FORCEPOINT
POWERED BY Raytheon

Datasheet

SureView® Analytics Security Operations

INCIDENT RESPONSE INVESTIGATIVE INTELLIGENCE ENTERPRISE APPLICATION RAPIDLY MITIGATES THE COSTS AND RISKS OF BREACHES WITH A LOW TOTAL COST OF OWNERSHIP

FEATURES AND BENEFITS

- **Federated searching enables** availability of all pertinent information across the enterprise for response to a breach investigation. Analysts can immediately search all database servers, documents, file systems, web pages, e-mail servers and third party sources
- **Virtual data warehouse** environment eliminates the cost and burden of housing a massive set of duplicate data, and facilitates interdepartmental information sharing across the organizations. Data ownership issues are eliminated as the owner controls data access
- **Platform-independent**, graphical analysis tool is used to examine connections, system activity patterns, trends, associations and hidden networks in any number and type of data sources. Data is presented graphically, uncovering underlying relationships and patterns and addressing the entire analytical process
- **Use in-house resources** to rapidly respond to a breach. The immediate exploration for incident assessment across the security infrastructure is achieved quickly and easily with an established federated searching structure, automated data discovery technology and advanced analytical algorithms
- **Provide** daily information security intelligence briefs to management for a holistic view of the enterprise security posture by integrating investigative analytics into the existing suite of security intelligence systems

THE CHALLENGE

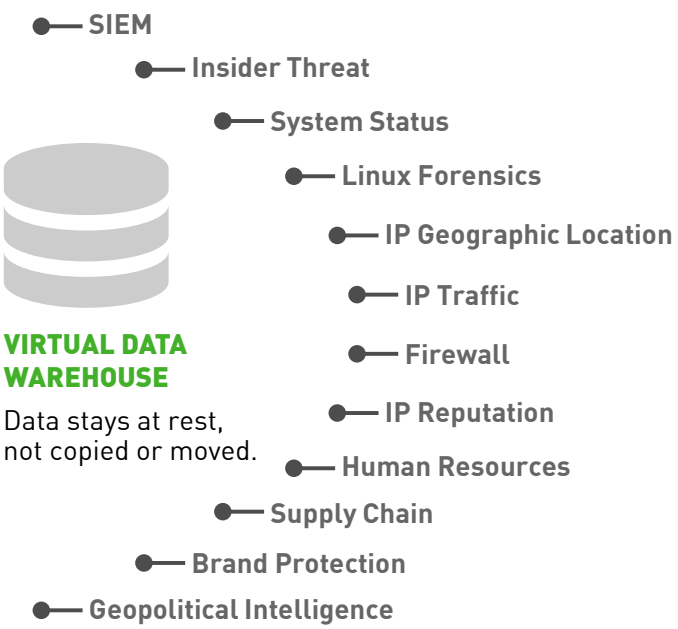
The challenge of long dwell times before eradication of a security breach is growing exponentially year over year due to multiple uncontrollable variables. We see an enormous increase in the quantity of cyber criminals world wide. What were traditionally purpose-driven hackers have turned into well-paid assets for financially motivated transnational cybercriminal networks. Having to confront big data during the assessment of a breach and throughout the investigation is both a benefit and a burden. Most importantly, the enterprise is facing an extremely sophi sticated adversary as hackers hone in their attack skills by leaps and bounds over time. As security officers are challenged with engaging in a plethora of investigations, we add the parallel component of the internal expectations of the organization on the security team to provide speedy incident response. The pressure on the timeliness, efficiency and productivity of security operations is at an all-time high. Security officers are looking to technology that quickly turns big data into actionable security intelligence for risk and cost mitigation of attacks, while maintaining a low Total Cost of Ownership (TCO) for the enterprise.

SUREVIEW ANALYTICS

SureView Analytics is a comprehensive cyber threat intelligence application for swift mitigation of the risk and cost of a security breach. SureView Analytics' federated searching technology rapidly accesses vast amounts of information located across the enterprise and returns relevant results as easily digestible pictures in seconds. SureView Analytics provides an advanced analytical

Figure 1: Federated searching across the enterprise coupled with automated discovery tools and investigative analytics results in security programs with intelligence-led rapid response to attacks.

environment that allows for comprehensive data visualization and cross-functional team collaboration resulting in a speedy response to sophisticated attacks (Figure 1).



VIRTUAL DATA WAREHOUSE

Data stays at rest, not copied or moved.

SUREVIEW ANALYTICS SEARCH

Federated searching seamlessly connects local and remote data sources to create the ultimate virtual data warehouse in order for analysts to have instant access to all data necessary to develop an all-inclusive picture of a situation. The timely process of internal approvals for access to information from multiple divisions across the enterprise is bypassed, as SureView Analytics' unobtrusive search capability does not ingest mass data into one central location. SureView Analytics does not copy the data source, but merely requests specific information across multiple sources, discreetly capturing key information across the enterprise simultaneously and securely with minimal impact or demands on the existing IT infrastructure.

- **Instantaneously search** live data across internal or external databases, websites, e-mails or office documents with the flexibility and scalability that the federated search technology offers.
- **Circumvent any costly demands of housing big data** with the unique virtual data warehouse approach to data aggregation. The technology mimics the outcome of a traditional warehouse while preserving the custody, security and physical ownership of the data on the original source (never copied or moved).
- **Comply with data privacy and security restrictions** via the integrated security manager, and identify options with unique permissions by individual user or group.
- **Quickly run search queries with minimized user interaction** through functionality that automates repeatable search processes.

Customize the types of results returned with full-text indexing designed with powerful search capabilities like phonetics and synonyms.

SUREVIEW ANALYTICS WORKFLOW

The system's advanced visualizations uncover information of interest impacting security operations. SureView Analytics' analytical workflow is designed to quickly map out connections that infected communications may have made, establish relationships among suspicious system behavior, and expose patterns, trends and anomalies in data. The platform optimizes a unit's productivity with automated data discovery, alerting functionality, and an integrated intelligence database to facilitate the understanding of large amounts of complex data and speed incident response to attacks.

Easily identify a bad host and other possible infected hosts with link analysis visualizations that map out the travel of suspicious communication across the enterprise.

Quickly bring forward suspicious behavioral patterns or unusual system conduct needing further investigation by laying out data as advanced temporal patterns.

Easily produce daily intelligence briefs and share situational awareness of the enterprise security posture with built-in reporting tools. Reports are easily ingestible as *drawing, labeling, legend* and *image import* features are centrally available for report customization.

Unearth important geospatial correlations of a breach due to its geographic location with geospatial visualization integrations.

Achieve rapid data discovery with faceted searching tools adding navigational searching in addition to direct searching to reduce the noise.

Enrich the data with metadata transformation tools that harmonize values of data by adding its real world meaning.

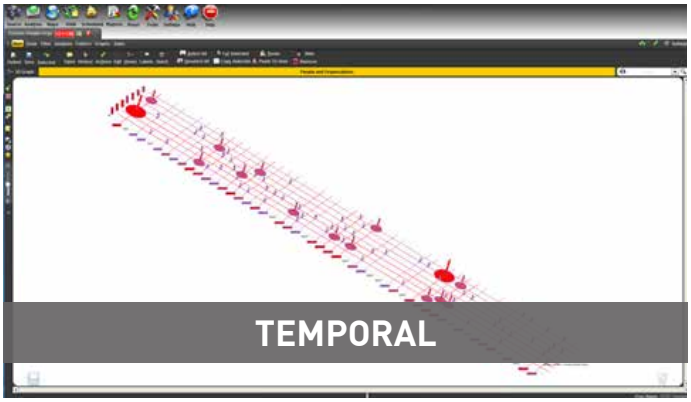


Figure 3: Temporal analysis. Quickly bring forward a change in behavioral pattern or unusual conduct needing further investigation by laying out data as an advanced temporal pattern.

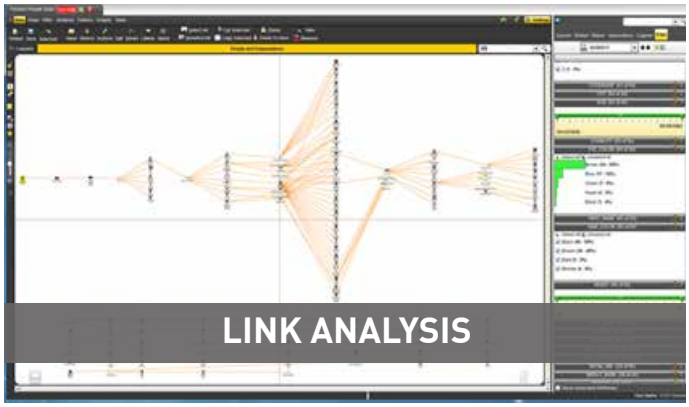


Figure 4: Link analysis. Understand the travel of possibly infected communications across the enterprise.

Figure 5: Geospatial analysis. Unearth an unknown relationship or importance of information due to its geographic correlation or location with geospatial visualization integrations.

Figure 6: Statistcal analysis. Identify unexpected peaks in activities or values with statistical representation of multisource data.

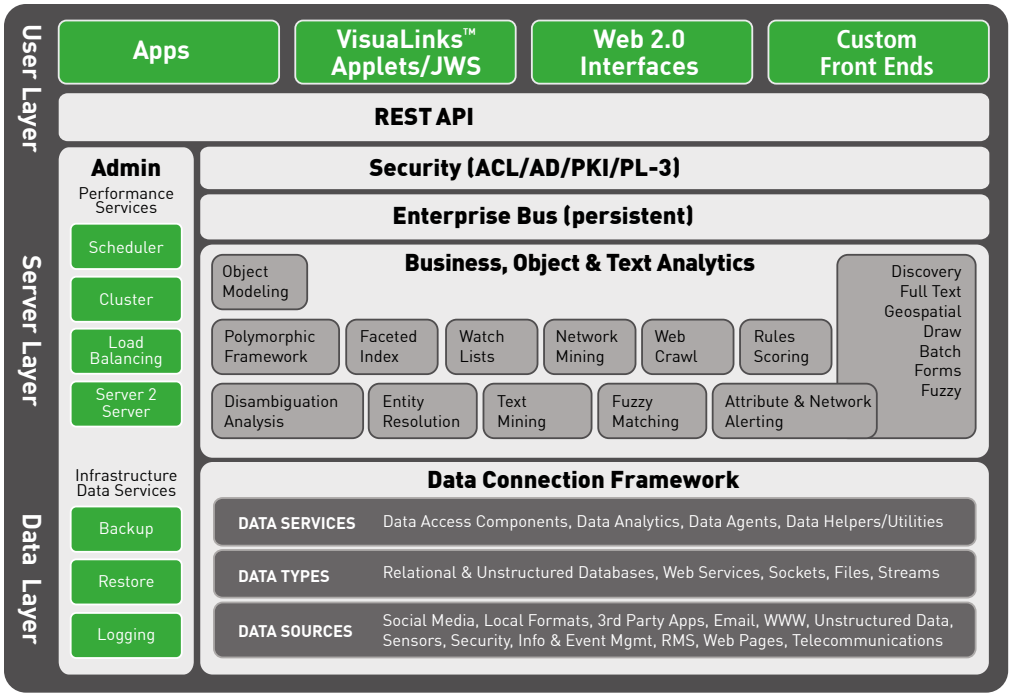


Figure 7: SureView Analytics platform. Federated searching across the enterprise coupled with automated discovery tools and investigative analytics for fast response to sophisticated attacks.

- **Minimal impact on the existing IT infrastructure**
- **Creates a "virtual" data warehouse**
- **Client-server application that uses commercial off the shelf hardware**
- **Optional Persistent Cache**
- **Runs on a virtual machine**
- **Easy to integrate with existing applications**

AN ENTERPRISE APPLICATION WITH A LOW TOTAL COST OF OWNERSHIP

The Forcepoint™ SureView Analytics platform has a low cost of ownership with minimal impact on the existing IT infrastructure. Unique to the industry, the technology connects directly to operational data stores and creates a "virtual" data warehouse, hence eliminating the need for IT to maintain yet another massive data warehouse as the data is never copied or moved. SureView Analytics is also a client-server application that uses Commercial-Off-The-Shelf (COTS) hardware, has an optional Persistent Cache that lets you publish content from any database without worrying about transactional load, can even run on a virtual machine and is easy to integrate with existing applications.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

Forcepoint™ is a trademark of Forcepoint, LLC. SureView®, ThreatSeeker® and TRITON® are registered trademarks of Forcepoint, LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks and registered trademarks are property of their respective owners.

[DATASHEET_SUREVIEW_ANALYTICS_SECURITY_OPS_EN] 100042.011416