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

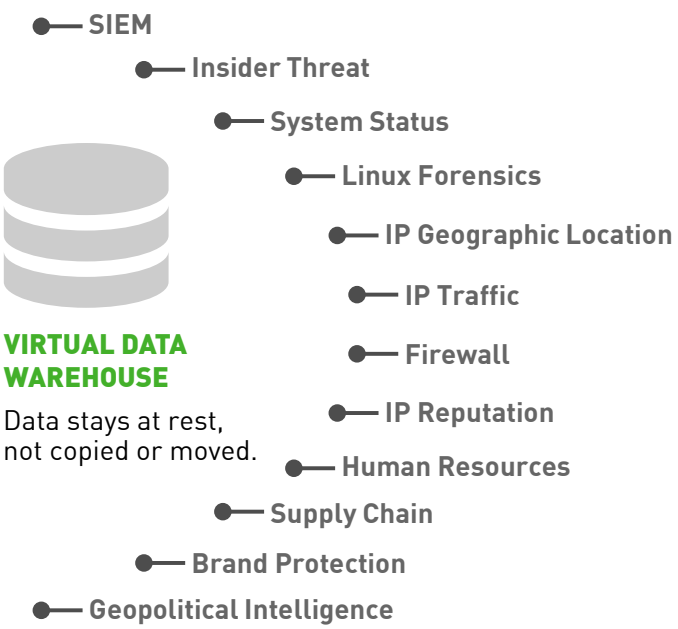
The challenge of long dwell times before eradication of a security breach is growing exponentially year over year due to multiple uncontrollable variables. We see an enormous increase in the quantity of cyber criminals world wide. What were traditionally purpose-driven hackers have turned into well-paid 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.

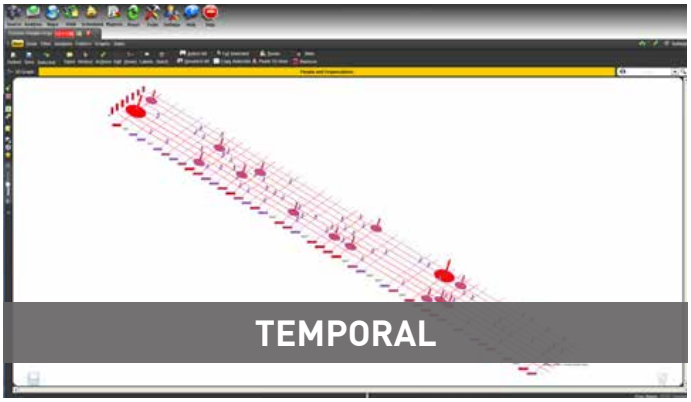


Figure 3: Temporal analysis. Quickly bring forward a change in behavioral pattern or unusual conduct needing further investigation by laying out data as an advanced temporal pattern.

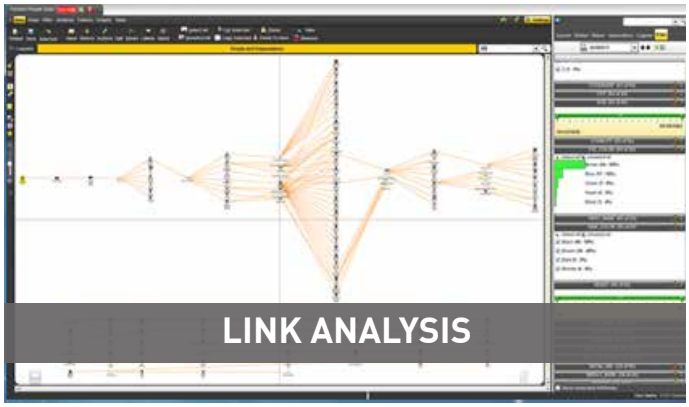


Figure 4: Link analysis. Understand the travel of possibly infected communications across the enterprise.

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.

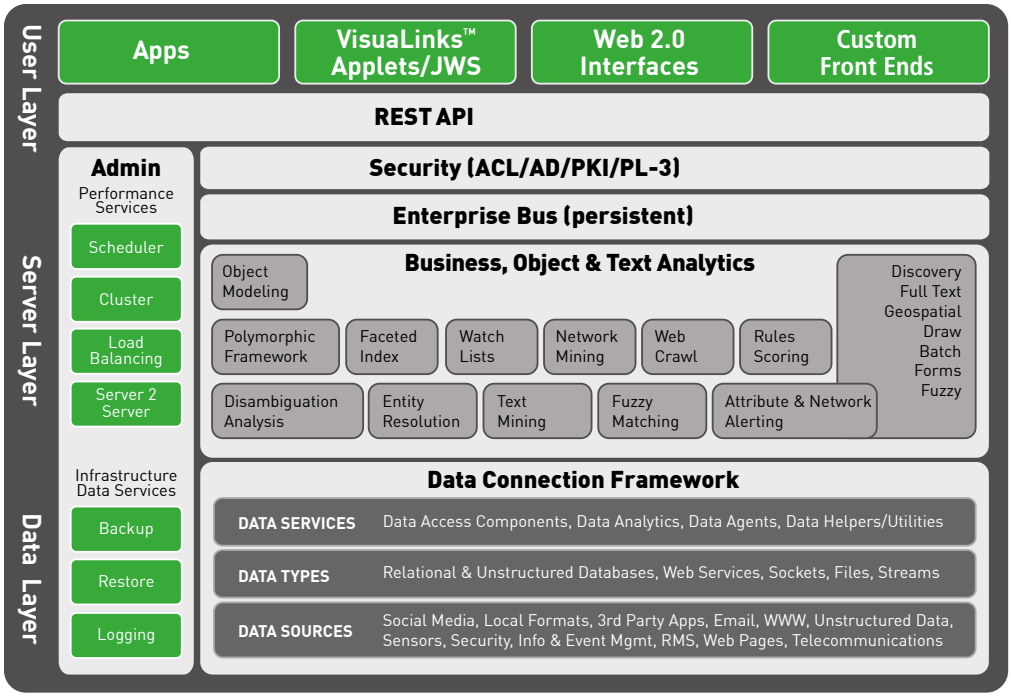


Figure 7: SureView Analytics platform. Federated searching across the enterprise coupled with automated discovery tools and investigative analytics for fast response to sophisticated attacks.

- **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

[DATASHEET_SUREVIEW_ANALYTICS_SECURITY_OPS_EN] 100042.011416

FORCEPOINT
POWERED BY Raytheon

Datasheet

SureView® Analytics Big Button 2.0 for Law Enforcement Solution

SPEED INVESTIGATIONS WITH AN EASY TO USE INFORMATION SHARING AND ANALYSIS PLATFORM PROVEN TO ENHANCE PRODUCTIVITY AND REDUCE CRIME

FEATURES AND BENEFITS

- **Retrieve** information from multiple data sources located across jurisdictions with federated search
- **Eliminate** massive data duplication and facilitate interdepartmental information sharing via a virtual data warehouse
- **Enable** granularity of access through multi-tiered security
- **Minimize** the quantity of working data with faceted searching
- **Enable** analytical teams to focus on analyzing instead of researching and collating
- **Visualize** and expose patterns in large amounts of data
- **Enhance** the accuracy and timeliness of intelligence with integrated geospatial, link, and statistical visualizations
- **Rapidly identify** connections between perpetrators and organizations with automated data discovery
- **Discover** hot spots for crime and quickly plot and analyze geographic and chronological data
- **Recognize** a low total cost of ownership with easy deployment and minimal impact on IT infrastructure

THE CHALLENGE

To be effective, law enforcement officials must constantly adapt to new situations, make greater use of intelligence, stay current with technology, and expand cooperation between agencies.

Today, organizations are fighting crime with tools that enable analysts and investigators to quickly access, understand, analyze, react to and share massive amounts of data across jurisdictions quickly and easily.

These information technology investments are enabling states to radically reduce criminal activity that impacts the public's safety. By providing advanced searching capabilities across vast amounts of information, agencies have access to critical information in seconds instead of what customarily takes days.

Searches are returned as actionable results by displaying information as: custom reports, lite link analysis, or geospatial visualizations- to ensure comprehensive situational awareness.

SUREVIEW® ANALYTICS BIG BUTTON 2.0

The SureView Analytics' Big Button 2.0 search solution is an agile, adaptable and scalable mobile-enabled federated search and visualization platform that boosts the speed, collaboration and efficacy of investigative and analytical divisions. It provides access to hundreds of sources that an organization deems mission critical and applies automation, advanced data discovery and visualization capabilities to rapidly deliver key insight to investigations. As individuals set and receive alerts to and from their mobile devices, they are empowered to immediately continue an investigation,

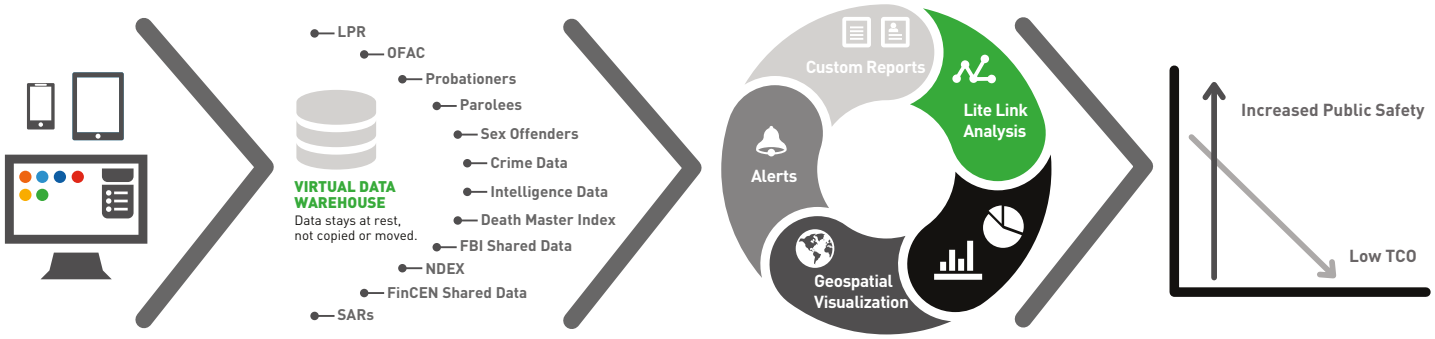
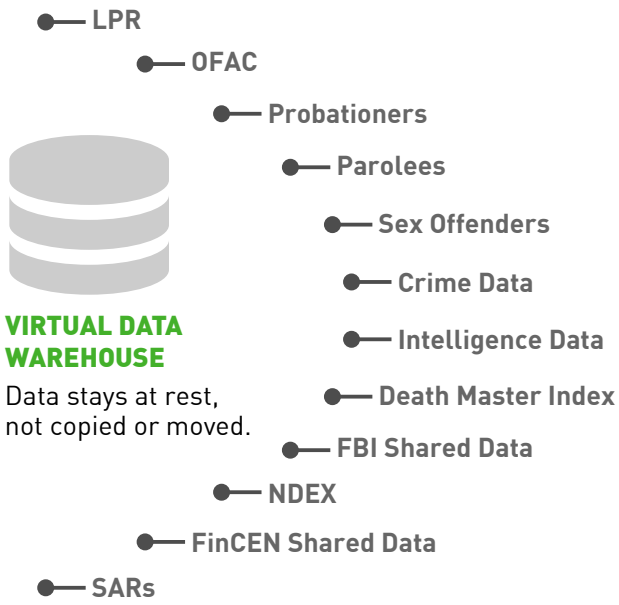


Figure 1: Federated searching across the enterprise coupled with automated discovery tools and lite-analytics supports intelligence-led law enforcement initiatives.

regardless of their physical location. The customizable and easy to use big button interface makes complex queries easy to run or schedule, delivering reporting and visualizations through a mobile device as confidently as it does on a desktop. Unique to the industry, the search technology does not need to duplicate data for processing, ensuring a low total cost of ownership and truly enabling information sharing, as the ownership of the data stays at the original source (Figure 1).



BIG BUTTONS

With decades of experience supporting law enforcement organizations world-wide, the platform comes with customized templates housing complex algorithms derived specifically in support of strategic law enforcement intelligence units. Time consuming and extensive search algorithms hide behind the friendly facade of a simple round button, bringing the capability of an advanced analyst to the fingertips of an entry level workforce. In addition to improving the accuracy and speed of a division's output, automating complex human-led processes eases the burden from the loss of subject matter expertise suffered by organizations with high turnover rates.

FEDERATED SEARCHING

Federated searching ensures that investigators and analysts have instant access to all data necessary to develop an inclusive picture of a situation. It seamlessly connects any number of local and remote data sources to create the ultimate virtual data warehouse that eliminates data duplication and enables effective information sharing. The timely process of cross jurisdictional and third-party approvals for access to information from multiple agencies is overcome.

AUTOMATED DATA DISCOVERY

Replace processes that require hours of human-driven big data collection, collation and correlation of information with automation, to reduce the amount of time dedicated to unnecessary investigations. Running active warrants against the publicly available Social Security Death Master File, for example, quickly identifies individuals with existing warrants that are actually deceased, therefore reducing the amount of time dedicated to unneeded investigations.

SCHEDULED SEARCHES

Substitute time-consuming manual routine searches with scheduled searches and make the platform your near real-time information asset. Scheduling repetitive complex searches takes the burden off the human analyst and allows their focus to remain on efficient actionable intelligence production using the latest information. Custom algorithms derived from decades of law enforcement support experience ensure investigators have the information they need at their fingertips while freeing up the analyst to focus on developing accurate actionable intelligence.

CUSTOM REPORTING

Provide researchers with the flexibility and uniqueness that enables them to maximize their work efforts with customized reporting capabilities that can be modified, sorted, prioritized

and scheduled. Arriving to one's shift with reports, run and populated in the optimal fashion that each unique individual needs for maximum performance, allows individuals to hit the ground running upon starting their shift or running new searches while on the road.

LITE LINK ANALYSIS

With lite link analysis visualizations of a search query on your mobile device, investigators can quickly deduce and act on next steps of a situation. Automated data discovery technology quickly unearths relationships between information stored across hundreds of data sources and returns information as actionable intelligence because it visualizes the associations between individuals, events, activities, locations, etc. enabling the investigator to naturally deduce progression of next steps of an investigation.

GEOSPATIAL

Geospatial representation of correlated data over time allows for the tracking of movement of assets or activities in a way that allows analysts to quickly see a change in pattern or behavior. Hot spots of activity or movement enable improved resource prioritization.

ALERTING

Today's investigators demand near real-time alerting to their mobile devices in order to take action quickly and easily. In tandem, alerting can be set up to several individuals participating within an investigation for instantaneous collaboration and progression.

CUSTOMIZABLE USER INTERFACE

This flexibility ensures compliance with organizational brand guidelines. The deployment of a graphical user interface and dynamic elements with a look and feel that is streamlined with the existing environment will accentuate a cohesive unit and reinforce its mission.

FAST AND EASY DEPLOYMENTS

Have your platform up and running quickly. Given the system's search architecture, deployments are fast. Organizations with knowledgeable database administrators can receive database deployment training and add sources to the search platform and expand the search capability independent of third party services as needed.

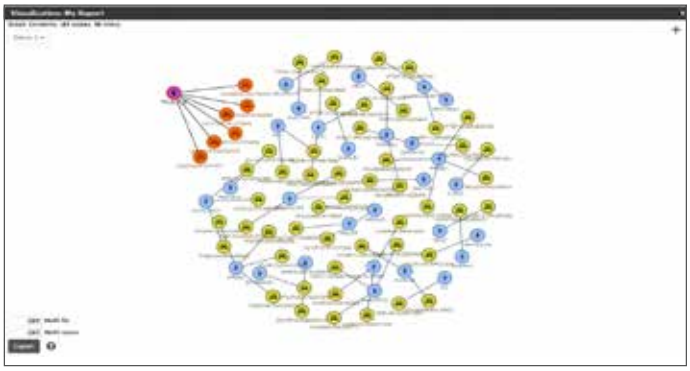


Figure 3: Quickly visualize previously unknown criminal associations on your mobile device.

Figure 4: Speed multiple investigations with customized reporting capabilities that can be modified, sorted, prioritized and scheduled.

Figure 5: Delivers the capability of an advanced analyst to the fingertips of an entry level workforce through simple to use big buttons.

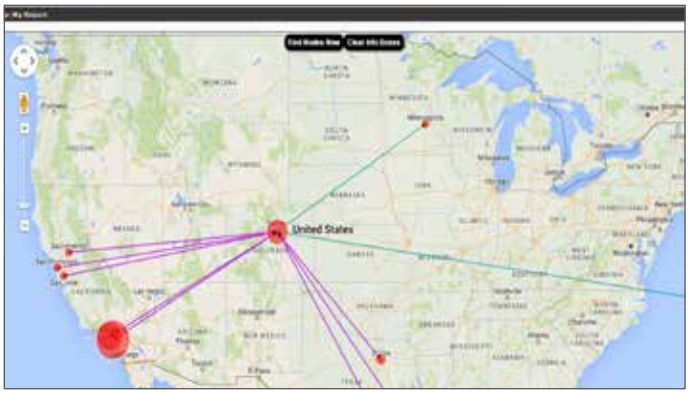


Figure 6: Track of movement of assets or activities to quickly see a change in pattern or behavior.

SEARCH TECHNOLOGY WITH A LOW TOTAL COST OF OWNERSHIP

The system resides on top of your existing sources, so there is no need to reformat or restructure your data; saving you valuable time and money while improving the quality and accuracy of your results.

- **Circumvent costs associated with housing big data** by implementing a virtual data warehouse approach (Figure 2). 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).
- **An infrastructure built to handle the typical big data problems** of incomplete, erroneous, and inconsistent types of data, but unlike most, we are still able to derive results and patterns out of the information. We can take imperfect and inconsistent information and still develop actionable intelligence.
- **Ownership of the data stays with original source.** Unlike other technology options, the data is not ingested into a proprietary database therefore ownership of the data stays with the data owner, reducing the need to share ownership of the data with a third party source which can create problems for the unit in the long run.
- **Comply with Law Enforcement Freedom of Information Act (FOIA)** requirements by leaving ownership of the data at the original source. Unlike other technologies that ingest data, SureView Analytics relieves the unit from legal responsibility of reporting on the data due to ingestion.
- **Instantaneously search live data** across internal or external databases, websites, emails or office documents. Other options will copy or move data as a batch import process overnight, leaving the analyst working with old data versus near real-time live data.
- **Comply with data privacy and security restrictions** via the integrated security manager, and identify options with unique permissions by individual user or group.
- **Customize the types of results returned** with full text indexing designed with powerful search capabilities like phonetics and synonyms.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_SUREVIEW_ANALYTICS_LAW_EN] 100038.011416