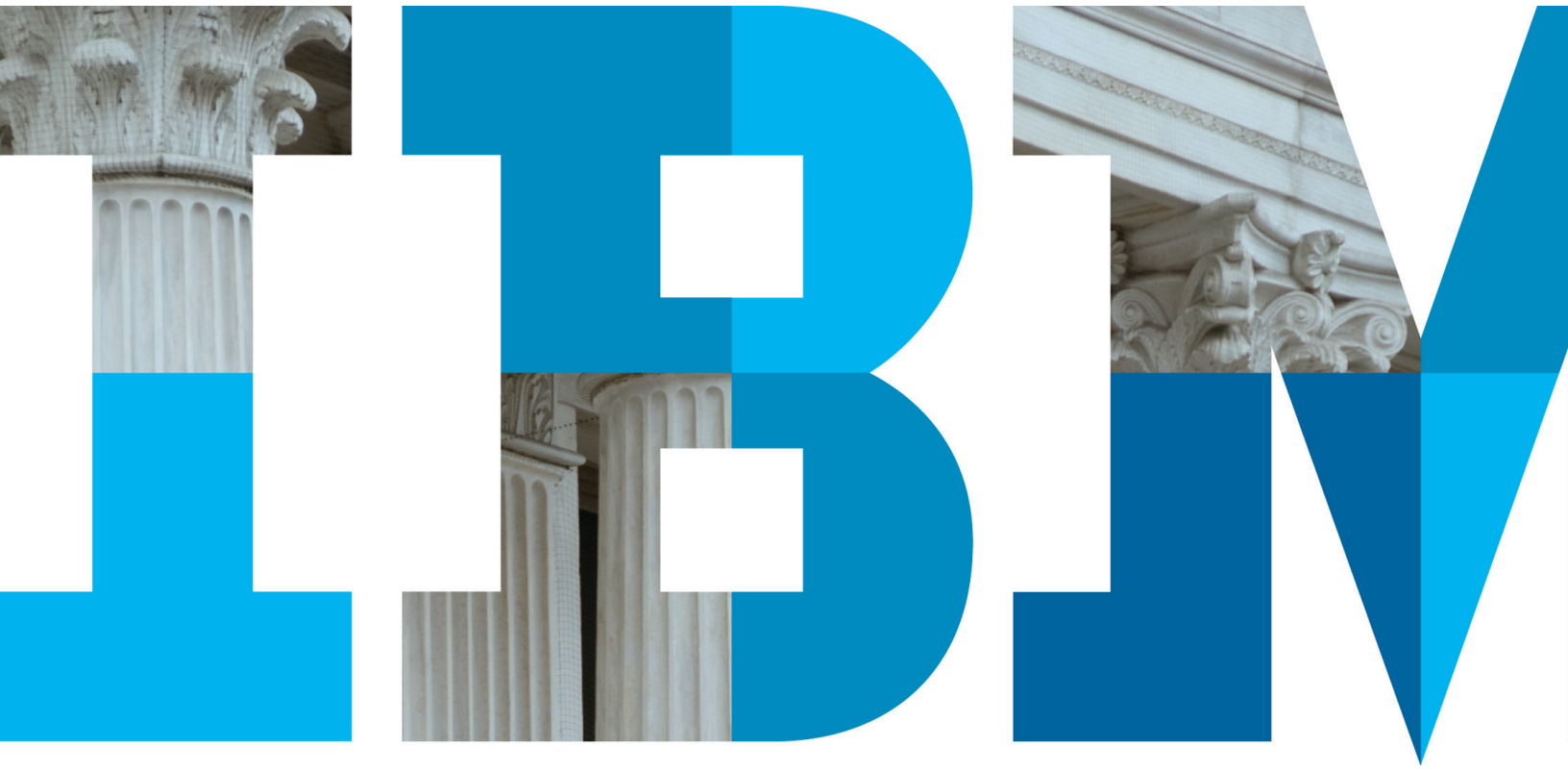
IBM Software
White Paper

July 2014

Extending government security intelligence with big data analytics and exploration

Confront evolving cyberthreats by enhancing traditional security methods



From cyber-espionage to cyber-warfare, the asymmetric nature of today's cyberthreats means that federal organizations face dangers from multiple fronts. For example, during fiscal year 2013, the US Department of Homeland Security logged 228,700 cyberincidents—more than 600 a day—involving federal agencies, critical infrastructure and the department's industry partners.[1] A recent US Government Accountability Office report stated that the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent over the past six years.[2]

Clearly, cybersecurity must be a top priority for governments around the world. In fact, during his 2013 State of the Union Address, President Barack Obama cited cybersecurity as a main concern for the United States.[3]

Unfortunately, traditional security measures alone are not enough to stand up to many of today's threats. Conventional cybersecurity methods are often predicated on a defensive mind-set and have significant shortcomings. They:

- Assume an explicit organizational perimeter
- Employ predefined attack vectors based on rules-signatures analytics instead of adaptable machine learning techniques
- Lack dynamic and adaptable real-time detection and characterization techniques
- Are optimized for combating external threats
- Presume that standardization mitigates risk
- Depend on general awareness of attack methodologies
- Require monitoring and control of traffic flows

As governments grow and change, cyber-perimeters are becoming increasingly blurred. While social media, mobility and the cloud increase opportunities for collaboration, they also bring greater risk and vulnerability by putting tremendous computing power into the hands of state and non-state actors. In this way, they open the door to a variety of threat factors, such as distributed denial of service (DDoS) and supply chain attacks, advanced persistent and insider threats (APTs), and sophisticated social engineering attacks.

Perhaps the most challenging aspect of all is the 360-degree nature of cyberthreats. As evidenced by a number of high-profile security incidents in recent years, attack vectors do not always come in the form of malicious code developed in dark basements. Rather, they might be privileged users with nefarious intent who simply bring a malware-infected mobile device through physical security to infect a system behind network defenses, or download classified documents onto a flash drive and walk the stolen intelligence out of the building.

To effectively combat this rapidly shifting threat landscape, it is clear that government agencies must utilize a comprehensive, 360-degree approach to protecting critical systems and infrastructure from all manner of threats. In addition, the platform supporting these capabilities must be flexible enough to grow and evolve based on known and zero-day threats. Economic realities dictate that these next-generation systems must be able to leverage existing investments in security assets. Today's buzzwords are "grow and enhance"—not "rip and replace."

But perhaps most important of all, security professionals must be able to establish unified visibility across all security fronts. They must be able to identify and correlate incidents, social media activity, video surveillance, geospatial records and sensor data—essentially all sources of data including data in motion—to proactively monitor, detect and prevent potential threats.

In short, they need big data and analytics.

Identify and protect against threats by building insights from broad data sets

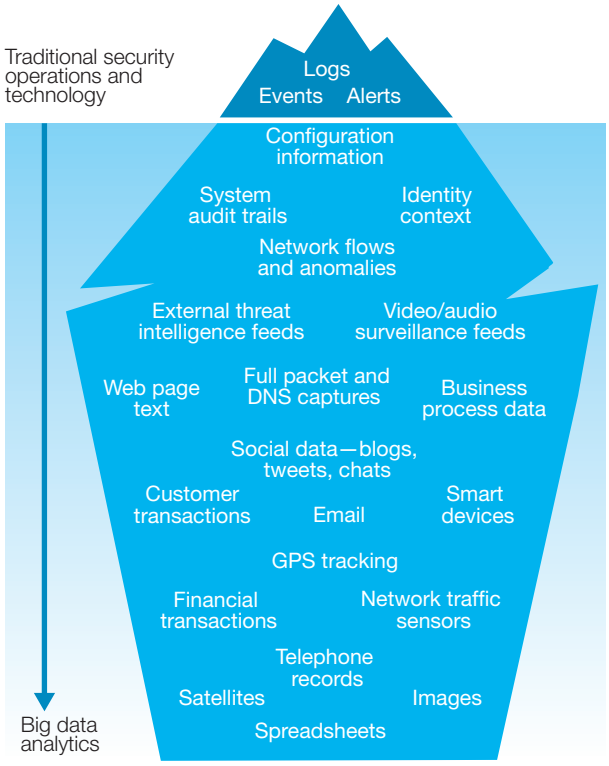


Figure 1. Data sources extend far beyond the most visible and traditional resources, but all of them should be mined for the most complete security intelligence picture.

Amplifying security intelligence with big data and advanced analytics

Big data solutions now enable government entities to analyze the world around them and not only react to security incidents, but also predict and take real-time action to prevent them. Big data and analytics present unique opportunities for government organizations to capitalize on data coming from a wide variety of sources to enhance their security systems. Data sources can include traditional structured data as well as new unstructured sources, such as logs, instrumentation data, network data, video surveillance feeds, geospatial information, social data and much more (see Figure 1).

Bolstering security intelligence with big data and machine learning analytics helps government organizations take advantage of large volumes of data from multiple avenues to anticipate and predict threats, and act on predictive analytics. It allows organizations to analyze constantly changing data in motion and perform sophisticated analytics on captured data. Big data solutions help extend traditional security measures, giving government security analysts the ability to:

- Analyze data at the millisecond level to understand, predict and act on security threats in real time
- Analyze a variety of nontraditional and unstructured data sets
- Significantly increase the volume of data stored for forensics and historic analysis
- Visualize and query data in new ways
- Analyze streaming data to keep up with the velocity of data
- Integrate with current operations
- Protect both physical assets and cyberassets, and correlate events
- Conduct behavioral and pattern analysis

Big data security solutions help security professionals sift through massive amounts of information—both internal and external—to reveal complex patterns and hidden relationships in seemingly unrelated people, data and events. In this way, organizations can gain deeper intelligence around security threats—and the ability to stamp them out.

The four pillars of comprehensive security intelligence

In the new era of comprehensive security intelligence, big data can help government agencies—defense, national security and civilian alike—support and extend traditional security measures in four key ways.

Protecting networks from probing and attacks: Intrusion detection

Effective network protection requires the ability to monitor network behaviors to detect known and unknown cyberthreats. Many types of threats (malware, botnets and others) can easily go undetected when transmission control protocol/Internet protocol (TCP/IP) volume is high and contains huge amounts of domain name system (DNS) traffic. To protect networks and identify such vulnerabilities, organizations must monitor all activity on a TCP/IP network to pinpoint anomalous activity—no small feat given current data volumes.

Big data and analytics can help organizations detect, identify and monitor network threats by analyzing a large amount of data in real time. Organizations can monitor all traffic—such as DNS requests, blacklists, whitelists and database access—to understand and proactively avert the threats.

Detecting data leaks and malware activity: Infection detection

Understanding data access and change history not only makes good security sense but also is required by many common industry and government mandates, such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX). To determine if data is being leaked, government organizations must monitor the information being accessed and determine if and what confidential or sensitive data might be at risk.

Big data and analytics enable government agencies to analyze usage patterns in large volumes of data to detect anomalous or changing behaviors, thereby signaling potential data compromise. For example, if an employee who normally accesses an average of 25 records per day suddenly spikes to 500, there may be cause for concern. Organizations can improve surveillance by leveraging new data sources and types, such as the Internet, satellite, video and audio, to make broader correlations and pattern matching possible.

Incorporating forensic, fraud and criminal intelligence: Attacker identification

Tracking criminals in real time to predict and prevent crime means monitoring various open and covert sources of information to determine:

- Who is talking to whom about what, and how
- What people think about a certain person, organization or government
- Whether threats exist among activities, locations, interests, and plans of persons and groups, especially those on a blacklist
- Whether there is any other suspicious content

To support these efforts, big data analytics can create insight into database activity patterns, call data records, web traffic, physical sensors and more. Advanced analytics on social media posts, geospatial information, text, images, videos and voice data help government agencies identify and predict behaviors to prevent crime.

Supporting and enhancing law enforcement efforts: Attacker identification and pursuit

Real-time data-mining analytics on the location parameters of forces or persons of interest can be obtained through geospatial location detectors, such as GPS-enabled cell phones, and can help authorities predict and proactively prevent their activities. Smarter surveillance includes powerful predictive analytics on multiple concurrent streams of structured and unstructured surveillance data, which can be drawn from such sources as manned and unmanned vehicles and security cameras in real time to alert law enforcement agencies of potential security issues. Blended with real-time name recognition and identity and relationship resolution, big data approaches can help law enforcers gain insight into cross-border and intra-border transactions.

The IBM Analytic Security 360° solution

A pioneer in big data analytic methodologies, IBM delivers a complete solution framework that enables government agencies to confront an evolving cyberthreat landscape. Most network security systems are designed to deal with a single aspect of the threat—such as detecting and eradicating malicious code, or recognizing activity anomalies indicating a potential attack. By contrast, IBM solutions marry the power of traditional security intelligence with the integrated analytics and exploration capabilities of big data and analytics—for a 360-degree approach to protection (see Figure 2).

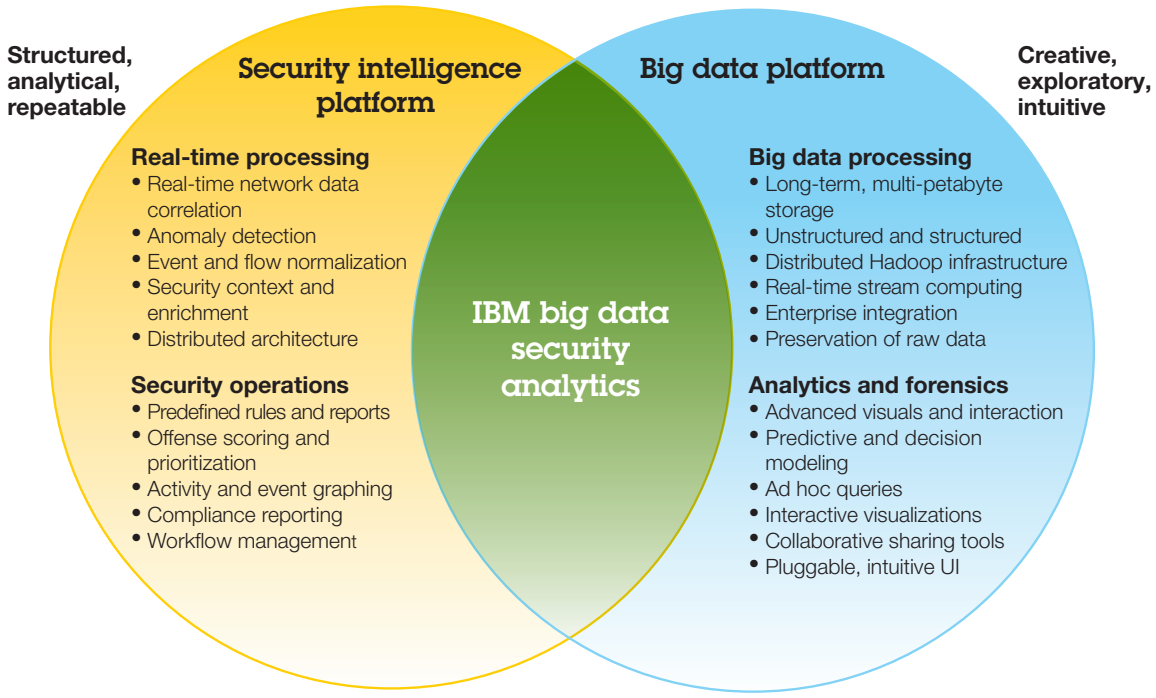


Figure 2. IBM integrates analytics and exploration in a new architecture.

IBM® Analytic Security 360° is a flexible, multi-technology solution built to help government agencies address not one, but multiple critical information system attack vectors—protecting agencies from all sides. Unlike products that confront only a limited aspect of a threat, Analytic Security 360° (AS360°) extends the security paradigm, tackling everything from sophisticated network intrusion and stealthy advanced persistent threats to continuous privileged user identity and activity vetting.

AS360° uses a framework-based approach that allows clients to leverage the industry's deepest, fastest-growing portfolio of analytic and big data capabilities. Designed to optimize existing security investments to address defensive blind spots, while evolving to meet changing security threats, AS360° enables governments to:

- Analyze and correlate broader data sets to prevent cyberattacks, fraudulent claims or account takeovers
- Enrich security solutions with email, social and other unstructured data to improve cyberthreat detection and remediation
- Better detect and monitor criminal and terrorist activity by correlating a broader variety of sources to uncover associations or patterns
- Enhance security and surveillance systems with real-time data from video, acoustic, thermal or other devices/sensors

IBM AS360° encompasses endpoint management, secure identity management, blocking, continuous monitoring, data masking, predictive analytics for anomaly detection, identity vetting, nonobvious relationship awareness, real-time analysis at the millisecond level, analysis of petabyte range data volumes, and the ability to analyze unstructured data.

The AS360° solution includes the following capabilities from the IBM portfolio.

IBM InfoSphere® BigInsights™ builds on the open source Hadoop framework to help organizations reliably manage large volumes of structured and unstructured data. With better management of and access to big data, organizations can more easily identify security threats. InfoSphere BigInsights also helps security analysts feed data into or store data from QRadar for greater contextual richness in data analytics.

IBM InfoSphere Streams is an advanced computing platform that enables continuous analysis of massive volumes of streaming data with sub-millisecond response times, enabling users to view information and events as they unfold—a must for security intelligence.

IBM Security QRadar® security intelligence platform is designed to consolidate log source events and network flow data from thousands of devices, endpoints and applications, helping analysts perform immediate normalization and correlation on raw data to distinguish real threats from false positives.

IBM SPSS® is predictive analytics software that delivers high-volume optimized decisions to frontline systems and decision makers. It can analyze multiple data sources to monitor for suspicious activity and help control outcomes to predict criminal activities and minimize exposure and loss.

IBM Identity Insight is an advanced entity analytics solution with sophisticated recognition algorithms optimized to help predict and preempt criminal activity faster. Identity Insight leverages advanced algorithms specifically optimized to recognize nefarious individuals and organizations in spite of their sophisticated attempts to mask their identity, their unscrupulous relationships and their activities.

IBM PureData™ for Analytics, powered by IBM Netezza® technology, is a smart data appliance for serious analytics. It streamlines and optimizes performance of data services for analytic applications, enabling complex algorithms to run in minutes instead of hours, delivering speed (10 to 100 times faster than traditional custom systems[4]), faster time to value (5 TB/hour load speed[5]) and simplicity.

IBM InfoSphere Guardium® and IBM InfoSphere Optim™ address data security and management. **InfoSphere Guardium Data Activity Monitor** provides centralized controls for real-time data security and monitoring, fine-grained database auditing, automated compliance reporting, data-level access control, database vulnerability management and auto-discovery of sensitive data. **InfoSphere Optim** provides a simple, robust solution for data lifecycle management.

Securing government agencies around the world

AS360° solutions are designed to help mission owners deploy powerful preventative network defenses, monitor the actions and identities of privileged users and build preemptive measures based on previous attack scenarios—for a comprehensive approach to cybersecurity.

IBM government clients worldwide are taking advantage of AS360° to expand their existing security approaches, and are seeing measurable results. For example, a defense agency used AS360° to detect more than 350 documents identified with the keyword "confidential" being transferred across its network. It also identified 43 infected hosts across hundreds of possible domain names, as well as over 900 Facebook accesses in a 45-minute window. Armed with this information, the organization was able to address these potential threats, tighten security measures and close the gaps in its existing cybersecurity profile.

Backed by the power of its comprehensive big data platform and industry-leading expertise, IBM is equipped to help government agencies like these—defense, national security, civilian and more—meet the challenges of today's dynamic cyberthreat environment. Find out how IBM can help advance your mission today.

For more information

To learn more about IBM big data solutions for government security, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/bigdata&analytics/operations-management.html

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2014

IBM, the IBM logo, ibm.com, BigInsights, Guardium, InfoSphere, Optim, PureData, QRadar, and SPSS are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Netezza® is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Actual available storage capacity may be reported for both uncompressed and compressed data and will vary and may be less than stated.

Please Recycle

[1] "Healthcare.gov: Stringent protections for security and personal information." U.S. Department of Health and Human Services Fact Sheet. January 7, 2014. www.hhs.gov/healthcare/facts/factsheets/2014/01/health-care-gov-security.pdf

[2] "ENISA Threat Landscape: Responding to the Evolving Threat Environment." European Network and Information Security Agency. January 8, 2013. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

[3] "President Barack Obama's State of the Union Address—As Prepared for Delivery." February 12, 2013. www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address

[4] Based on IBM customers' reported results. "Traditional custom systems" refers to systems that are not professionally pre-built, pretested and optimized. Individual results may vary.

[5] Based on IBM internal testing using IBM PureData System for Analytics N2001. Single rack load speed of 4.8 TB/hour, multi-rack load speed of 5.25 TB/hour. Assumes customer source systems and network can accommodate quoted load rates. Individual results may vary.

IMW14784-USEN-00