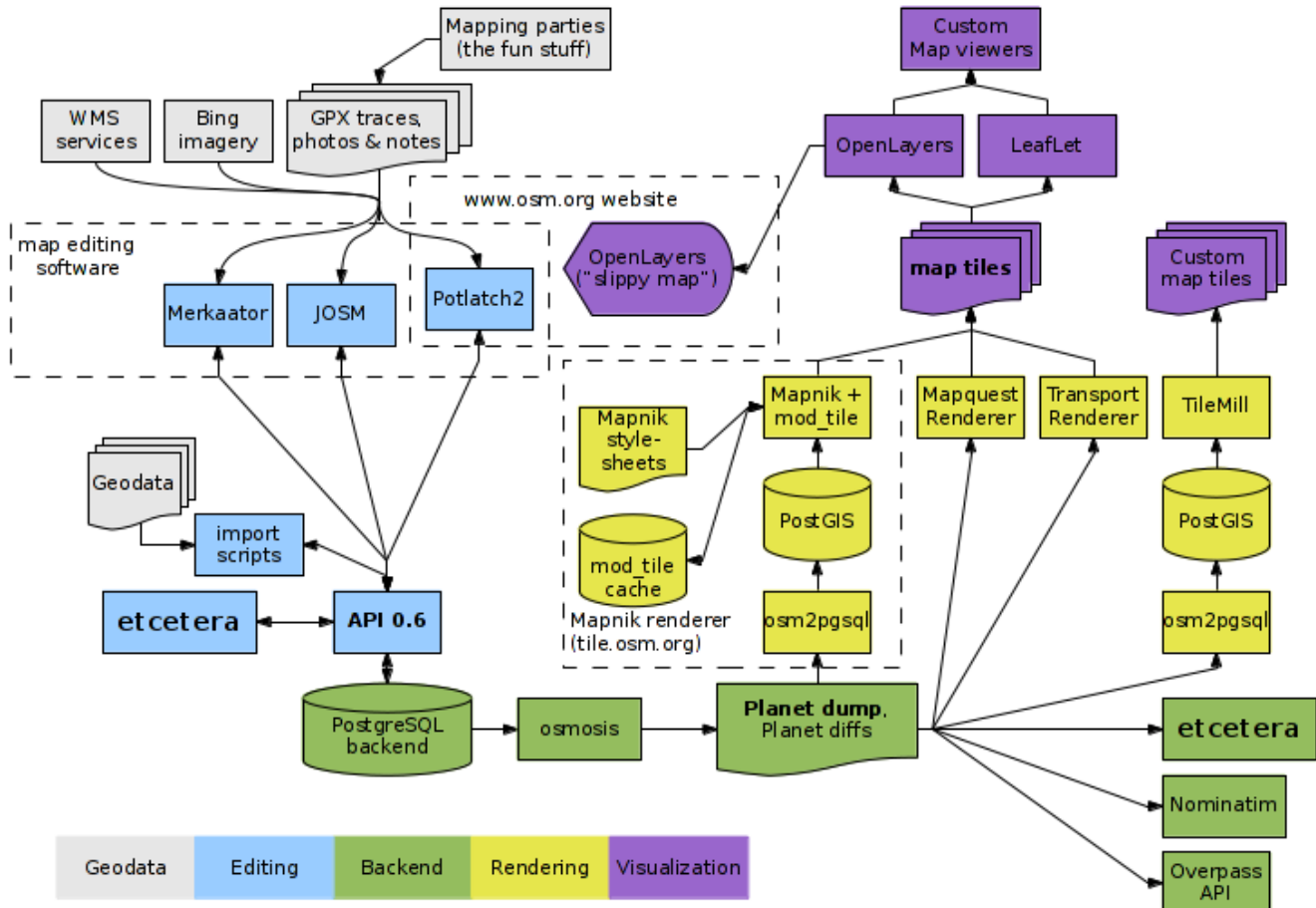
#	Detailed Technical Collection Requirements	Compliance	Comment
4.1	Ability to query, view and/or save geo-tagged content on a map in near real time	Comply	The platform supports querying, viewing and saving geo-tagged content on a map in near real time
4.2	Ability to query, view and/or save geo-inferenced content on a map in near real time	Comply	The platform supports querying, viewing and saving geo-inferred content on a map in near real time
4.3	Ability for end users to apply a geo-fence to an area and display a stream of content from that point forward	Comply	The end users can define various queries criteria. For example, the user can define a query criteria that include a geo-fence and list of monitored web sources (e.g. twitter, Instagram, etc.)
4.4	Solution shall have the ability to query historic content within a geo- fenced area	Comply	
4.5	Ability for users to select the time period for which geo-tagged content appears on the map	Comply	
4.6	Solution shall have the ability to turn view geo-tagged data, geo-inferenced data, or both on the map based on a user's selection	Comply	
4.7	Ability to apply all of the solutions inherent search capabilities geospatially	Comply	The platform supports various data discovery capabilities among them geo spatially capabilities which enable to narrow down the results to specific geo location or geo areas , cluster results ,etc.
4.8	Solution shall have the ability to display geo-tagged or geo-inferenced content from one or more stored queries on a single, continually updating map interface	Comply	
4.9	Solution shall have the ability to view an image of the actual address where the content was posted from and the street view of the actual location where available via commercially available street level imagery (for example, Google Street View)	Comply	Done using Google Street View integration
4.10	Solution shall have the ability for users to geo-fence an area and receive alerts when new posts occur within that area that meet specified search criteria	Comply	

#	Detailed Technical Collection Requirements	Compliance	Comment
4.11	Geospatial content collected and stored using the solution must be easily integratable into ESRI GIS solutions	Comply	The solution can be customized to be integrated with ESRI GIS based solutions allowing to share geo-tagged and inferred geo content to ESRI GIS based solutions
4.12	Ability to create heat maps relative to density of geo-tagged and geo- inferred data, to include various search/query logic/algorithms	Comply	
4.13	Ability to conduct geospatial analysis functionalities, such as temporal and cluster analyses	Comply	The platform supports geospatial analysis capabilities such as cluster analysis, geo-fencing, geo-coder and other tools to support analysis of tagged geo data and inferred geo originated content

3.1.4.1 Plan of Services – Geo Spatial (RFP Section 8F)

1. What GIS basemap vendor(s) will the geospatial pieces of the solution use?

The GIS basemap is OSM (OpenStreetMap). It includes worldwide maps.



Database

The database holds all the map data in the form of nodes, relations, and ways. The database software used is **PostgreSQL**

Tiles and tile rendering

Mapnik is the rendering system which powers the display. The rendering process runs on the 'tile' server, and Mapnik tile images are served from that machine. This renderer takes its data from a postgres database (also on the tile server).

Geo-coder

Nominatim (from the Latin, 'by name') is the geo-coder to search the data by name and by address and to generate synthetic addresses of OSM points (geo coding and reverse geocoding).

Frontend

Is powered by **Leaflet**, a JavaScript library which is designed with *simplicity, performance* and *usability* in mind. It works efficiently across all major desktop and mobile platforms.

- 2. Please describe how the solution will facilitate the import and export of geospatially enabled data sets for re-use in other GIS software currently in use at the BPD/BRIC? Can BPD/BRIC managed data layers be imported into the system for geo-referencing and additional geospatial analysis capabilities?***

The GIS capabilities of the system are currently supported by OSM (open street map). As we understand it, ESRI has several tools that support such integration. Among them are tools such as “ArcGIS Editor” which enables the user to import ESRI data to an OSM format. Another available tool is “OSM Loader” a tool used to import OSM data to ArcGIS.

- 3. Please describe how the system will handle the geo-inferencing process for content? How does it visually differentiate between geo-inferenced and geo- located content?***

Verint WebInt includes GIS capability so that all geo-tagged entities are represented on the map, and manipulations to data (such as filtering) are synchronized in real-time with the active map display.

Geo-inferenced and geo- located content are presented on the maps in different colors.

All location information is merged into a uniform geographic system by geocoding. The same geocoding process is applied when users search the system, so they can search for a street address or postal code and the search process automatically translates these into searchable coordinates.

Verint WebInt offers various geospatial analysis tools. Geographical display enables investigators to view events, activities and data on the map, related information, such as type and time of event, is displayed to give users a complete intelligence picture. Geospatial display depicts the routes and routines of suspect entities to reveal location links between suspects or links to crimes or events that have taken place.

3.1.5 Summary Requirement 5 – Administrative (RFP Section 7B5)

#	Detailed Technical Collection Requirements	Compliance	Comment
5.1	Solution shall provide an easy to use, intuitive GUI that is operational with minimal end user training	Comply	The platform use an intuitive GUI that was design by analysts to serve analysts
5.2	Administrators should be able to add, edit, and maintain user accounts without interaction needed with the proposer	Comply	
5.3	Administrators shall have access to an interface that facilitates data review, retention, and purge procedures to ensure .compliance with regulations such as 28 CFR Part 23 and other applicable laws, policies and procedures	Comply	Specific to 28 CRF Part 23, the proposed solution allows compliance to which adherence to the policy is generally up to the end user and the use case. Should future or other related laws, policies or procedures not identified cause required changes to the product, the parties will negotiate in good faith how these costs will be borne
5.4	Solution shall produce an audit log that tracks system use by individual users	Comply	The platform logs and stores each and every data access, search, investigation and analysis action performed by all users. Auditing allows the tracking of data usage – this is not limited only to actions of a specific user but also enables general tracking of how a data item has been used, by whom and for what purposes.
5.5	Administrators shall have access to audit logs	Comply	
5.6	Solution shall have role-based access controls to distinguish user permissions across all components of the solution	Comply	The platform supports strict yet adaptable control of data access management including the following range of security mechanisms: Content access control – Data is controlled by user access permissions ensuring each item is accessed by authorized users only. User level permissions – User permissions determine which data items each user can access, and for

#	Detailed Technical Collection Requirements	Compliance	Comment
			what purposes
5.7	Solution shall have option to integrate with host's Active Directory to facilitate user authentication procedures	Comply	The platform can be integrated with the customer active directory to facilitate user authentication procedures
5.8	Solution shall have an Administrative interface that allows for oversight of all collection activities	Comply	The platform offers centralized command and control capabilities that enable monitoring of all collection activities
5.9	Solution shall have an Administrative interface that allows for monitoring of system performance and alerts administrator of system errors or downtime	Comply	The platform have a back office and dashboards interface which allows to monitor the system performance and configure and view alerts , the back office is accessed via role based permission allowing authorized users to monitor and control the system
5.10	End-user Solution shall be clientless web-based system accessible via web browser from any workstation on the department network (or designated secure networks)	Comply	
5.11	Proposer will provide training on all components of the solution for all levels of users (e.g. basic, standard, advanced, administrator, etc.)	Comply	Verint offers tool based methodology and technology training. Consultancy services are available at the time of system setup, or later on for advanced users.

3.1.5.1 Plan of Services – Administrative (RFP Section 8G)

1. Please describe the capabilities the solution will provide to facilitate the retention management process for saved content?

The collected data is stored in the system and is managed in FIFO based manner.

The user can retain specific data and to be kept and not be removed in the cyclical deletion process.

User inputs are not part of the cyclical deletion process and are kept in the system database.

2. What types of user authentication mechanisms will the solution support?

Different authentication sources can be implemented, including integration of enterprise LDAP. Organizations can retain existing enterprise authentication systems or implement Verint WebInt's own authentication system.

Verint WebInt authentication is based on username/password. Interface between the user client and the administration layer is secured.

3. How does the solution handle role-based access controls?

Verint WebInt provides a strict yet adaptable control of data access management, user data access and auditing of user actions.

Verint WebInt offers the following range of security mechanisms:

- **Content access control** – Data is controlled by user access permissions ensuring that the items are accessed by authorized users only. WebInt
- **User level permissions** – User permissions determine which data items each user can access, and for what purposes (read/write).

The WebInt active security mechanism uses a unique query-time join technique that binds security permissions during the initial retrieval action, which results in high flexibility for permission changes and no risk of retrieving unauthorized content.

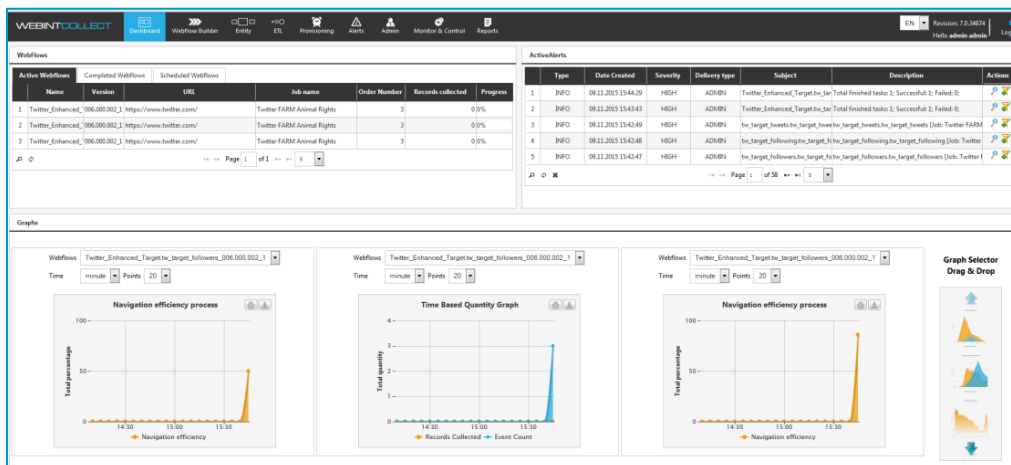
4. What audit mechanisms exist and how are they used by administrators?

The system logs and stores investigation and analysis actions performed by all users. Auditing allows the tracking of data usage – this is not limited only to actions of a specific user but also enables general tracking of how a data item has been used, by whom and for what purposes.

5. What tools are included to alert administrators to system errors, failures, etc. and to monitor system performance?

The platform supports a monitoring dashboard that enables users to view the existing Webflows, set schedules for running, view historical runs and running errors, and monitor the outcome of the collected data. The dashboard provides a graphic display of the operational status of all the system's Webflows and servers, allowing quick monitoring and troubleshooting to ensure system functionality around the clock, and to prevent unnecessary breakdowns.

A preset selection of options provides the monitoring options required for the system. In addition, a graph selection pane allows users to drag and drop new graphs or monitored controls onto the dashboard to meet any ad hoc monitoring needs:



Crawler Monitors - The crawler monitors indicate which crawlers are overloaded or have malfunctioned. A built-in mechanism performs validity checks on the site, checking to what extent the site responds to the crawl, to ensure that the crawler adjusts its activity and to avoid overloading the site. Depending on the scenario, the system might be able to adjust automatically; otherwise an administrator must make the adjustment.

Collection reports - Collection reports display the information over the Webflow history – how many times the crawler ran, what problems were detected during operation, what was collected, and so on.

The report also displays Webflow performance characteristics and proxy performance, to learn about bandwidth consumption, blockages, etc.

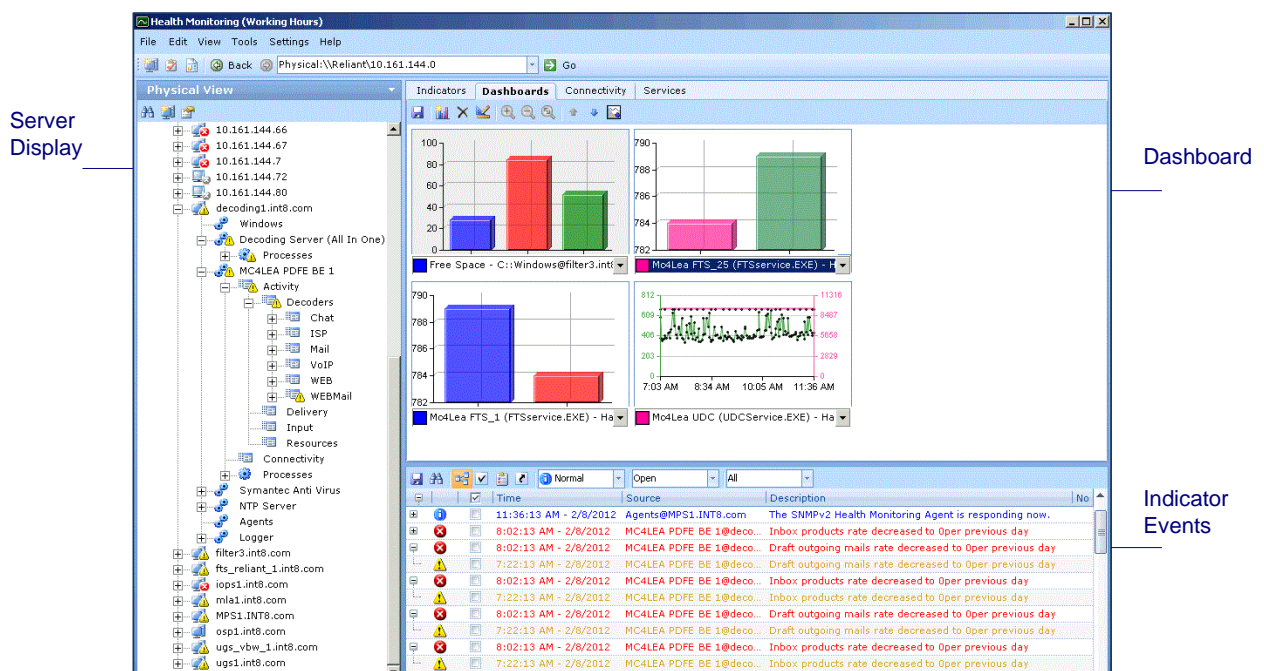
System components monitoring -

The Health Monitor (HM) enables the customer to monitor the system components and functionality from one centralized intuitive interface, eliminating the need to separately monitor the status of each subsystem. With the HM, the customer is empowered to quickly respond and prevent potential problems. Operators can view the physical status of all elements, general information such as free storage, CPU usage, as well as the status of the system logical functionality (such as number of collection tasks executing, number of collection tasks ended, etc.).

Alarms and events are triggered based on user-defined thresholds and are accompanied by detailed troubleshooting information, instructive system failure notifications, and a range of tools that enable efficient and immediate failure management.

The system's HM offering enables only authorized personnel access to the display, reports and status monitoring tools. In addition, access to the HM is protected by user names and passwords. A smart password-handling mechanism is deployed, offering tight control over user passwords. Specific user privileges are defined and assigned to each user once granted access by the administrator.

The HM dashboard shown in the figure below provides a graphical display of the system's status. It includes the status of all the system's hardware, software, and vital processes. The HM dashboard is configurable by the user.



Health Monitoring Dashboard

4 IMPLEMENTATION PLAN

This section describes Verint’s management approach towards project implementation, detailing the steps taken to assure technical and managerial implementation of the project towards a fully operational solution while minimizing risk factors

The Verint project management methodology is based upon on over two decades of large scale project implementation experience and hundreds of projects delivered and implemented successfully. Verint’s trusted project management methodology consists of three (3) major items:

- Comprehensive Project management processes & programs
- Solid Quality Assurance (QA) & control processes
- Utilization of the Theory of Constraints (TOC) delivery methodology

4.1 Project Management Processes & Programs

Successful project implementation is achieved by focusing on four (4) key success factors:

Project scoping; Project planning, Project execution, Project Go-Live process

4.2 Project Scoping process

This process ensures that while interacting with the customer, Verint will gain an understanding of the customer’s organizational as well as operational needs to turn them into a precise design covering architecture, sizing, capacity, system functionality, IT operational constrains, production deployment, knowledge delivery, Go-Live and project closure.

The scope of functionality is clarified both Internally within Verint and with the customer.

The scoping process is a key success factor for ensuring an efficient and effective project delivery. The process is structured to understand, verify and clarify with the customer the detailed requirements of the project. It covers functionality, user workflows and methodology of work, organizational roles, data workflows, system interfaces, IT environments, architecture concerns, training and installation requirements. The main objectives of this process are:

- Concluding project detailed requirements with customer
- Full understanding of the project scope in order to make sure all requirements are fulfilled
- Reducing risks of implementation with an emphasis on minimizing impact to ongoing operations
- Removing vagueness early on in the process
- Committing internally to the project scope
- At the end of this process the Customer and Verint will have a joint agreement on overall project requirements and scope.

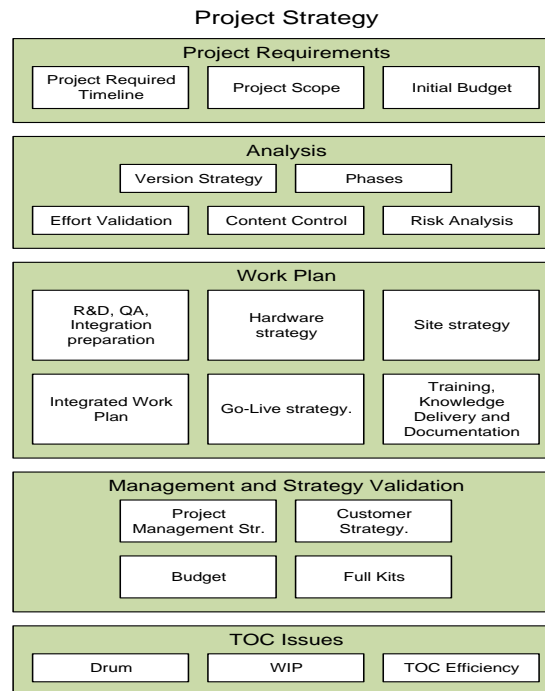
4.3 Project Strategy Planning

The customer is highly involved in this planning stage and Verint with the Boston PD shall maintain open communication to define and refine the project scope, develop the project management plan and identify and schedule the project milestones.

Strategy Planning involves the stages of the implementation process according to the plan defined at the Kickoff meeting.

This stage outlines a clear plan for obtaining project targets and also involves defining the required preparation tasks before project execution can begin. The flow of a strategy phase is comprised of five (5) logical blocks:

- Project Requirements
- Analysis
- Work Plan
- Management
- Strategy Validation and TOC issues



4.4 Project execution process

The execution process consists of the processes used to complete the work defined in the project plan and to accomplish the project's objectives. The execution process involves coordinating people and resources as well as integrating and performing the activities of the project. The deliverables are produced as outputs from the processes performed as defined in the project management plan.

This is the most intense and important stage of the project. This stage combines multi-disciplinary activities by developers, system integration, QA, operations, training, documentation and the PM. This stage begins with a Detailed Planning stage and ends with SAT (customer acceptance).

All the previous stages were designed to prepare the project for smooth execution. The execution stage begins after the following is ready: a high-level validated and committed plan, a final Project Requirements and Specifications (PRS) and an approved (Critical Design Review) CDR. This means that the execution of the project can commence with full attention.

This chapter combines several types of elements that have been joined together to form the execution methodology. These elements include:

- **Project Flows:** Each activity falls into a project flow. Flows are usually assigned according to the department that runs them (for example, Development, QA, Operations, System Integration and so on). Each flow is generally department oriented. For example the Operations flow is performed by the Operations department, QA flow is performed by the QA department and so on. The Site flow is the only one that is performed by multiple departments.
- **Control Gates and Processes:** Throughout the process, there are management gates that control the readiness to run a certain phase. These gates are described within the relevant flow. There are three (3) gates:

Gate 1: Execution Gate

Gate 2: Drum Gate (QA)

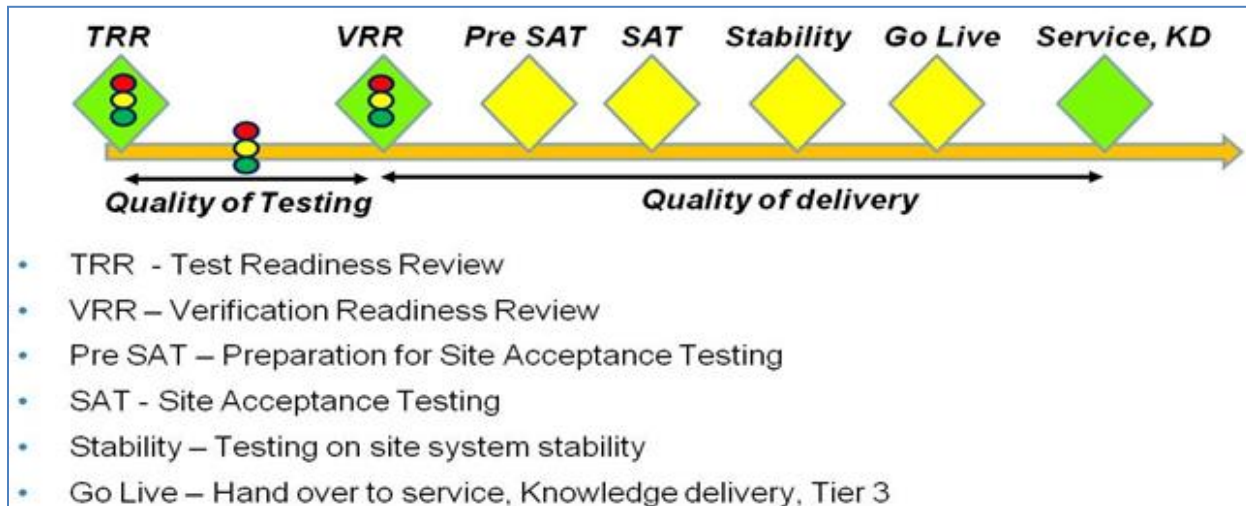
Gate 3: Site Gate

Tools and Templates: Throughout the methodology, several tools and templates are used.

After successfully passing the gate all relevant departments commence their activities. Each aspect of the execution has a dedicated *flow* in the methodology. The main flows are:

- **Operations Flow:** Includes purchasing, subcontractor aspects (if applicable) and shipment.
- **Development Flow:** Includes software design and development.
- **System Deployment Flow:** Includes all in-house system integration activity to prepare and support the systems for the various development and QA stages.
- **Quality Assurance (QA) Flow:** Includes all testing activity in Verint, such as testing preparation, testing and factory acceptance testing (FAT).
- **Site Flow:** An integrative stage that includes multiple disciplines (PM, Deployment, Development and QA). It includes all stages leading to the site activity followed by site installation, integration, testing and site acceptance test (SAT).

Project Quality Processes



4.5 Project Go Live Plan & Strategy

4.5.1 Overview

The Go-Live plan establishes the project go-live process focusing on the operational needs and usage of the system in full production mode and to smooth migration to operational mode. This section describes the Go-Live process. It will describe the steps and the activities that should be taken in order to allow Boston PD to move to full production with the Web Intelligence Center Solution.

- Process Scope
- Process Timelines
- Roles and Responsibilities
- Success Criteria
- Problem Management and Risk Mitigation

4.5.2 Key Elements

- Go Live Package: mutual set of steps to assure a smooth implementation of the delivered system into production mode
- Training and Knowledge Transfer:
 - Operational usage including, operational flows and specific requirement, methodology. Training kits and documentation
 - End users, admin and maintenance basic training

- End users, admin, analysts advanced training
- Methodology and advanced Analytics tools training
- Monitoring: Process will be monitored by both project management teams (Verint and QS)

4.5.3 Success Criteria

Success criteria for the Go-Live process at which point the project can move into its next phase and the Boston PD team can start using the system in full production mode. In order for the End users to start working with the system the following shall be done:

- Go-Live process was concluded according to the agreed plan
- Boston PD team is confident operationally to work with the system
- Boston PD team is confident to support the system internally

4.6 Project Communication & Cooperation with Customer

As part of our primary focus in project management, communication management is given a high priority. In keeping with open communication, our customers are encouraged to communicate directly with the Project Team whenever required. However if any issue needs to be highlighted, we provide an escalation mechanism that is defined in the escalation hierarchy section of the project management plan. To ensure such communication, Verint recommends the following processes and tools during the project life cycle:

- The Boston PD and Verint to agree and mutually maintain a project scoping document that contains the details and agreed functionality and scope of the project including features, sizing, capacity, design considerations, limitations, deployment plan and knowledge delivery plan. The scoping document will have constant traceability to the Boston PD requirement matrix.
- The Boston PD and Verint will maintain a joint project plan that includes all project timetables and milestones as well all major tasks to be completed before each milestone approval. The project plan will be the baseline for all timetable discussions.
- The Boston PD and Verint will jointly maintain a “Roles and Responsibility” table that represents the tasks and the responsibilities of each party in the project.
- The Boston PD and Verint will maintain project “Open Issues” table to be followed constantly by both Project Managers.
- The Boston PD and Verint will maintain a “Risks” table with a mitigation plan to overcome the identified risks.

The above five (5) documents and tools are the baseline for joint project management and alignment between the Boston PD and Verint.

4.7 TYPICAL SOW TIMELINE

The below table represents a typical SOW timeline for a Web Intelligence solution implementation process. Specific timeline will have to be determined once the entire project scope has been solidified however the milestones outlined in Section 7C of the RFP with a proposed project kickoff in January of 2017 and a completion over the course of a 6 month timeline wrapping up by June 2017 are considered quite achievable.

Milestone	Description	Task Owner	Comment
1.	Purchase Order / LOI / Contract Signature	CUSTOMER	The signing of the contract and the issuance of a purchase order constitutes the first milestone and is typically the baseline for all subsequent milestones.
2.	End User certificate + System Design Meetings	CUSTOMER + Verint	
3.	Customer Design Review (CDR) Approval Meeting + Site survey	CUSTOMER + Verint	
4.	Delivery of the Site Preparation Guide (SPG) and Network Design Document (NDD)	Verint	
5.	Shipment and Delivery to Boston PD Site	Verint	
6.	Installation Readiness Review (IRR)	CUSTOMER + Verint	All relevant components are ready on customer end for integration
7.	Phase 1 Site installation	Verint	Conducted on customer site
8.	Go-Live / SAT - Site Acceptance Testing	CUSTOMER + Verint	Conducted on customer site
9.	Phase 1 Operator Training	Verint	Conducted on customer site
10.	Phase 2 Advanced Training	Verint	Conducted on customer site

4.8 Support Services Offered

Verint provides its customers with comprehensive support services. These support services ensure that the systems deployed by Verint continue to meet customers' operational requirements on an on-going basis.

The following describes the generic support services and plan offered by Verint. Note that each plan will be tailored to the specific project to include those deliverable elements per project.

A project specific SLA document will become part of the Master Software License, Service and Support Agreement which is executed and the terms of such Agreement govern the provision of support and maintenance services by Verint.

4.8.1 Definitions

Below are the definitions of various terms used throughout this support description:

Definitive Solution – Correction of a problem in such manner that no further actions are required.

Local Business Hours – normal working hours in the country of the Customer.

Problem – Circumstance that a Customer encounters that inhibits the Customer from utilizing the installed System in a normal operational mode.

Response Time – Measured from the time the Customer initially contacts the Help Desk until Verint Support Engineer responds to the Customer's problem.

Site – Customer premises where the System is installed.

Software Recovery Time – Measured from the time the Customer notifies the Help Desk, reports and identifies the problem until the severity of the problem is reduced.

Support Engineer – Certified Verint personnel that is trained, knowledgeable and technically capable of analyzing, diagnosing and supporting the System.

System – Combination of hardware, software and/or firmware delivered by Verint as per the Purchase Agreement.

Temporary Solution – Correction of a problem / workaround ensuring that the problem will not occur again and restoring the functionality of the system, until a Definitive Solution is implemented.

GA Version – General Availability version of the Verint WebInt-Center suite

Web Flow – A Web Flow is a set of instructions that define to the WebInt-Center system exactly how to find and extract the desired information from an Internet URL. The main function of Webint-Collect is to assist users in building and maintaining web flows. Usually each web site requires a dedicated Web flow.

Web flow can be defined by Verint for **GA Web flows** and **Project Web flows** or by the customer for **Customer configured Web flows**.

GA Web Sites – A set of web flows provided as a part of the WebInt-Center general availability product (GA) designed to collect data from pre-defined list of web sites. The list of supported web sites and their specifications included in the predefined web sites specification document.

Project Web Sites – The Web Flows that Verint builds at customer request. The list of supported web sites and their specifications will be part of the project definition.

Customer Configured Web Sites – The Web Flows configured by the customer.

Pro-Active Test - Periodical test of the delivered Web Flows. These tests are performed by Verint to proactively insure product functional performance.

Collection Issue – The situation where a Web Flow has difficulty collecting data from a web site due to an element of the website that is interfering with the process. Collection issues are described in the technical specifications during a Pro-Active Test or reported by customers.

Major Web Site Change – A major change in a supported web site that completely changes the way that it holds or displays the data. The change can be reflected by changes in layout, web site API, technology or policies. Such a change may lead to a complete or partial failure of the data collection process of the Web Flow.

To clarify, new RFC or a new request for new data type that is available on a web site, is not considered as Major Web Site Change and not supported as part of the support plan

Non-Major Web Site Change – A change in the layout or API of a supported web site that causes a collection coverage gap but doesn't completely change the way the site holds or displays the data. Usually the purpose of this change is medium or small changes to the visual design of the web site

Rich vs. Regular web sites – Rich web sites are usually ones that include enhanced social aspects, relations and a variety of objects. Web sites can also be classified as rich due to its advanced layout presentation, technology, etc.

Our GA Web Sites list classifies the different sites into regular and rich sites.

Problem Severity Level Definitions

Level	Definition
Critical (Severity 1)	<p>The System has a Critical Problem if:</p> <ul style="list-style-type: none"> (a) there is a complete System failure in which no field procedure resolves the Problem; or (b) the System needs to be reset several times a day; or (c) the functionality of the System is drastically impaired. <p>A Critical Problem that can be circumvented or avoided is considered a Major Problem.</p>
Major	The System has a Major Problem if:

(Severity 2)	<ul style="list-style-type: none"> (a) the System administration or major maintenance functions are severely impaired; or (b) there are intermittent failures of System services; or (c) the System restarts and/or resets resulting in loss of some user functions; or (d) Web Flows provided as part of the GA Web Sites are non-functional and do not collect any data; <p>A Major Problem that can be circumvented or avoided is considered a Minor Problem.</p>
Minor (Severity 3)	<p>The System has a Minor Problem if:</p> <ul style="list-style-type: none"> (a) there is minor impact to a System that restricts use of features and functionality of the System. (b) there is how-to/help requests. (c) there is a documentation error (d) there are non-critical activity log messages (e) the Web flows provided as part of the GA Web Sites are partially functional and collect partial data; (f) Any other Problem that is not defined as Critical or Major.

4.8.2 Scope of Services

Verint provides extensive support and maintenance services as detailed herein with respect to software and hardware items supplied by Verint.

All services offered hereunder are subject to (1) Verint’s security policy and (2) receipt of any necessary support and assistance from Customer as may be required to complete the efforts described herein.

4.8.2.1 Help Desk

Verint’s Help Desk is the first point-of-contact for customers to resolve faults or operational problems. The Help Desk also assists with troubleshooting and resolving related technical issues.

In each of Verint’s regional customer support offices, Verint Support Engineers are on staff to receive the Help Desk calls. All faults and operational problems reported by the Customer to the Help Desk are recorded in a computerized, internal workflow management system. During a Customer’s initial contact with the Help Desk, the Verint Support Engineer handling the call, together with the Customer, determine the severity of the Customer’s System Problem.

The Help Desk system also manages and follows up the resolution of all recorded faults and operational problems. Verint's Help Desk ensures that all communication and exchange of information is handled and

performed securely and in accordance with Verint’s strict security standards. Please see section 3 on Problem Resolution Workflow.

As part of the Help Desk system services, the Help Desk may generate data reports, as per customers’ requirements based on different profiles and individual requirements.

Verint Help Desk Contacts Details:

All Hours - Help Desk Toll Free Number	1-888-983-7468
Help Desk Email	contactcenter@verint.com

4.8.2.2 Remote Access

Remote connection is recommended in order to achieve faster issue analysis and resolution. In order to achieve faster and more efficient service, Verint recommends remote access to Customer locations (or end users location with respect to partner Customers).

Upon mutual agreement, Verint will use Remote web-based access or a Site to Site connection.

4.8.2.3 On Site Support

In the event that a Problem is beyond the scope of support provided by the Help Desk, Verint undertakes to dispatch, subject to the provisions herein and with the Customer’s approval, a Support Engineer to the Customer Site, who will remain there until the Problem is resolved or an acceptable recovery is in place. At all times, the Support Engineer must be accompanied on site by the Customer representative. Prior security approval, if needed, is the responsibility of the Customer and must be provided prior to arrival of Verint Support Engineer.

4.8.2.4 Software Maintenance

In the event of a Problem requiring a software repair, Verint will provide a software fix that can be integrated into the System. Software fixes are generally delivered in a secure, electronic format and are executable by the Customer.

For Critical problems, correction work shall commence within the Response Time and shall continue non-stop until a workaround is provided allowing the reduction of the severity of the problem.

Recovery Time specified in Section 4 is on average in 90% of the cases.

In addition, Verint develops permanent fixes for Problems. These are incorporated into Service Packs Updates that are periodically distributed to the Customer as and when required, in Verint's sole discretion, to fix bugs or maintain System performance. These Service Packs Updates do not include new features or functionality.

4.8.2.5 Collected Web Site Changes

WebInt-Center is an open source intelligence system and as such offers a web collection mechanism that collects various types of publically available information from the Web such as Web pages, Social Media Network data, , comments, images, forums, blogs, news etc.

The nature of the Web is dynamic; web sites and interfaces change constantly. These changes are differentiated between Major changes and Non-Major changes. The support for both Major and Non-Major Changes are equivalent with different resolution time.

4.8.2.6 Collected Web Site Change – Tracing

A Verint team of dedicated professionals is proactively and continuously monitoring GA Web Sites. When a change is encountered in one of the supported web sites that prevents the web flow from collecting data, Verint will issue a notification on the impact of the change.

Based on the Verint analysis, Verint will provide a notification indicating when a solution will be available. The solution will be provided in accordance with the resolution time as described in section 4.

The same procedure is followed when an issue is reported by a customer.

During the support period, Verint releases support software versions to its customers including the latest application fixes, collection fixes and detailed release notes.

4.8.2.7 Collected Web Site Change – Coverage

Verint GA Web Sites are covered for both a Major change and Non-Major change. Verint is entitled to classify the Web Site Changes to major or non-major and the classification is subject to Verint's discretion.

The changes are covered within the time frames described in section 4 and subject to the support plan limitations described herein.

If the change requires not only a Web Flow update but also a software update, (e.g. WebInt-Collect needs to support a new action), Verint will release a software update for that issue in the next service pack release.

For uncovered changes on Project Web Sites and Customer configured Web Sites, the Verint team will offer the customer suggested alternatives for resolving the issue. Verint engineers can also provide fixes for those issues as a separate service available via a Verint Time and Materials proposal.

In very rare situations, some web changes may be significantly more difficult to address or potentially technically impossible. Those changes may be fixed on the next major version of the WebInt-Center or, based on the specific circumstances, not at all.

Coverage Summary Table

	GA Web Sites	* Project Web Sites	Customer Configured Web Sites
Proactive Monitoring	Yes	By Customer	By Customer
Change on Web Site	Yes	By Customer	Help desk consulting during working hours

*Support and proactive monitoring for Project Web Sites can be purchased separately.

4.8.2.7.1 Problem Correction

For Critical and Major Problems, Verint will initially provide a Temporary Solution in order to resolve a Critical Problem. A Definitive Solution for the problem will be released as soon as reasonably possible. Verint will use its commercially reasonable efforts to complete the Temporary and Definitive Solution promptly and in any case within the time periods specified in Section 4. Verint will inform the Customer periodically about the progress of the resolution activities.

For Minor problems, Verint will examine the problem and create a solution as soon as reasonably possible according to the planning and resources required, and in any case within the time periods specified in Section 4.8.4 – Support Plan Summary below.

4.8.2.7.2 Upgrades

- **Service Pack Release**

A service pack version will be released on a periodic basis, subject to Verint’s discretion. The support plan includes Service Pack Releases related to Web site changes and system application malfunctions.

- **Major Version Release**

A major version will be released on an “if and when available” basis, and subject to Verint’s discretion. The support plan includes major versions updated for the customer. The major versions will include improvement of existing functionality, User Interface changes, bug fixes and performance improvements but will not include new licensed features that can be purchased separately. In the event a major release will require any 3rd party new software components or hardware replacement/addition, the customer will cover such costs based on the Verint updated pricelist.

- **Issues on a Non- Updated Version**

In the event of an issue raise on a non-updated version, Verint will be entitled to require the customer to upgrade to its latest GA version. Verint is entitled to release the fix only for the latest GA version and that upgrade will be the customer’s responsibility.

- **Hardware**

Hardware purchased from Verint will be compatible for at least three years of version upgrades from project's Purchase Order date, not including new licensed features that may require new hardware and not including storage size that may require expansion and which depends on system usage and purging definitions.

4.8.2.8 Antivirus Software Maintenance Policy

For new Systems, Verint installs antivirus software, with the latest virus inoculation file updates on all servers that Verint supplies. Maintenance of the Norton Antivirus virus protection updates is transferred, along with any yearly subscription fees, to Customer and it's the customer responsibility to keep the system up to date with the latest virus protection update.

In the event a virus infects Verint Products and field service dispatch is required, and the virus would have been blocked with an available antivirus file update, Customer agrees to reimburse Verint for time (based on Verint's then-current Time and Materials Price List), materials and expenses (based on actual expenditures).

4.8.2.9 Hardware Maintenance (If H/W provided by Verint)

In order to maintain proper SLA for hardware maintenance, it is Customers' responsibility to purchase and maintain Verint's recommended spare parts.

4.8.2.9.1 Hardware Repair

Verint undertakes to repair or replace, at its own discretion, faulty parts returned by Customer in accordance with the RMA procedure defined herein. Verint will deliver said repaired or replaced parts within the time interval set forth in Chapter 4, Support Plan, commencing from receipt of the faulty part at the Verint repair center until delivery of the returned part to Customer. These provisions shall not apply if the System or any part thereof has been damaged by improper operation, maintenance, misuse, accident, neglect, fault or negligence or has been subject to the opening of any sealed components without Verint's prior written approval. Verint will extend its support period, as per this proposal, for the repaired or replaced parts for a period of six months after delivery of said part to Customer.

4.8.2.9.2 SWAP – Replacement of Critical Part

Verint undertakes to maintain a reasonable emergency stock of spare parts for servicing the Customer's equipment in the field.

Verint undertakes to exchange faulty parts, reported and returned by Customer in accordance with the RMA procedure defined herein, with Verint's spare parts stock. The replacement part shall be delivered to the Customer immediately after receiving the written notification of the faulty part at the Help Desk.

This Swap procedure is contingent upon the Customer owning and maintaining Verint's recommended spare parts kit.

In case the faulty part does not reach Verint within 60 days from reported RMA, the customer will be charged the cost of the faulty part.

Packing of faulty parts will be inspected at customer site. If the packing is not correct, the parts will not be collected from site.

4.8.2.9.3 Repair Material Authorization (RMA) Procedure

The following procedure must be followed when handling parts that need to be repaired or replaced, as per paragraph 4.8.2.6.1 and 4.8.2.6.2 above:

- 1) Customer contacts the Verint Help Desk to report the faulty part;
- 2) Verint Help Desk provides an RMA number to the Customer;
- 3) The Customer provides details of the fault including the part type and serial number;
- 4) A Verint Support Engineer subsequently reviews and approve the request;
- 5) An RMA number is assigned and sent to the customer;
- 6) The Customer packages and ships the faulty part for return to Verint as per Verint's instructions, within seven (7) days of reporting the fault
- 7) The Customer notifies Verint of dispatch of the faulty part in writing, including the RMA number, serial number of the faulty part and the date of dispatch from the Customer's premises; and
- 8) Verint ships the repaired or replaced part to the Customer.

4.8.2.9.4 Packaging

All parts shall be packaged by Verint (and Customer, if relevant) in accordance with proper industry standards. The RMA number must be clearly marked on the return item as well as on the package and shipping documents. In the event of the replacement of an entire subsystem or system, all parts must be packaged in their original packaging.

4.8.2.9.5 Delivery

Regarding parts to be delivered by Verint to Customer, delivery terms shall be CIP Airport of Destination (Incoterms 2010) at Verint's expense.

Delivery of faulty parts by the Customer to Verint shall be CIP Airport of Destination (Incoterms 2010) basis at the Customer's expense. When the Customer is delivering faulty parts to Verint, the shipment of parts must conform to the Repair Material Authorization ("RMA") procedures described in Clause 4.8.2.6.3 above in the Support Plan.

4.8.2.10 Third Party Software Installations

Verint recommends that in the event that Customer requires installation of any third-party software, the Customer should notify Verint prior to such installation. Subsequent to the installation of third-party software,

should field service dispatch be required and it is determined that the problem is related to such third-party software, Customer agrees to reimburse Verint for time (based on Verint's then-current Time and Materials Price List), materials and expenses (based on actual expenditures).

4.8.2.11 Life Cycle

WebInt-CENTER suite policy has been created to address the needs of the open source web intelligence world and its dynamic, fast changing nature.

In order to supply the best service and functionality we recommend our customers to have an up to date system with the latest available version.

Once a new minor/major release is declared as a General Availability release, it is available for our customers as part of the SLA.

Six months after a G.A. release is declared, Verint will be entitled to declare the previous major release as an "end-of-support".

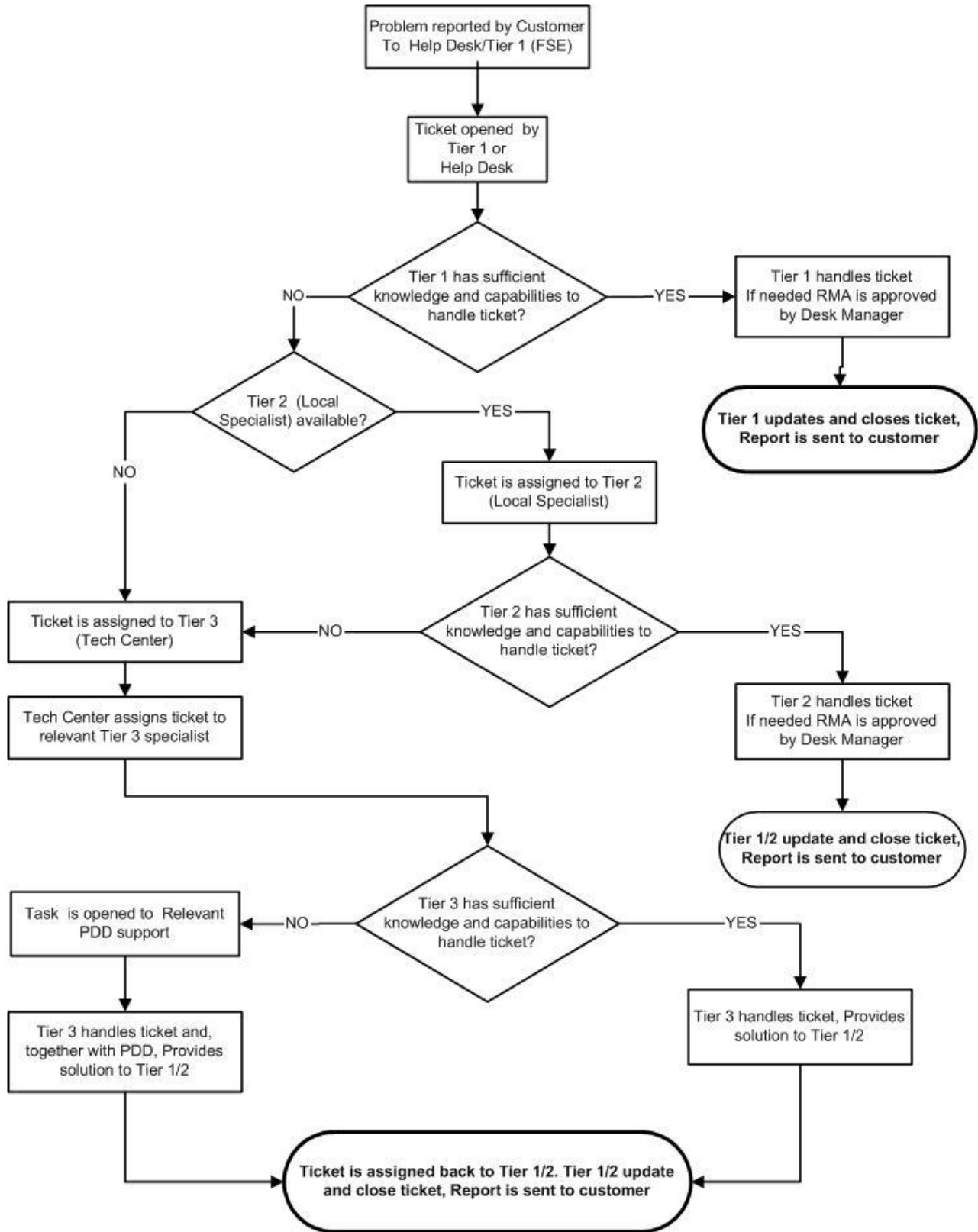
As long as a major version is in its support period, Verint will proactively test the G.A. web sites and main functionality on that version with the last minor release.

Once "end-of-support" is declared, Verint will stop proactive testing the G.A. web sites on the "end-of-support" version.

4.8.3 Multi-Tier Problem Resolution

The following support tiers outline the workflow process for resolving problems reported by a customer to the Verint Help Desk.

- a. **Tier 1 Support** – technical support level that is provided by field engineer. Support activities at this level should include software and hardware installations, basic troubleshooting, pre-arranged configuration changes, operation optimization, site survey preparation, and training.
- b. **Tier 2 Support** - technical support level that is provided by field specialist. Support activities at this level should include all Tier 1 activities, customization management, configuration changes, diagnostics and advanced troubleshooting.
- c. **Tier 3 Support** - technical support level that is provided by Verint's Technical support specialist. Support activities at this level should include all Tier 1 and 2 activities, in-depth System instructions, advanced diagnostics and troubleshooting at the R&D level.
- d. **Tier 4 Support** - technical support level that is provided by Verint's development engineer. Support activities at this level should include design level consultation and solutions, hardware chip-level diagnostics, software R&D diagnostics, and high level of software and hardware fixes and solutions.



4.8.4 Support Plan Summary

Verint is pleased to offer the WebInt-Center Support plan:

Parameters	Support Plan	
Help Desk Availability	7 days / week 24H	
Phone Response Time	Critical	30 min
	Major	1 hour
	Minor	Next business day
Software Recovery Time**	Critical	2 days
	Major	4 days
	Minor	As part of the Service Pack Update
Web Flow recovery time** (No change on web site)	Major	6 days
	Minor	As part of the Service Pack Update
Web Flow recovery time** (Change on web site)	As described on the Web Flow recovery time table below	
On Site Support	Included	
Hardware Repair***	Critical	SWAP */ 5 days No Swap / 15 Days
	Non Critical	15 days
Hardware Replacement ***	Critical	15 days
	Non Critical	30 days

Delivery Terms	DDU (Incoterms 2000)
Annual Preventative Maintenance Visits	2

* The Swap procedure is contingent upon the Customer owning and maintaining Verint’s recommended spare parts kit.

** For at least 90% of the cases

*** For at least 90% of cases if supplied by Verint

Web Flow recovery time for change on a GA web site

Web Site type	Change Level	Severity Level	Support Plan
Regular	Major / Non-Major Web Site Change	Major	6 days
Rich	Non-Major Web Site Change	Major	15 days
Rich	Major Web Site Change	Major	30 days
Regular / Rich	Major / Non-Major Web site Change	Minor	As part of the Service Pack Update

4.8.5 Service Level Agreement Annual Cost

Annual support fees after warranty expiration are calculated as a percentage of total undiscounted system value excluding services. Support plans must be purchased and activated prior to system warranty expiration to ensure the system is maintained in a manner consistent with the operational needs.

This maintenance fee includes not only the system maintenance and support as with regular IT software & Hardware deployment:

- a. Regular: System Maintenance, that includes hardware (if provided) and software maintenance, upgrades and ongoing support;

- b. Special: GA Web-Flow updates provided by Verint. Those updates will save the customer considerable investment of manpower in coping with website changes and updates.
- c. Special: Ongoing advisory services on proper use of the system

Project	Support start date	Support End date	System Value	Support price	Total Price
				20% of Verint's list price	
Total					

- a. All prices are quoted in US Dollars.
- b. First year maintenance is included in the sale price.

Second year maintenance will start 12 months from first installation and the date of connectivity to the internet to start collecting data, and will be paid every year in advance.

Other Support Terms:

Verint's undertakings as per the terms of this proposal are contingent upon Customer's compliance with the obligations and responsibilities set forth herein.

Verint's responsibilities for the System purchased ends at the cross connection to other vendor equipment. If the trouble appears to reside in the cross connection or in the other equipment not provided by Verint, then the Customer should refer the trouble to the vendor serving that equipment. Verint will cooperate with the Customer and the other equipment vendors with the aim of resolving such problems.

Verint shall not be responsible for repairing the System or providing other services required as a result of negligence, misuse or mishandling of the System by Customer or any third party not under Verint control, unauthorized repairs or maintenance, inappropriate environmental conditions (such as power and air-conditioning failures), or damages to the System caused by events such as lightning, fire, earthquake, or floods. Repairs or other services required in such circumstances will be negotiated by the parties on a case by case basis.

Lapse in Coverage, Verint recommends that maintenance coverage remains in place at all times. In the event maintenance coverage lapses, Verint will reactivate maintenance coverage on the following conditions: (i) Verint will assess the System performance, and Customer agrees to reimburse Verint for time and material required to assess and/or restore System to its normal operation (based on Verint's then-current Time and Materials Price List); (ii) Customer will be required to prepay for a new one (1) year Maintenance Plan; and (iii) Customer will be required to pay a reactivation charge equal to twenty five percent (25%) of the annual cost of the new

Maintenance Plan which covers Verint's expenses associated with setup, back office support, database maintenance of System, site configuration, etc.

In order to avoid any doubt, in the framework of this proposal, VERINT'S SOLE UNDERTAKING IS TO PROVIDE SUPPORT SERVICES AS DESCRIBED HEREIN. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID AND ARE IN LIEU OF ALL OBLIGATIONS OR LIABILITIES ON THE PART OF SELLER FOR DAMAGES.

As part of the support services, Customer may provide live system access rights to authorized Verint personnel. In such a case, Customer acknowledges that by providing Verint with such access rights it is aware that Verint authorized personnel may be exposed to Customer's information including, but not limited to, Personally Identifiable Information (collectively, "**Customer Data**"). Customer consents to the disclosure of Customer Data to Verint and its affiliates for the limited purpose of carrying out the tasks defined above. Such consent is conditioned on the Customer Data being maintained as the confidential information of Customer in accordance with any terms of confidentiality and non-disclosure between Customer and Verint.

5 QUALIFICATIONS & EXPERIENCE

5.1 Verint's Experience

Founded in 1994, Verint® Systems Inc. (NASDAQ: VRNT), is a global leading provider of Actionable Intelligence® solutions. In today's dynamic world of massive information growth, Actionable Intelligence is a necessity for empowering agencies and organizations with crucial insights and enabling decision makers to anticipate, respond, and take action.

Our Actionable Intelligence solutions help organizations address three areas of the market — customer engagement optimization, security intelligence, and fraud, risk & compliance — by capturing large amounts of information from numerous data types and sources, using analytics to glean insights from the information, and leveraging the resulting intelligence to help optimize customer engagement, enhance security, and mitigate risk.

We have established leadership positions in our respective markets by developing highly-scalable, enterprise-class solutions with advanced, integrated analytics for both unstructured and structured information. Our innovative solutions are developed by a large research and development team, which has led to more than 700 patents and patent applications worldwide. We offer a range of services, such as strategic consulting, implementation services, training, maintenance, and 24 x 7 support, as well as a broad range of deployment models, including on premises, hosted, managed services, and software as a service ("SaaS").

In each of our operating segments, we believe that we compete principally on the basis of:

- Product performance and functionality
- Product quality and reliability
- Breadth of product portfolio and pre-defined integrations
- Global presence and high-quality customer service and support
- Specific industry knowledge, vision, and experience
- Price

Our solutions help organizations make timely, effective decisions for improving enterprise performance and making the world a safer place. Today our solutions are used by more than 10,000 organizations in over 180 countries, including more than 80 percent of the Fortune 100.

Verint is headquartered in Melville, New York, with offices worldwide, more than 4,500 dedicated professionals, and an extensive global network of selling and support partners. Verint is financially strong and positioned for growth as a highly diversified, customer centric business with over \$1.158B in revenue last fiscal year.

We are committed to conducting our business in an ethical manner and creating value for our customers, partners, employees, and shareholders, as well as the communities in which we work and the global community at large. At Verint, we view corporate responsibility as key to our success and integral to the way we do business.

Law enforcement, national security and intelligence agencies are responsible for investigations related to crime, terrorist networks, drug trafficking, cyber-attacks and other illegal activities. Such investigations involve highly complex methods and include the collection, integration and analysis of information from multiple sources, including cyber space and a variety of communications networks.

Verint's Cyber Intelligence solutions include:

- **Cyber Security** - Enables government, critical infrastructure, service providers and enterprise organizations to address advanced cyber-attacks by deploying a pre-integrated cyber security platform capable of delivering threat protection through Actionable Intelligence capabilities. Integrates multiple advanced detection engines and provides unified workflows for investigation, behavioral analytics and forensics in order to analyze attack paths, enable remediation and help protect against future attempts.
- **Network Intelligence** - Enables law enforcement, national security and intelligence agencies to generate Actionable Intelligence from network traffic to rapidly uncover critical information for investigating and proactively addressing criminal, national security and terrorist threats. Can be configured to address a wide range of communications networks and can scale to address large traffic volumes.
- **Web Intelligence** - Enables investigative units to leverage web, and open source data in order to identify insights and help accelerate investigations of fraud, criminal, terror, cyber and national security threats. Helps transform large volumes of content into meaningful intelligence and identify suspicious behavioral patterns including locations of suspects and links between suspects.
- **Intelligence Fusion Center** - Enables government organizations to build a centralized analytics platform for generating insights, identifying potential threats and generating Actionable Intelligence. Provides a cross-source / cross-format single point of access to all intelligence data sources to enable organization-wide investigation, management and analysis.
- **Lawful Interception Compliance** - Helps communications service providers comply with ETSI, CALEA, and other lawful interception regulations and standards. Supports many different network types and provides a high degree of automation of the lawful interception compliance processes with complete audit trails and low administrative overhead without disrupting service.

Based on over 20 years of field proven experience, Verint offers a diverse portfolio of communications intelligence solutions. Our solutions deliver the comprehensive technology and functionality to collect any means of communication and turn raw data into actionable intelligence, while complying with relevant government mandates. Verint has implemented these solutions in countries around the world and is supporting the complex operations of some of the most prominent lawful enforcement agencies, intelligence organizations and communications service providers worldwide.

As a leader in the communications collection market, Verint is an active member in CALEA, ETSI, 3GPP and other international and regional standardization organizations. Verint is committed to developing products and delivering solutions according to the recognized standards of these organizations.

A key differentiator for Verint is the fact that we not only work with agencies and governments for the collection, fusion and analysis of data either warranted or open source, but we also work with many of the

leading telecommunications providers for lawful communications compliance requirements. Verint boasts the fact that within the US, we are the incumbent lawful intercept compliance vendor in most Tier 1, Tier 2 and many Tier 3 telecommunications networks. This is a distinct advantage for our data collection, fusion and analysis customers in terms of experience, technology roadmap and overall operation of the various facets of producing Actionable Intelligence through data collection.

Verint has extensive project implementation experience ranging from small, one-site configurations to complex, countrywide implementations. Verint has successfully deployed data collection, fusion and analysis solutions at hundreds of sites around the world.

Verint initiates a partnership approach to project implementation and customer support activities. Based on our recent customer Satisfaction Survey, a majority of our customers declared that they perceive Verint as a valuable partner, expressing that our relationship is characterized by mutual trust and respect. Furthermore, our customers identified that our implementation activities are performed in a professional manner, while conveying a high overall satisfaction with Verint.

System Security is fundamental to the architectural design, application functionality and network configuration of all Verint products. This emphasis on security is an extension of the overall security-orientation of Verint. Among the inherent security features in Verint's products is an extensive range of authorization, authentication and audit measures to ensure appropriate internal access to functionality and information as well as safeguards against external penetration and computer viruses.

5.2 Response to RFP Sections 8A & B

The following sections are direct responses to the Plan of Services response as requested in RFP Section 8 A & B

5.2.1 Plan of Services – Company (RFP Section 8A)

- 1. Please describe the proposer's organization (i.e., origin, years in business, annual revenue, regions of operation, etc., including any and all affiliates and subsidiaries, whether location inside or outside the City of Boston and or U.S.) and staff with details on additional personnel, organizational changes and equipment (including local distributor) required.***

As described in detail above in [Section 5.1](#)– “Verint’s Experience”, Verint is a leading global provider of Actionable Intelligence® solutions that is headquartered in Melville, NY. The team leading the opportunity for the Boston Police Department deployment is a specialized group primarily based out of Gainesville, VA which is responsible for North American deployments and support of Verint’s various communications and intelligence solutions. The core group consists of 14 individuals, some with federal law enforcement experience, several with current US security clearances and many of which are field support engineers deployed across the US and Canada with a high concentration on the north-central east coast. Verint generally provides full turn-key solutions which are architected, developed, produced, deployed and fully supported by Verint. The proposed solution for the Boston PD is a hybrid solution consisting of both an on premise solution called Verint WebInt as well as a SaaS solution called Verint WebAlert. The overall solution will be a turnkey system deployed and supported by Verint.

- 2. Please provide information on recent installations (last 12 months) of proposed and/or related solutions for law enforcement, intelligence, defense, and/or security organizations. Please indicate whether or not the organization(s) is a U.S.-based organization. Please include total number and articulate nature of the solutions delivered if NOT exact proposed solution. Please note all supporting systems and any business partners involved with those implementation(s).***

The most recent and relevant installation is described in more detail in [Section 9](#) – “References”, of our proposal below. This was a US based implementation and was comprised of a Verint Web Intelligence Center Solution of very similar configuration as is being proposed for the BRIC. It consisted of both Verint WebAlert and Verint WebInt products and was deployed within a large enterprise environment under strict IT security controls. The deployment was recently completed in July 2016 and the system is fully operational. As is described in [Section 9](#) – “References”, this customer has agreed to host the BRIC for a demonstration of the overall operational solution. Verint personnel alone deployed, trained and continue to support this customer and their Web Intelligence operations.

- 3. Please provide total number of installations of proposed solution and/or related solutions, as well as the number of installations that are still in use (i.e., installed 5 years ago and still in use vs. installed 5 years ago but no longer in use), for law enforcement, intelligence, defense, and/or security***

organizations. Please indicate whether or not the organization(s) is a U.S.-based organization. Please differentiate between proposed and related solutions.

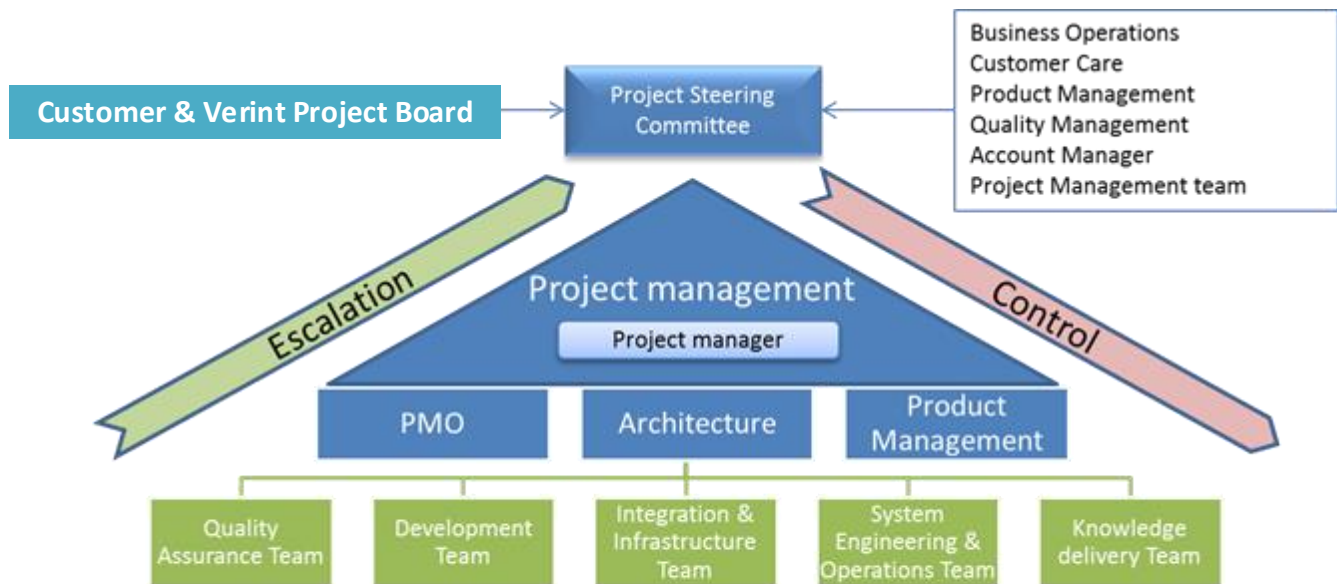
Verint’s Web Intelligence Center serves over 30 different active organizations in over 20 countries that are actively using the solution for Web data harvesting the deep and the dark Web, Web monitoring, analytics and investigation. Proposed solutions similar to that being offered to the BRIC are being used by law enforcement agencies in the criminal intelligence units (including those fighting drugs, pedophilia, human trafficking, etc.), anti-terror units, cyber defense at national intelligence levels, financial fraud prevention in government and enterprise, customs, immigration and border control among others. These Verint solutions also support related deployments for Non-Governmental Organizations (NGO’s) and large private enterprise customers using our social media monitoring platform for public safety as well as for protection of assets, IP, and senior executives. More detailed information can be found in [Section 9](#) – “References” of our proposal below.

4. Please describe any third-party relationships or dependencies that would be relied upon for the solution described in response to this RFP.

Verint will be fully responsible for the implementation and support of the entire turn-key solution. We do however re-brand and re-sell our Verint WebAlert SaaS solution from another vendor who may be utilized on occasion for Tier 4 support if necessary.

5. Please describe the implementation team. How many individuals will be involved in the delivery and implementation of the solution (i.e., from installation to operation to advanced user training)? What are their backgrounds? What certifications are held?

As detailed in [Section 4](#) – “Implementation Plan”, we discuss our project management methodology from the project planning phase through execution, deployment and on-going support services. Verint is structured in teams as shown in the diagram below and as described in more detail in [Section 4](#) – “Implementation Plan”.



Each team of the organization takes the responsibility of its respective functions to ensure that all aspects of a project are handled. Various members of each team will be assigned with project tasks based on the project requirements and other members of the team will be assigned to the project for its duration. Some of the key implementation team members identified to execute the Boston PD project are the following:

- Account Manager – Chris Polito
- Project Manager – Allan Williamson/Ronen Lampert
- Systems Engineering (Technical Expert) – Gil Yaakovi
- Knowledge Delivery – Alexander Aronovich/Orna Kenet-Guler
- Deployment & Infrastructure – Joe Mahaney/Adi Drori
- Support – Adi Drori/Ben Wheaton/George Busenberg

Mr. Chris Polito

Mr. Polito joined Verint in March of 2013 and is currently Vice President of Communications & Cyber Intelligence for North America. He is acting account manager for the BRIC. Prior to joining Verint, Mr. Polito served for 10 years as Senior Vice President of Global Sales and Marketing for TruePosition, a location-based safety and security company specializing on E-911 mobile location and a wholly owned subsidiary of Liberty Media.

Prior to TruePosition, Mr. Polito worked for Ericsson, a global leader in wireless and wireline telecommunications infrastructure. His last position at Ericsson was as Vice President of Sales.

Mr. Polito attended the Rochester Institute of Technology, the University of Maryland and the College of Charleston. He is a six-year U.S. Navy veteran.

Mr. Allan Williamson

Since February 2008, Mr. Williamson has served as Project Manager, North American Communications & Cyber Intelligence, for Verint Systems Inc., a leading provider of analytic solutions for communications interception, digital video security and surveillance and enterprise business intelligence.

From 2002 to 2008, Mr. Williamson served as a Senior Verint Field Engineer focusing on the implementation of enterprise workforce optimization and security intelligence solutions for major telecommunications entities. Responsibilities included project management, account management, solution implementation and full scale project planning.

Prior to joining Verint Systems Inc., Mr. Williamson was employed by Interland Inc. as the Call Center Manager for their European Region. This involved managing day-to-day operations of multiple call centers across various regions of Europe.

Mr. Williamson attended college at Georgia Institute of Technology, Oglethorpe University and University of Amsterdam-Vestermarkt, with an emphasis on Information Technology, Computer Science and Project Management. Mr. Williamson is a US Citizen currently residing in Atlanta, GA.

Mr. Ronen Lampert

Since March 2014, Mr. Lampert has been serving as Director, Customer Success Management for the Americas and APAC Regions for Verint Systems Ltd., a leading provider of analytic solutions for communications interception, digital video security and surveillance and enterprise business intelligence. This includes managing a team of project managers, having overall responsibility for customer success, leading the regions' operations, projects and priorities.

From July 2009, Mr. Lampert served as the Program Manager for Empire, responsible for the project from its inception to final customer acceptance.

From February 2008, Ronen Lampert has served as Project Manager, West Europe and North America RELIANT™ Solutions, for Verint Systems Ltd., a leading provider of analytic solutions for communications interception, digital video security, surveillance and enterprise business intelligence.

From 2005 to 2008, Mr. Lampert served as Service Desk Manager for West Europe and North America Region with an overall responsibility for operational support of mission critical communication interception solutions for both law enforcement and major telecommunications service providers throughout North America and Europe.

From 2004 to 2005, Mr. Lampert served as technical expert for North America customers positioned at Verint Headquarter in Melville, NY. Responsibilities included Tier-II support for field engineers, systems & network integrations.

From 1999 to 2004, Mr. Lampert served in multiple Customer Support Engineering positions and Technical expert (Tier-III) for Verint Systems Ltd.

Mr. Lampert earned a Bachelor of Business Administration (BBA) degree from the Open University, Israel, in 2007. In addition, he has earned a Practical Engineer degree from the Ort College, Jerusalem in 1995.

Mr. Gil Yaakovi

Since 2012 Mr. Yaakovi has served as Director, Sales Engineering NA Communications & Cyber Intelligence Solutions, for Verint Systems Inc., a leading provider of analytic solutions for communications interception, digital video security and surveillance, and enterprise business intelligence.

Since June 2006, Mr. Yaakovi served in different roles in Verint North America, including account management, project management and sales engineering.

Prior to his employment in Verint North America, Mr. Yaakovi worked as sales engineer for Verint System Ltd. in Israel from 2000 to 2006.

Prior to joining Verint Mr. Yaakovi served from 1992 to 2000 as program manager for the Israeli Defense Force, managing software development team of 11 engineers.

Mr. Yaakovi holds Master of Business Administration from Bar Ilan University and Bachelor of Science in Mechanical Engineering from the Technion – Israel Institute of Technology. Mr. Yaakovi is a US Citizen and resides local to the NY City area.

Mr. Alexander Aronovich

Since 2014, Mr. Aronovich has served as a Customer Success Manager specifically for the Web Intelligence Product Methodology group within Verint. In this capacity, Mr. Aronovich proactively manages the customer life cycle from post contract throughout the duration of the operational solution deployment ensuring the operational and intelligence harvesting success of customers. Mr. Aronovich performs training and on-going professional support to customers and colleagues by coaching and providing professional development to team members to enhance their web based analytical skills.

Mr. Aronovich holds significant Sigint/Cyber/Web intelligence background from both government and enterprise positions. Mr. Aronovich has served as an intelligence analyst and advisor on information gathering and filtering from Web intelligence and network sources in government and open source business and private sector intelligence.

Mr. Aronovich holds a BA in Government Diplomacy and Strategy from Interdisciplinary Center Herzliya, Israel specializing in terrorism and regional security.

Mrs. Orna Kenet-Guler

Since 1997, Mrs. Kenet-Guler has served in a variety of positions related to the development, writing and delivery of technical and operational information, documentation and hands-on training regarding Verint's intelligence system solutions.

Mrs. Orna Kenet-Guler has held positions of technical communicator, information coordinator, Documentation Team Leader and operational trainer at Verint Systems LTD, since its early days as Efrat Technologies Inc. in the early 1990's.

Mrs. Kenet-Guler has accumulated extensive know-how and an in-depth understanding of users' needs and operational requirements with major focus on the methodology and functional needs of analysts, operators and administrators. This results in user-oriented and task-oriented knowledge delivery tools such as applications online help and quality material for user training kits. Mrs. Kenet-Guler contributes her know-how and knowledge expertise to both online help and documentation tools, and to the content and scope of training materials, with special focus on providing material, tools and knowledge that support customers' modes of work, and facilitate the achievement of their organizational objectives.

Prior to joining Efrat Technologies, Inc., which subsequently became Comverse Infosys and then Verint, Mrs. Kenet-Guler worked as a professional translator, working in her native tongues, English and Hebrew, and focusing on business, marketing, legal and technological material. Mrs. Kenet-Guler's educational background consists of B.A. in both Business Management and English Literature from the University Of Jerusalem, Israel. Mrs. Kenet-Guler is also engaged in Translation Studies from Bar-Ilan University, Israel.

Mr. Joseph Mahaney

Since 2012 Mr. Mahaney has served as Director, Operations & Technical Support Services, for Verint Technology Inc., a leading provider of analytic solutions for communications interception, digital video security and surveillance, and enterprise business intelligence.

From August 2007 to November 2012, Mr. Mahaney has served as the Support Manager, North American STAR-GATE Solutions, for Verint Systems Inc., a leading provider of analytic solutions for communications interception, digital video security and surveillance, and enterprise business intelligence.

From 2007 to 2010, Mr. Mahaney was a part-time business student at the University of Maryland. He earned his MBA in May 2010 from the Robert H. Smith School of Business at the University of Maryland with a concentration in Information Systems.

From 2002 to 2007, Mr. Mahaney served in multiple Field Support Engineering positions for both Verint Systems Inc. as well as Verint Technologies Inc.; a cleared subsidiary of Verint Systems Inc.

Responsibilities included field installations, systems & network integrations and operational support of mission critical communication interception solutions for both law enforcement and major telecommunications service providers throughout North America. Mr. Mahaney is a US citizen and currently holds an active security clearance with the US Government. Joe currently resides in the Maryland area.

Mrs. Adi Drori

Mrs. Drori serves as a Senior Professional Services Specialist at Verint Technology Inc. Prior to that, Mrs. Drori was a Senior Software Developer. In her 18 year tenure with Verint, Mrs. Drori has served in many capacities including QA Engineer, Subsystem Product Manager and R&D Developer in several different software development teams. These responsibilities have ranged across all of the different Verint communication interception and intelligence solutions. The responsibilities included participating in all phases of the product life cycle pre-sales support, design, developing, quality assurance, installation deployment and training.

Mrs. Drori's education includes a Bachelor of Science in Mechanical Engineering from Tel Aviv University and many internal and external training classes such as: QA methodology , Telephony ,communications, C ++ programming ,web programming, databases and C# programming. Mrs. Drori is a US Citizen and resides local to the NY City area.

Mr. Ben Wheaton

In his 9 year tenure with Verint, Mr. Wheaton serves as a Technical Support Engineer for enterprise solutions & network integrations and technical resolutions for communication interception and intelligence solutions for both law enforcement and major telecommunications service providers throughout North America.

Prior to Verint, Mr. Wheaton worked for Future-Tech Inc., as a Technical Analyst supporting custom IT solutions for Enterprise clients. His responsibilities included Security, Networking and functioning installations and maintenance.

Mr. Wheaton's education includes a Bachelor of Science in Computer Science from Franklin Pierce University, where he graduated Summa Cum Laude. Advanced training includes many internal and external training classes such as: Telephony, communications, Network methodology and tools. Mr. Wheaton is a US Citizen and currently holds an active security clearance with the US Government. Mr. Wheaton currently resides in the NY City area.

George Busenberg

Mr. Busenberg has been employed by Verint since August of 2001 and works out of the Verint Gainesville, Virginia facility. Mr. Busenberg has held multiple positions in his 15 year tenure with Verint

which include Field Support Engineer, Tier 2 Engineer and Tech Center Subject Matter Expert. Mr. Busenberg's primary technology focus has been on lawful intercept solutions and intelligence systems. His main responsibilities include Product Planning and Design, Solution Implementation, Customer Training and Tier2 Support. Mr. Busenberg is a US citizen and currently holds an active security clearance with the US government.

Mr. Busenberg has a Computer Information Systems degree from James Madison University in Virginia. After graduation, George earned an MCSE and Cisco CCNA Certifications. He worked as a Windows Administrator prior to Verint.

6. *Where will the technical support resources for this implementation of the solution be physically located? Does the proposer have support abilities that operate within the U.S. Eastern Time Zone?*

Most of the technical resource supporting this implementation and system support will reside within the NY to DC corridor of the U.S. East coast.

7. *Please describe how the company ensures the proposed solution maintains pace with both policy and configuration changes applied by open source and social media platforms?*

This goes to the very heart of Verint's strengths. Verint invests about 20% of our annual billion dollar revenue in research and development. While no one can predict changes imposed by social media content owners as they provide or impede access to their data, what is critical is that BRIC align with a vendor with enough experience to anticipate changes and respond to them when they occur. One example is our ability to move from "Fire Hose" to API for content sourcing. While no vendor can honestly guarantee uninterrupted access to all social media content, Verint provides unparalleled experience in social media monitoring.

8. *Please describe how the company continues to innovate and update the proposed solution, to continue to provide value to system operators, in response to dynamic changes in technology, capability, availability of data (and nuances to volume, variety and velocity), tradecraft applied by criminals, and the threat environment?*

Clear and quantifiable examples of Verint's ability to evolve our solutions can be demonstrated by identifying just a few of the major enhancements we've made to our Open Source Information platform in the prior two quarters. Version 7 of our software, which is included in our proposed solution to BRIC, includes updates and upgrades such as:

- **Improved AVATAR management.** Recognizing the unique requirement of law enforcement to maintain the anonymity of agents during investigations, we have enhanced our avatar profiling tools and improved our human emulation protocols.
- **Significant improvements to Secure Web Browsing.** We've implemented a unique way to extract content on-the-fly while browsing the Web. The analyst can either manually capture specific items or an entire page and report it as insight or automatically issue a collection request for the relevant page data or the whole site using the WebInt-COLLECT platform.

5.2.2 Plan of Services – Delivery & Implementation (RFP Section 8B)

1. ***Please describe the project management and implementation process approach. How does the proposer manage the implementation of projects like this? How long will the implementation of the proposed solution take? Please provide details of estimated timelines for each phase of the project (i.e., discovery, initiation, planning, execution & control, closure, evaluation; installation, configuration, testing, training, initial solution operation by operators [hand-off], independent operation by operators [optimal proficiency of operators]).***

A detailed description of our project management and implementation process approach can be found in [Section 4](#) of the proposal titled “Implementation Plan”, (4.1 through 4.7 for implementation) above as well as a detailed training plan which can be found in [Section 7](#) titled “Training Plan”, of our proposal below. Timelines of each phase are wholly dependent upon customer system configuration requirements (turnkey or otherwise), customer network security needs and other factors which are not completely known until final contract. The implementation milestones outlined in Section 7C of the RFP are considered fully achievable.

2. ***Will the implementation team require access to onsite networks and/or data facilities? Will secure, remote access to the onsite network be required?***

A turnkey implementation will require access to onsite networks and/or data facilities to facilitate the installation, implementation and testing of the overall solution. Secure remote access is also recommended during the implementation phase and can also serve to reduce the onsite time required for an effective implementation.

3. ***Please describe the hardware requirements, if any, necessary for operating the solution in the optimal manner? Please include detailed specs of specific types of recommended equipment, as well as options for top 3 (max) recommended configurations (if only 1 option exists, please provide only this option).***

[Section 2.13](#) of the proposal titled “The Proposed Solution for Boston PD”, details the recommended on premise solution configuration with hardware and software specifics.

4. ***Please describe the software requirements for operating the solution in the optimal manner (e.g., 3rd party software)? Please include all dependencies and detailed specs for browser types, version numbers, etc.***

[Section 2.13](#) of the proposal titled “The Proposed Solution for Boston PD”, details the recommended on premise solution configuration with hardware and software specifics. The latest version of Google Chrome browser is recommended.

5. ***Please describe any cloud-based solutions required for operating the solution in the optimal manner, as well as options for top 3 (max) recommended solutions.***

The Verint WebInt solution can include on premise hardware and software or can be implemented in the cloud by any customary hosting provider. [Section 2.13](#) of the proposal titled “The Proposed Solution for Boston PD”, details the recommended on premise solution configuration with hardware and software specifics however similar hosting services could also be utilized for this component if desired. The Verint WebAlert component is a SaaS solution only and is hosted on a US based resident cloud.

6. ***Please describe all services that will be provided by the proposer to securely connect the user of the solution to both at rest and streaming real-time open source and social media data via the solutions various tools and interfaces (e.g., social media "fire hose", servers, secure browsers, SSL and/or TSL protocols, communications protocols, etc.).***

Verint WebInt-COLLECT is an advanced data extraction and collection solution, capable of extracting data from vast amounts of web sites, by using one of the following techniques:

- a. Fire hose/API: Supports a broad range of social media channels, Twitter, YouTube, Instagram, Blog, Board, Tumblr, YikYak, Sina Weibo, VK, News, and Facebook. For sources with fire hose agreements in place (Twitter, Tumblr, and commenting platforms for blogs and websites), there is a very low latency between when the post is made and when the platform displays it. For sources with API access, there may be a short delay between when the post is made and when the platform receives it from the API
 - b. Crawlers - This solution supports web data extraction from virtually any HTML-based Web source, including social network sites, portals, forums, blogs, news, and more. Handles simple static HTML-based sites, rich dynamic Web pages, and even password-protected and dark websites.
7. ***What are the anticipated maintenance requirements, incumbent upon the purchaser (BPD/BRIC), for all 3rd party hardware, software and services over the next ten years, for optimal performance of the solution (e.g., Will server licenses need to be upgraded at a pace consistent with the manufacturer in order to run the solution in an optimal manner through its life cycle of updates/upgrades? Is this the intention of the solution provider?).***

[Section 4.8](#) of the proposal titled “Support Services Offered” outlines the support services proposed throughout the lifecycle of the solution. This includes hardware, software, updates and other ancillary services in order to keep the system running in its most optimal manner throughout its anticipated life cycle.

8. ***What types of training will be required for optimal performance of solution? Is there a separate training requirement for administrators, basic users, mid-level users and advanced users? How will the***

proposer facilitate this training (e.g., onsite training, instructor-led web-based training, on-demand web-based training)?

Section 7 of the proposal titled “Training Plan”, details the types of training that will be provided throughout the solution deployment. Our experience has shown that initial training which is followed by as much as 30 days operational use and then additional refresher training tends to serve the customers well by reinforcing the operational methods through repeated use and the ability revisit operational scenarios in a training environment.

9. ***Please describe the overall user interface and user experience of working with the proposed solution.***

Section 2 of the proposal titled “System Proposal” details the interface and overall user experience of working with both the Verint WebInt and Verint WebAlert systems.

10. ***Does the proposer’s organization have contracts with open source and social media data providers, allowing access to data? Do these contracts authorize the proposer’s organization to provide this data to third parties for purposes described in this RFP?***

The data acquired through our WebAlert platform is collected from publicly available APIs (with the exception of some Twitter data). Each one of those APIs has specific terms of use and limitations that the end users would have to abide to in terms of permissible use cases. For Twitter, there is a contract in place to acquire the data that also comes with limitations in terms of acceptable use cases that would have to be observed as well to remain within terms of use. Verint (or its suppliers and licensors) hold the permits and license required to provide the customer with access to such data for the purposes described in the RFP. If, and as applicable, in accordance with the terms of use of our service which is available on our website or will be furnished to you upon request.

11. ***How will the proposer’s organization ensure continuity of access to real-time open source and social media data for the purpose of this RFP?***

The WebAlert data sources are provided mainly through publicly available APIs which the social channel providers support for all public access. Provided that those APIs continue to be publicly available, the access to the open source data would remain intact. The WebInt data sources are provided through the integrating mechanisms as described in **Section 2.6** – “WebInt Collect”.

6 FINANCIAL STATEMENTS

Verint Technology Inc. is a wholly owned subsidiary of Verint Systems Inc. (NASDAQ: VRNT); a global leader in Actionable Intelligence solutions.

Actionable Intelligence is a necessity in a dynamic world of massive information growth because it empowers organizations with crucial insights and enables decision makers to anticipate, respond and take action. With Verint solutions and value-added services, organizations of all sizes and across many industries can make more timely and effective decisions.

Our Actionable Intelligence solutions help organizations address three areas of the market—customer engagement optimization, security intelligence, and fraud, risk and compliance—by capturing large amounts of information from numerous data types and sources, using analytics to glean insights from the information, and leveraging the resulting intelligence to help achieve their customer engagement, enhanced security, and risk mitigation goals.

Our Customer Engagement Optimization solutions help organizations enrich customer interactions, improve business processes, and optimize their workforces in order to enhance loyalty, increase revenue, mitigate risk, and manage operational costs.

Our Cyber Intelligence solutions help organizations prevent, detect, neutralize, and investigate crime, terror, and cyber threats, as well as protect people, property, and assets.

Our Fraud, Risk, and Compliance solutions help organizations prevent loss; comply with regulations; investigate cyber, retail, and financial crime; and help ensure continuity of business and protect private information.

Today, more than 10,000 organizations in 180 countries—including over 80 percent of the Fortune 100—use Verint solutions to improve enterprise performance and make the world a safer place.

Headquartered in Melville, New York, Verint is publicly traded on the NASDAQ Stock Market under the symbol VRNT and all of our publically disclosed SEC financial filings can be found here:

<http://www.verint.com/about/investor-relations/all-sec-filings/>

An up to date Verint Investor Relations Financial Presentation dated September 2016 is attached in the Appendix of this document.

7 TRAINING PLAN

When performing entity and target investigations, the definition, access to, and analysis of the collected information play a critical part in the success or failure of the investigation.

Analysts must have a good understanding, not only of the analysis tools, but also of the manner in which Web activities are handled, and how the collection process might affect their investigation. An understanding of the collection and analysis processes are a must when using the *Web Intelligence Center* tools. For this purpose, Verint offers tool-based methodology services, designed to help customers set up their systems according to their specific needs, and hone them to specific ad hoc requirements as they arise.

7.1 Available Professional Services

Based on its extensive know-how and experience in the intelligence field, Verint offers various professional services that help customer organizations set up or improve their intelligence collection capabilities:

- **WebInt-COLLECT Initial web flow setup** – Each system can be delivered with an initial set of fields/rules that are adjusted to the customer's fields of interest and requirements.
- **Migration** of common legacy collection systems existing at the customer sites, to ensure continued use of legacy systems and no loss of data.
- **Consultancy** – Guidance in defining web flows and overcoming problematic Web collection scenarios. Verint has extensive intelligence experience to help overcome intelligence blocks or difficulties in reaching the necessary sources and data.
- **Initial setup of WebInt-ANALYTICS ontologies and keywords** – Defining the appropriate ontologies and keywords for extracting and analyzing the necessary data is not always straightforward. Experience and expertise help create effective and efficient ontologies and keywords from the onset of initial system setup.
- **Virtual agent implementation** – The analysis environments rely on the subject-material and target-data gleaned from the Web. For this purpose, WebInt-COLLECT must be able to access relevant related activities, such as social networking sites and forums. The defined collection tasks must be able to overcome site-access and page-access obstacles, and then search for the requisite target-related data. Often, to access the home environment of social networks and forums, a virtual agent is used. Several agents can be used to conceal the web flow's activities and generate a cover for the collection activities.

- **Social engineering** – In some scenarios, social engineering is required to approach the target and retrieve the required information. Social engineering refers to the exploitation of vulnerabilities in human relations, to set up virtual relationships that provide the necessary access to closed sites and forums. For example, to approach a target on the social network, a fake character can be set up, with similar (or interest-arousing) profession, tastes, location, and other attributes that comply with the purpose of research. Various strategies are used to gain access to a target: trust-building scenarios, common interest or aims, gender-related characters, etc. are used to gain access as friends of the target, or of the target’s friends. Knowledge of social engineering activities is key to target research on the Web.

7.2 Methodology and Training

Methodology training and consultancy services are available at the time of system setup, or later on for advanced users, allowing analysts to develop and improve strategies for social engineering, creation of agents, and promotion of the investigation methodology using WebInt-ANALYTICS and WebInt-COLLECT.

Each training program is tailor-made to best suit the needs of each customer, and follow a progressive guideline to build the users knowledge according to their experience. Each program includes both operational training on each interface, as well as system management training, along with a methodological emphasis to achieve the shortest possible time to production and ensure the successful implementation of the WebInt Intelligence Center.

7.3 Proposed Training and Professional Services

Web intelligence is a dynamic field requiring deep understanding of the world of WebInt as well as domain expertise in analysis and investigation methods. The large amount of data harvested from the Web gets its operative meaning and becomes Actionable Intelligence only when efficiently analyzed. In addition, when performing entity and target investigations, the definition, access, and analysis of the collected information play a critical part in the success or failure of the investigation.

Investigators must have a good understanding, not only of the analysis tools, but also of the manner in which Web activities are handled, and how the collection process may affect their investigation. The methodology and understanding of the collection and analysis processes are a must when using the Verint® Open Source Web Intelligence™ – Collect tools.

For this purpose, Verint offers tool-based methodology services, designed to help customers set up their systems and organization according to their specific needs, and help them to specific ad hoc requirements as they arise.

Based on its extensive know-how and experience in the intelligence field, Verint offers various professional services that help customer organizations set up or improve their intelligence collection capabilities. The following plan describes the different sessions.

7.3.1 Verint® WebInt Training – Analytics (10 Days)

	Description	Topics
Day 1	Overview and Intro to Verint® WebInt™ - Analytics	Opening Session About the course, Supporting Training Materials
		Introduction to the Web Social Networks, Forums, News Sites, Dark Web
		Web Search + Exercise Search techniques, Search engines, Basic Search, Advanced search
Day 2	Verint® WebInt™ - Analytics Operational	Web Search + Exercise Web search- hands on, URL and Keywords investigation exercise
		Verint® Open Source Web Intelligence™ overview General architecture, Analytics concept
		Verint® Open Source Web Intelligence™ – Collect overview Collect flow, Web flow protection
Day 3	Verint® WebInt™ - Analytics	Quiz & Recap
		Introduction to Verint® Open Source Web Intelligence™ – Analytics System workflow, System architecture, Basic terminology
		Administration Basic concepts, Creating sections, Creating a virtual agent, FA Administration messages, Creating agents exercise, Creating sections (Hands on), Section Scheduling, Information Monitoring
Day 4	Analysis Methodology	Quiz & Recap
		Operational workflow – Build your own dashboard Using widgets, Alert list, Search, Slice & Dice, Tabs
		Operational workflow cont. Ontology libraries, Hands-on
Day 5	System Operation	Quiz & Recap
		Exercise: System Search
		Viewing the VLA maps Map types, Editing maps, Exporting maps
		Tool Bars Persons & Cases (Hands on), Exclude Phrases (Hands on)
Day 6	Analysis	Recap
		Intelligence Cycle EEI, Research document
		Workflow and role definition

	Description	Topics
		The Analyst, The Administrator, The Team Manager
		Hands On
Day 7	Research & Collection	Quiz & Recap
		PPT & Exercise: Research
		Target Analysis (Hands On) Finding new identifiers, Mapping routine, Identifying links
		Hands On (Includes Collection)
Day 8	Research & Collection	Topic Analysis (Hands On) Mapping hierarchies, Identifying key roles, Identifying links
		Hands On (Includes Collection)
		Dead Ends
		Hands On (Includes Collection)
Day 9	End to end investigation	Exercise: End to end investigation
Day 10	End to end investigation & Summary	Exercise: End to end investigation – cont.
		Summary session Analytics flow, Summary session, Executive session (optional)

Methodology training and consultancy services are available at the time of system setup, allowing investigators to develop and improve strategies for social engineering, creation of agents, and promoting the investigation methodology using Verint® WebInt Further Professional Services activities can be added at additional costs.

7.3.2 Verint® WebAlert Training

Day 1: Introduction & Background

- Introduction and course goals
- Web Intelligence 101
 - o The intelligence process
 - o The OSINT domain
 - o Types Investigation
- Introduction to the WebAlert system
 - o System demo
- Structure of information on the Web
 - o Google land, Deep Web & Dark Web
- Social media
 - o API

Day 2: WebAlert Workflow

- WebAlert sources
 - o Short description of each one of the system supported channels
- Collection
 - o Queries
 - o Hands on
- Processing
 - o Live Monitoring
 - o Flagging
 - o Subjects
 - o Hands on
- Analysis
 - o People
 - o Knowledge maps
 - o Hands on
- Setting up queries for hands on practice

Day 3: WebAlert Workflow Continued

- Notifications
 - o Alerts
 - o Hands on
- Advanced features
 - o Historic search
 - o Hands on

Day 4: Operational Hands On

- Live work on organizational intelligence needs, with guided support and periodical statuses

Day 5: Operational Hands On Continued

- Presentation of summary intelligence products

Closing remarks & feedback

7.3.3 On-Site Analyst Training

Training will be conducted on selected topics based on customer needs (to be defined at a later stage), from among the following items:

Description	Topics
<p>Preliminary Research & Topic Analysis</p>	<p>The Internet (history & structure) TCP/IP protocol Web 2.0 Websites Browsers (features & add-ons) Search engines Dark Net Exercise: Topic analysis</p>
<p>Source Development</p>	<p>Social networks SNA (Social Network Analysis) Target analysis Organizing sources Building monitoring plan Exercise: Online SNA tools</p>
<p>Agent Management</p>	<p>Planning an agent (considerations & limitations) Registration to social networks API advanced Exercise: Agent creation</p>
<p>Collection</p>	<p>System architecture Web flows Collection requests Exercise: Facebook reconstruct & Twitter streaming</p>
<p>Processing</p>	<p>Filtering Widgets Ontologies Alerts Ignore phrases [Optional: Geo search] Exercise: Widgets functionality</p>
<p>Analysis</p>	<p>System hierarchy (Cases & Persons) Social Circle VLA (Visual Link Analysis) Exercise: Target enrichment</p>
<p>Reporting</p>	<p>Intelligence writing methodology Export feature Exercise: Report generation</p>

Administration	System maintenance Troubleshooting 101 Integrative summarizing exercise: Web Intelligence operation
-----------------------	--

8 SPECIFICATION SHEETS

The following Verint specification sheets can be found in the Appendix.

- 1) Web Intelligence Center Brochure
- 2) Web Intelligence Center Executive Briefing
- 3) Web Intelligence Center Presentation
- 4) WebAlert Brochure
- 5) WebAlert Executive Briefing
- 6) WebAlert Presentation
- 7) WebAlert Product Description

9 REFERENCES

Due to the non-disclosure agreements and required confidentiality that our customers expect for this type of sensitive solution – the same confidentiality which Verint will provide to BRIC -; we are unable to disclose most of our customers' names or contact persons as references, but we can share with you the following general information and provide you with one large enterprise customer as a US-based reference.

Verint's Web Intelligence Center serves over 30 different active organizations in over 20 countries in all regions of the world that are actively using the solution for Web data harvesting the deep and the dark Web, Web monitoring, analytics and investigation. Proposed solutions similar to that being offered to the BRIC are being used by law enforcement agencies in their criminal intelligence units (including those fighting drugs, pedophilia, human trafficking, etc.), anti-terror units, cyber defense at national intelligence levels, financial fraud prevention in government and private enterprise, customs, immigration and border control among others. These Verint solutions also support related deployments for Non-Governmental Organizations (NGO's) and large private enterprise customers using our social media monitoring platform for public safety as well as for protection of assets, IP, and senior executives. All prior Web Intelligence deployments are still in use.

Existing non-disclosure and security agreements now in place with these customers prevent Verint from identifying specific users and user profiles in a public document. However, we can disclose the following:

Verint's Webint Center serves mainly 3 types of customers:

- Law Enforcement Agencies (LEA)
- National Security Agencies (NS)
- National Intelligence Agencies (NI)

In addition to the government agencies described above, Verint also supports a large domestic U.S. enterprise customer that has volunteered to act as a direct reference for Verint and will allow an on-site demonstration in the United States.

US Domestic Enterprise Customer: This customer makes use of the platform in the following ways:

Global Security (GSOC)

- Identify, monitor and alert on protest activities, work related incidents and other events
- Geofence locations to monitor for 'chatter' relative to threats
- Monitor for negative information about executives, people and other company assets
- Proactive approach to intelligence gathering and dissemination

Global Security Intelligence & Investigations

- Aid in Global Security investigations related to product, personnel conduct and due diligence profiling.
- Generate investigative leads.

- Identify work related material or posting during work hours
- Harassment of individuals using open sources and company owned equipment
- Defamation of corporate name and products on open sources

Global Security Information Security

- Monitor and identify information leakage on the surface, deep and dark web

Forensic Investigations

- Insider threat identification such as users behaving strangely
- Individuals working for other companies in conflict with our charter as well as potential FCPA violations
- Searching for email addresses and builds evidence of whom they are associated to
- Suspicious companies and their activities
- Relationships in conflict with corporate policies

Threat Intelligence

- Forums, groups or individuals discussing zero day vulnerabilities, targeted campaigns against us
- Registration and use of domains similar to ours and our products. This could be an indication of a new campaign targeting us or counterfeit products
- Following known actors/groups related to cyberattacks
- Information released either directly or indirectly against us or our colleagues such as user names, email addresses and passwords

** Additionally, this customer has volunteered to act as a direct reference for Verint and will allow an on-site demonstration within the United States.

International Federal Law Enforcement Customers:

Two individual, centralized National Police Agencies in Africa whose mandate includes communications interception and intelligence, all signals intelligence as well as Web intelligence and various tactical solutions are using the Verint Web Intelligence Center Solution as a central component of their crime fighting arsenal. Their purpose is to provide intelligence solutions and technologies to the various domestic police units and they are doing so by leveraging the power of the Verint Web Intelligence Center solutions to collect data and enrich other data sources into one integrated intelligence picture. The system is used anonymously to collect information from the Internet (open, dark and deep Web), integrate it with other open and proprietary databases such as crime records database, vehicle registration database, population database, border control database and other public and private sources to generate intelligence insights in order to prevent crime or to solve ongoing criminal investigations. These two deployments have been such a great success that many other African countries are now following their lead.

10 INSURANCE REQUIREMENTS

The insurance requirements as identified by the City of Boston are acceptable as written. Attached please find a sample Certificate of Insurance which will bear the name of the City of Boston as the certificate holder or additional insured should we be the successful bidder on this contract.

<2 pages>



Sample COI
2016-2017.pdf

11 CITY OF BOSTON PROCURMENT FORMS (RFP SECTION 14)

11.1 Standard Contract & General Conditions (Form CM-10 & 11)

We have reviewed the standard contract & general conditions forms from the City of Boston and have the following comment:

“With regards to Sections 7.3 and 8 of Form CM 11, Verint’s standard policy with respect to limitation of liability (which we believe is quite industry-customary) excludes liability for indirect or consequential damages (except for cases such as fraud, injury, etc.) and limits Verint’s liability for direct damages to the amounts payable to Verint under the Contract. If the aforesaid is not agreeable to you, we propose to discuss this matter prior to contract signing and are certain that a mutually acceptable solution will be reached.”

11.2 Contractor Certification (Form CM-09)

<3 pages>



Contractor
Certification

11.3 Certification of Authority (Form CM-06)

<1 page>



Certificate of
Authority

11.4 CORI (Form CM-15A)

<2 pages>



CORI Form

11.5 Wage Theft (Form CM-16)

The following form has been completed and will be executed upon contract award.

<2 pages>



Wage Theft
Prevention

11.6 Living Wage (Form LW-2)

The following form has been completed and will be executed upon contract award.

<3 pages>



Living Wage
Agreement

11.7 Living Wage Affidavit (Form LW-8)

The following form has been completed and will be executed upon contract award.

<3 pages>



Living Wage Affidavit

12 PROFILE DOCUMENTS (RFP SECTION 3)

<3 pages>



Completed Section 3

13 MINIMUM EVALUATION CRITERION (RFP SECTION 11)

<2 pages>



Executed Section
11.pdf

APPENDIX

- 1) Financial Summary Presentation (Reference RFP Section 6 – Financial Statements)
- 2) Specifications Sheets (Reference RFP Section 8 – Specification Sheets)
 - Web Intelligence Center Brochure
 - Web Intelligence Center Executive Briefing
 - Web Intelligence Center Presentation
 - WebAlert Brochure
 - WebAlert Executive Briefing
 - WebAlert Presentation
 - WebAlert Product Description
- 3) Cashier’s Check for Bid Security Deposit