

Realizing Efficient Enterprise Security Intelligence by Using IBM Security Intelligence Solutions



Redguides
for Business Leaders

Nilesh Patel
Arun Madan
Sridhar Muppidi
Axel Buecker



- Understand the necessity of security intelligence in today's world
- Learn about the IBM Security Intelligence Solutions
- Follow a typical deployment scenario



Executive overview

No matter how large or small an organization, the demands for security intelligence are growing. Organizations of all sizes face tremendous challenges to keep their assets secure. Most organizations use heterogeneous IT technologies and software solutions that produce a wide variety of disparate data. Such technologies and solutions include compliance and vulnerability scans, IDS/IPS alerts, asset data, access logs, and more. They monitor and track network performance, monitor and track application security, and collect and manage event logs in an attempt to meet overall IT objectives. Also, compliance mandates are on the rise, and data threats and breaches continue to challenge organizations.

This situation is compounded by the large amount of data and events that are generated by an ever-increasing number of users and devices. Without finding new ways to stay on top of this data flood, an organization will be left vulnerable.

Security intelligence provides the means to analyze this enormous collection of data and deliver meaningful incidents to the right people. Security intelligence is not just nice to have; it is a necessity. Security intelligence is built on the same concepts that have made business intelligence an essential enterprise technology. It is the critical next step for organizations that recognize the importance of information security to their business health.

Too often, the response to new security threats is a “finger in the dam” approach with a particular point technology or reactive new policies or rules. This response is in large part because a unified security program, which is based on automated analysis of unified information from across the IT infrastructure, can be costly, complex, difficult to implement, and inefficient. As a result, most organizations lack accurate threat detection and informed risk management capabilities.

In this IBM® Redguide™ publication, you see how security intelligence addresses these shortcomings and empowers organizations from Fortune 500 companies, to mid-sized enterprises, to government agencies, to maintain comprehensive and cost-effective information security.

The need to know

C-Level executives are facing an enormous task to establish programs that bridge people, processes, and technology to minimize *risk*. The term *risk* can have a different meaning, depending on an individual's area of responsibility and industry in which they work. From an information security perspective, one of the top concerns for C-Level executives, IT executives, and security professionals is to reduce the risk of potential breaches of *information*. Your organization can be the next one to be added to Figure 1 if appropriate information security controls are not in place.

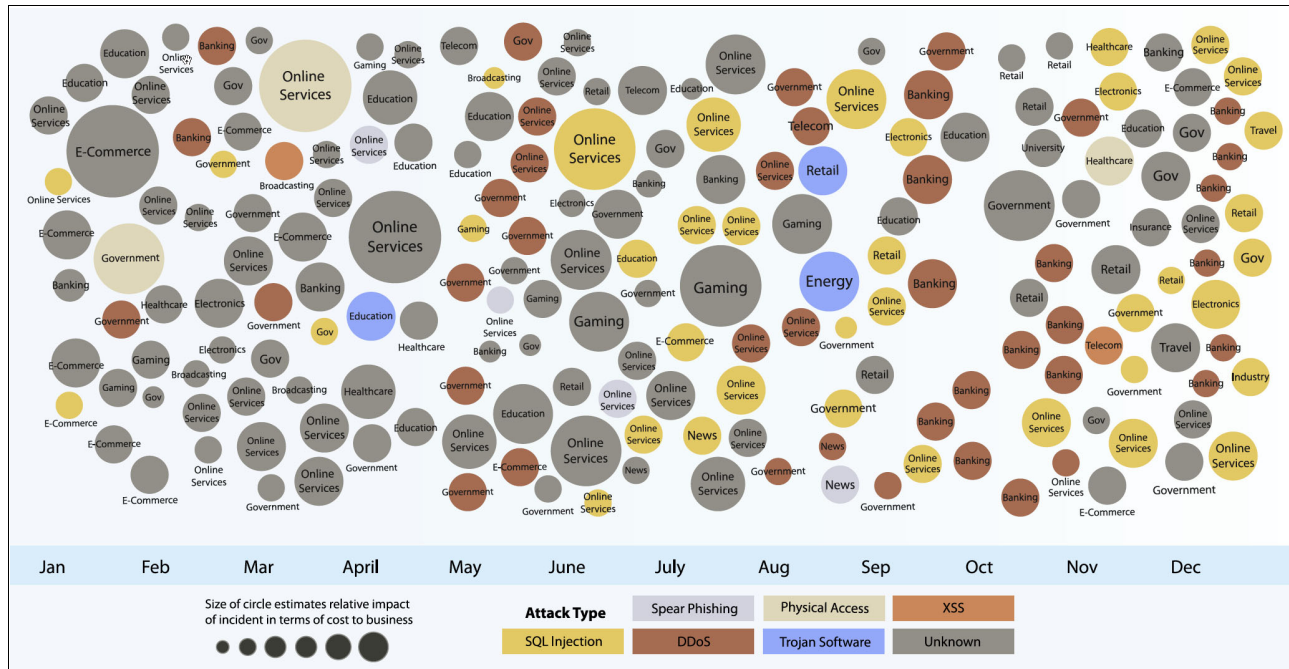


Figure 1 Sampling of 2012 security incidents by attack type, time, and impact (source: IBM X-force¹)

The diagram in Figure 1 shows that 2012 was the year of the security breach. It is based on reports about almost weekly wide-scale network security breaches, leaving a wake of leaked customer data, inaccessible web services, and billions of dollars of damages. Because of this impact, information security has become a board room discussion that affects business results, brand image, supply chain, legal exposure, and audit risk.

These 2012 incidents did not discriminate against any industry or sector. Law enforcement, governments, social network communities, retail, entertainment, banks, non-profits, Fortune 500, and even security companies were attacked. No single geographical region was the focus, but clearly these attacks occurred on a global scale. As the year came to a close, the trend showed no signs of slowing. December marked some of the largest impact-by-cost breaches that affected several massive social and entertainment sites in China, with billions of dollars of potential losses.

Most security professionals agree that the maturity of an organization's information security program is directly proportional to their ability to protect *information*. Compliance and regulatory mandates, in addition to security incidents, are the most prevalent business drivers for information security today. To properly address these drivers, an organization needs access to real-time knowledge about their risk posture. In today's malicious world, insider fraud and security breaches are rising day by day, and security is of the greatest concern for

¹ IBM X-Force© 2012 Trend and Risk Report, <http://www.ibm.com/services/us/iss/xforce/trendreports>

business executives. The world of information technology threats has changed from *targets of opportunity* to *targets of choice*.

The established *defense-in-depth* security model is no longer adequate to meet contemporary challenges, as Internet hooliganism has given way to organized and sophisticated criminal activity. It is outmoded and does not scale in the face of today's threats and IT environments. Perimeter-based security has evolved to a highly distributed model. As employees, business partners, and customers conduct business remotely across the Internet, criminals take advantage of new attack vectors and misplace user trust.

The four key areas of modern information security technology, as shown in Figure 2, include *advanced analytics*, *cloud computing*, *mobile computing*, and *regulation and compliance*. These areas keep chief information security officers (CISO) awake at night. This IBM Redguide publication takes a closer look at advanced analytics regarding information security using security intelligence.

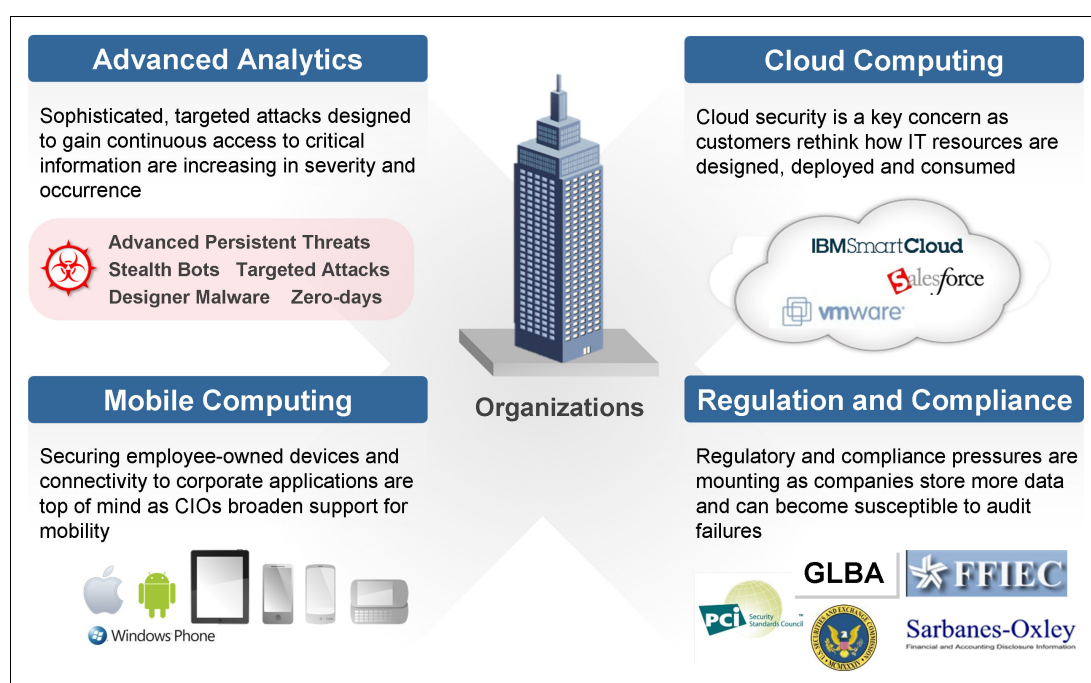


Figure 2 Key trends of new information security technology

Business challenges

The selection of the most effective IT technology is a major concern for organizations of all sizes and across every industry. In the current economic climate, organizations face the difficult task of prioritizing where to best spend their limited budgets so that they emerge from these uncertain times as strong and viable companies.

Feeling this pain most are those companies that deliver critical network services and applications. Regardless of adverse economic conditions, they must still meet various requirements, such as the following examples:

- Meet evolving and increasing numbers of regulatory mandates.

Over the last few years, the burden of regulatory compliance has grown significantly and affected nearly every industry. The list of regulations is long and the potential penalties for non-compliance are significant.

This list includes the following regulations:

- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley (SOX)

Many regulations continue to evolve with significant impact across organizations.

Penalties for non-compliance vary from industry to industry. However, a common thread across all industries is that non-compliance can significantly impact the bottom line. Because the financial penalties and inherent security risks have become easier to quantify, organizations have become more acutely aware of the risks and costs of noncompliance. Conventional wisdom dictates that organizations *do the right thing* and implement common sense controls to best protect corporate IT assets. The reason is not only to meet regulatory requirements, but also to protect mission-critical business data.

- Secure IT assets from continually evolving threats.

Security professionals are keenly aware of the growing risk of threats from inside and outside the organization. News stories have emerged about complex and sophisticated crime operations that are behind some of the more significant breaches that have occurred. And the lengths to which criminals have gone to steal computer-based information in the past few years are almost unimaginable.

As a result, significant resources have been invested to investigate and respond to major security breaches that have compromised millions of confidential records, including credit card data, healthcare information, and proprietary intellectual property. The ramifications of any network security breach to an organization are far-reaching, and post-breach cleanup costs are significant. Organizations need to be prudent and implement proper security controls that will put them ahead of criminals and help them to detect complex, integrated attacks on their networks.

- Develop security controls for existing and emerging technology solutions.

An ongoing challenge to IT organizations is that networks are in a constant state of change. New technologies arrive as old technologies depart. Organizations must continually assess how new technologies impact their IT security program and ensure that the proper controls are in place to meet the security requirements of the business. In a challenging economic climate, organizations must look to solutions that meet the security requirements of their business and that also reduce overall costs. Organizations need to be selective in the acquisition of new technologies. For example, virtual and cloud computing is one of the most transformative advances in computing history, but it exposes an organization to new risks.

Difficult, economically driven choices must be made, and organizations need to be strategic in selecting the solutions that they will deploy.

Security intelligence

For high performance organizations, understanding how to put *information to work* is a key to excel in business. With the help of the automated use of business intelligence technology, they apply analytics to extract maximum value from the massive amount of data that is available to them. A similar approach should be applied to securing that *information* by implementing a *security intelligence* program. Just as business intelligence helps enterprises

make decisions to maximize opportunities and minimize business risks, security intelligence can enable them to better detect threats, identify security risks and areas of non-compliance, and set priorities for remediation.

The case for business intelligence is compelling. It enables organizations to support their critical decision-making by automating the data analysis processes at a level that manual analysis can scarcely approach. By applying computer-based business analytics to their unique environments, successful organizations derive the greatest possible value from their amassed terabytes and petabytes of data, from sales revenue and customer demographics to the cost of shipping and raw materials.

The case for security intelligence is equally, if not more, compelling. Enterprises and government organizations have access to vast quantities of data that can help detect threats and areas of high risk, if they have the means and the commitment to collect, aggregate and, most importantly, analyze it. This data comes from point security products and from other sources, such as network device configurations, servers, network traffic telemetry, applications, and users and their activities.

In today's security operation and technology implementations, the available information is only as good as the tip of the security data iceberg. It only reveals the small evident part of something much larger that is hidden from the casual view. Because attackers are constantly finding and using sophisticated techniques to bypass traditional defenses, there is a need to use next generation security operations and technology, which should collect and store massive amounts of security data as illustrated in Figure 3.

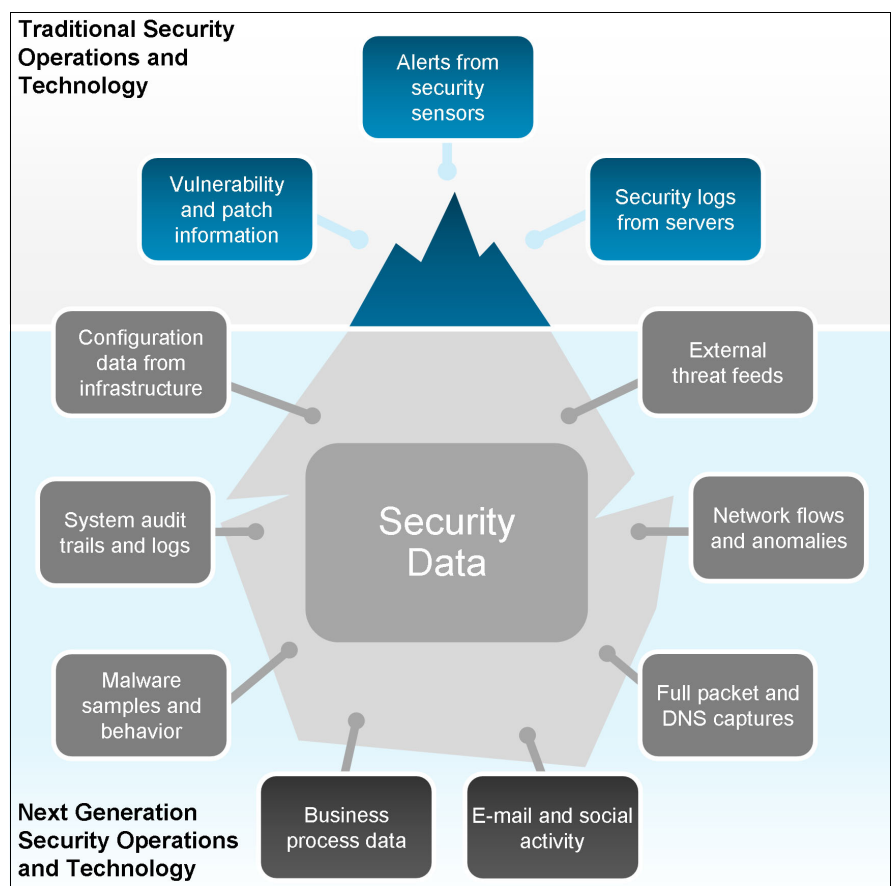


Figure 3 Security data iceberg

This collected massive amount of security data is of no use if no helpful insights can be derived by using analytics and decision modeling. This situation is where security intelligence comes into play, as shown in Figure 4.

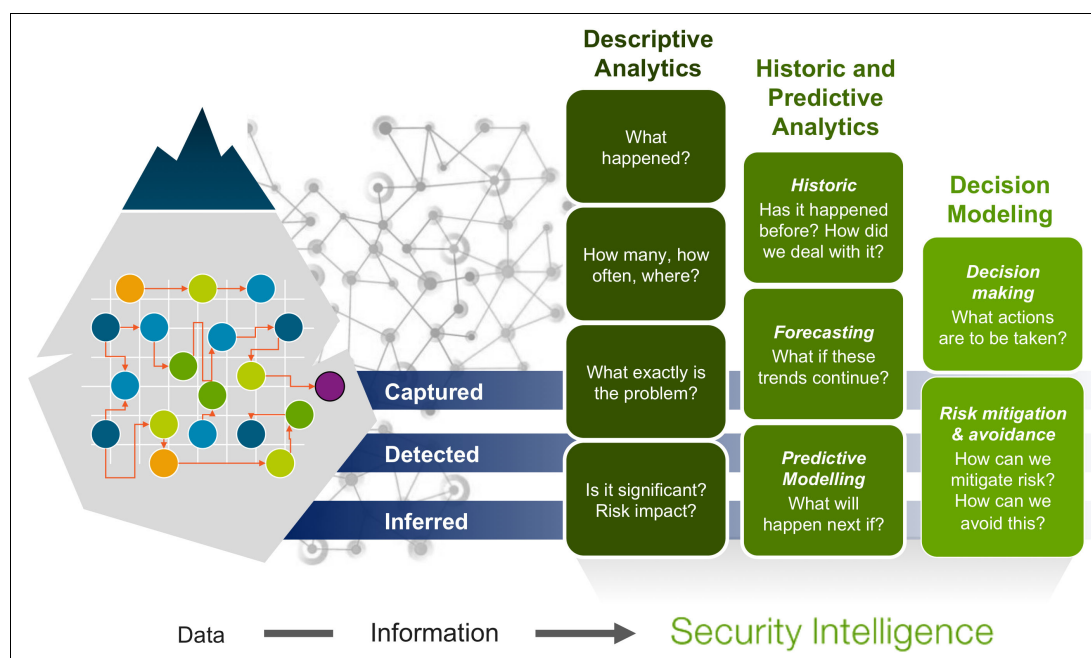


Figure 4 Applying real-time and historical analytics to build insights

Security intelligence is not just a set of technologies, processes, or the insight that results from them. It is a strategic approach that is focused on the following areas:

- ▶ Up-leveling the security and compliance conversation
- ▶ Achieving goals, especially stretch goals
- ▶ Delivering greater value to both IT and the line of business

Security intelligence can reduce risks. It can facilitate compliance, show demonstrable ROI, and maximize investment in existing security technologies. The basic definition for security intelligence is *the real-time collection, normalization, and analysis of the data generated by users, applications, and infrastructure that impacts the IT security and risk posture of an organization. The goal of security intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.*

The data that can be collected and warehoused by security intelligence solutions includes logs, events, network flows, user identities and activity, asset profiles and locations, vulnerabilities, asset configurations, and external threat data. Security intelligence provides analytics to answer fundamental questions that cover the *before-during-after* timeline of risk and threat management as shown in Figure 5 on page 7.

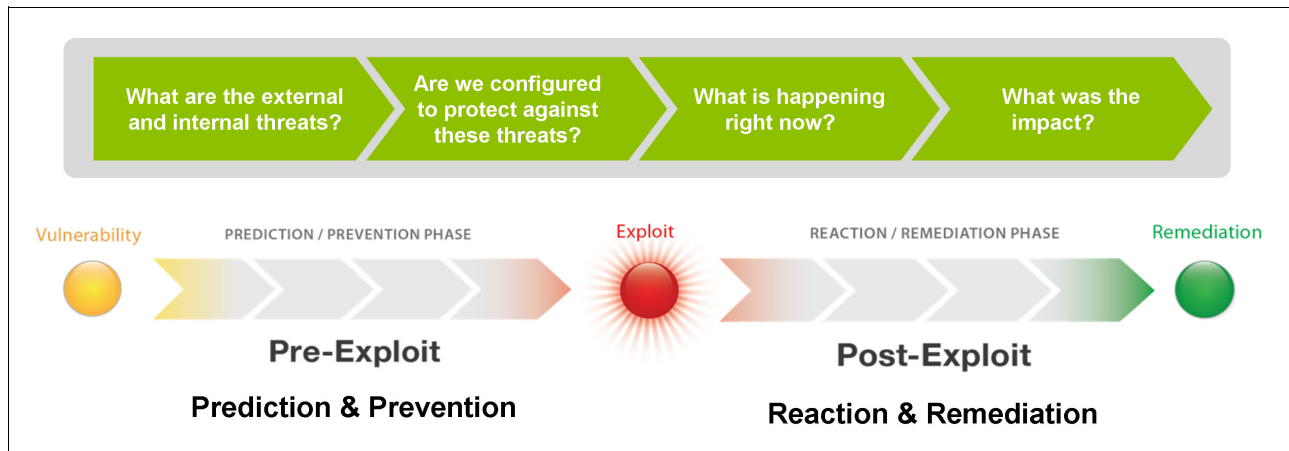


Figure 5 Security intelligence timeline

The business values of security intelligence

One of the most compelling arguments for security intelligence is operational efficiency: better use of people, time, and infrastructure. It is the ability to incorporate several security and network technologies into an integrated system rather than products operating independently.

The focus on security intelligence is relevant because operational responsibility for security is increasingly being placed in the hands of the network operations teams. It makes sense to mirror this consolidation of operational responsibilities with consolidation at the intelligence layer. Think in terms of enabling multiple tasks in a single platform and cross-functional development of skills across the organization and then deploying access based on roles.

Further, security intelligence adds value in other areas of IT, such as troubleshooting system problems, network issues, and user support and authorization analysis.

By using security intelligence, organizations can use integrated tools across a common framework and take advantage of a unified data set to address problems along the entire security spectrum. This approach can be illustrated in the following five most prominent use cases in which security intelligence provides high value:

- ▶ Consolidating data silos
- ▶ Threat detection
- ▶ Fraud discovery
- ▶ Risk assessment and management
- ▶ Regulatory compliance

Consolidating data silos

Without automated technology, business intelligence analytics are difficult to run. The data that gives you the ability to understand inventory returns and supply chains, for example, is available, but is siloed in different applications and databases. It falls upon the analyst to compile data from all those sources and pour them into spreadsheets or databases to perform manual analysis. Security analysis poses similar problems, and security intelligence provides similar efficiencies.

From a security perspective, data can exist in three types of silos:

- ▶ Data locked up in disparate security devices, applications, and databases
- ▶ Data that is collected from point products and applications, for example, creating another silo

It is another database where that data is stored, but without any communication or coordination between, for example, your configuration database.

- ▶ Organizational silos of data segregated by business unit, operations group, and department, for example

In the first two cases, security intelligence breaks down the silos by integrating data feeds from disparate products into a common framework for automated analysis across different security and IT technologies. From a security perspective, this approach brings in all the enhanced detection and risk assessment capabilities that the consolidated telemetry of security intelligence can deliver. From a CIO perspective, the reduction of these silos enables the rationalization of security products that might otherwise need to be managed on a point-product basis.

The third case requires considerable cooperation among groups that are typically separated, meaning a realigning of processes and responsibilities, and perhaps, some pressure exerted by management. The crushing cumulative volume of all this disparate data exacerbates the problem exponentially. Each silo can create enormous volumes of data, in different formats, for different purposes and, in some cases, different policies and compliance requirements. Only automated security intelligence can effectively manage petabytes of security-related data and analyze it across organizational and operational silos.

Threat detection

In a few short years, as organizations have opened themselves to Internet-based commerce and remote users, security has moved from a perimeter-based model with all policy centered on the firewall to distributed security. Security is now focused on hosts, applications, and the content of information moving out of the organization.

Moreover, we are seeing growing incidence of highly targeted attacks, such as the attacks on high-profile companies. Sophisticated, targeted intrusions are typically multistaged and multifaceted, difficult to detect, and difficult to eradicate. Advanced persistent threats (APT) are characterized by the tenacity of the attackers and resources at their disposal.

An over-arching intelligence should be applied to the diverse security technologies that have been developed in response to the evolving threat landscape. As noted for security, an activity that appears innocuous to one part of an infrastructure might be revealed as a threat when that data is correlated with other sources. For example, an attacker might disable logging, but cannot shut down network activity. Proprietary applications might not produce logs. Some parts of the network might be without firewalls. Security intelligence can still identify the applications and services that are running between the host and the network in these cases and flag a potential threat.

Fraud discovery

Security intelligence is essential for effective fraud detection. An understanding of the users and the application data is the key ingredient, in addition to network telemetry, data from the switching and routing fabric, and the security device enforcement layer.

Fraud detection requires monitoring of everything that goes on across the network, including network activity and events, host and application activity, and individual user activity. By using security intelligence, you can bind the user to a particular asset, by tying together network, domain name system (DNS) server, and application activity with directory information. For example, security intelligence can tie a specific user to a specific IP address for a specific virtual private network (VPN) session.

Risk assessment and management

Security intelligence provides the backbone for risk management through impact analysis and threat modeling. It is the difference between reacting to attacks on the network and proactively protecting your most important assets.

Impact analysis is based on the value that an enterprise assigns to a particular asset and negative consequences to the business if it is compromised. Security intelligence addresses impact analysis by asset and data discovery and classification to identify critical assets. Further, it answers questions such as the following examples:

- ▶ How exposed is the asset?
- ▶ Does it have direct access to the Internet?
- ▶ Does it have known vulnerability for which there are known exploits?

Threat modeling takes all these factors into account and more. It identifies vulnerabilities on the target system and possible attack paths based on revealing weaknesses between the target and the Internet such as poorly designed firewall rules and badly configured router access control lists (ACLs).

Regulatory compliance

Compliance is a foundational use case for security intelligence. It addresses many compliance requirements, particularly all aspects of security monitoring. For example, security intelligence does not meet all your PCI requirements. However, it meets all your PCI monitoring requirements in a way that security information and event management (SIEM) and log management alone cannot. Security intelligence provides the data that serves as a foundation to deliver and demonstrate audit requirements for all regulations.

By monitoring broadly across IT infrastructure (such as events, configuration changes, network activity, applications, and user activity), security intelligence consolidates compliance capabilities in a single product suite. It does not rely on multiple point products, each of which delivers its own piece of the audit puzzle.

IBM security intelligence solutions

The over-arching value of the IBM security intelligence solutions is the ability to tie intelligence from the network to the broader set of data that is collected from the entire enterprise infrastructure. It provides collection, analysis, and correlation across a broad spectrum of systems, including networked solutions, security solutions, servers, hosts, operating systems, and applications. The result is intelligence that provides a meaningful context for security professionals while radically reducing operational complexity across multiple systems.

IBM security intelligence solutions address the spectrum of the security lifecycle, centralizing data from disparate silos, normalizing it, and running automated analysis. By using this

approach, organizations can prioritize risk and cost-effectively deploy security resources for detection, prevention, response, and remediation.

IBM security intelligence solutions provide a unified architecture for collecting, storing, analyzing, and querying log, threat, vulnerability, and risk-related data. IBM security intelligence solutions are built upon three pillars of *intelligence*, *integration*, and *automation* as shown in Figure 6.

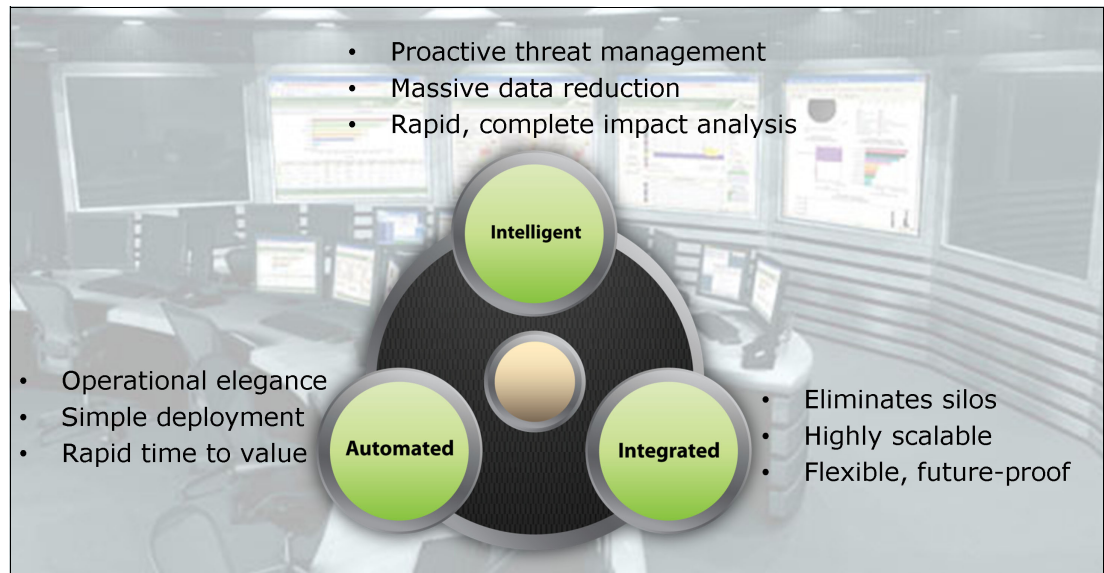


Figure 6 Intelligent, integrated, and automated IBM security intelligence solutions

IBM security intelligence solutions are highly intelligent, integrated, and automated. Organizations can benefit by having several departments and staff with various roles (such as operators, analysts, and auditors) and needs seamlessly using different modules.

► Intelligent

Figure 7 shows that, with more data under surveillance and more intelligent analytic techniques, IBM security intelligence solutions can detect threats that others miss. It can provide visibility that other solutions cannot provide.

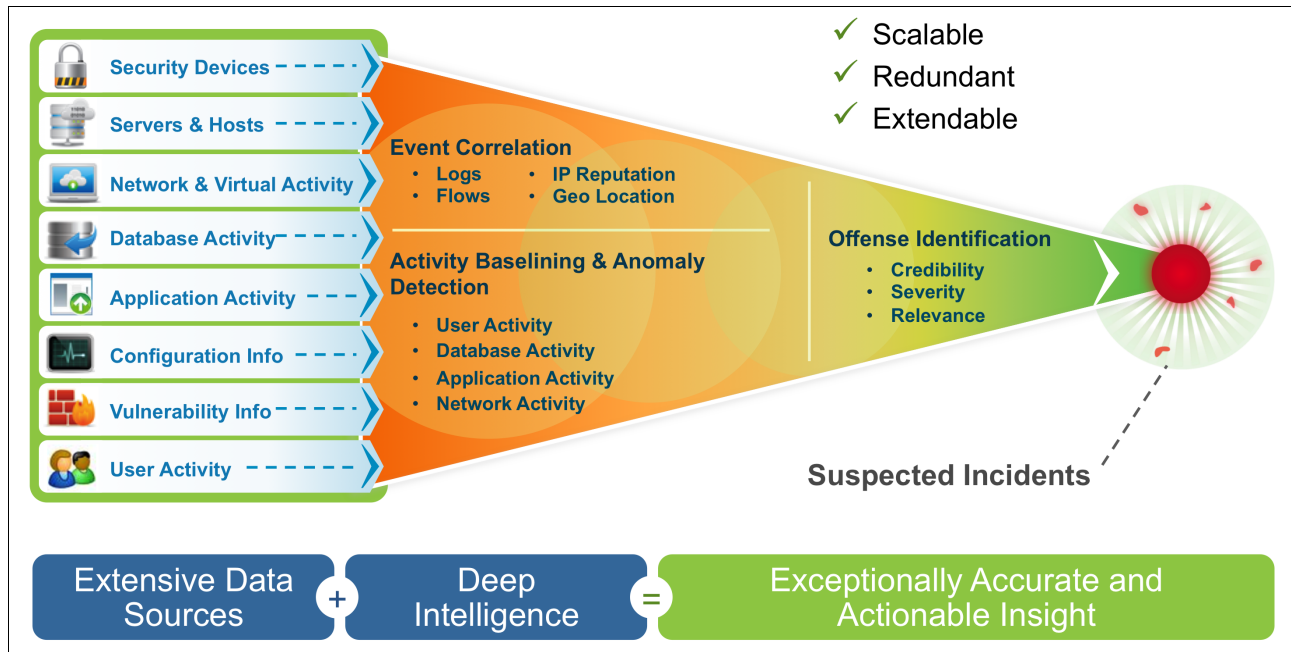


Figure 7 Intelligent context and correlation drive deepest insight

► Integrated

Designed from scratch to integrate log management, SIEM, and risk management in one solution, IBM security intelligence solutions can deliver a massive log management scale without any compromise on SIEM intelligence (Figure 8):

- A common platform for all searching, filtering, rule writing, and reporting functions
- A single intuitive user interface for all log management, risk modeling, vulnerability prioritization, incident detection, and impact analysis tasks

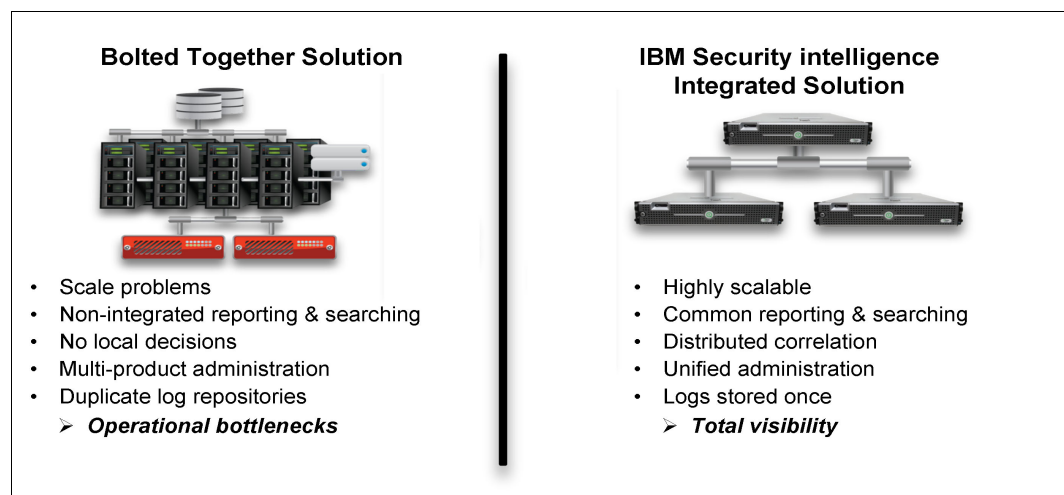


Figure 8 A truly integrated IBM security intelligence solution

► Automated

IBM security intelligence solutions can be deployed and managed by using automated security and network device discovery and compliance and policy functions (Figure 9). By automating tedious discovery and tuning functions, the IBM security intelligence solutions can remove complexity that inhibits many traditional security intelligence solutions.

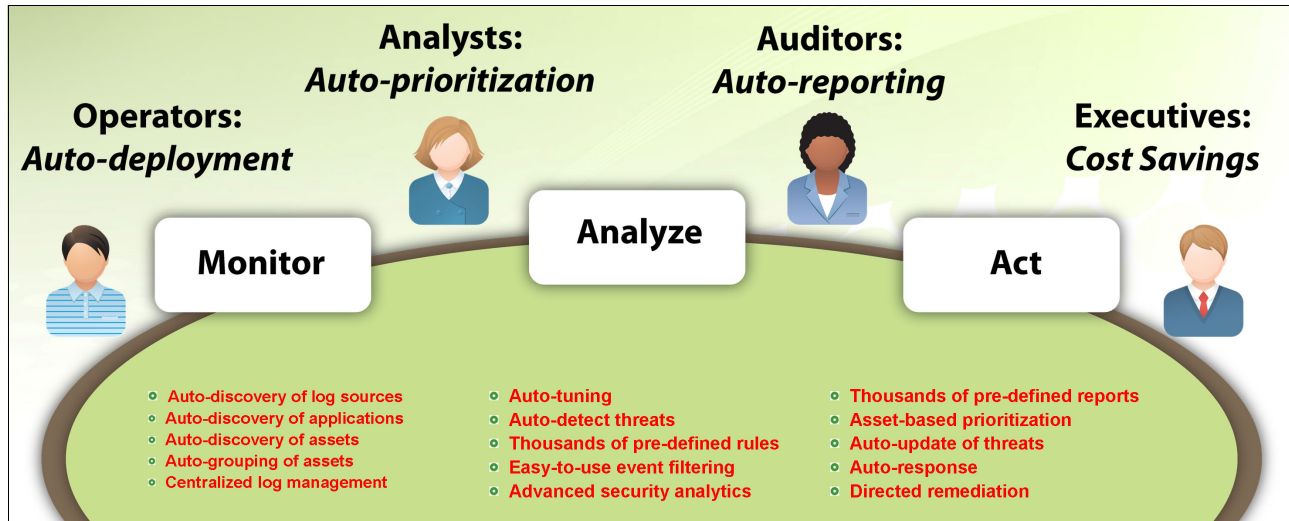


Figure 9 IBM security intelligence automation driving simplicity and cost effectiveness

IBM security intelligence solutions integrate previously disparate functions into one security intelligence solution, which makes it an intelligent, integrated, and automated security intelligence solution. Such functions include SIEM, risk management, log management, network behavior analytics, and security event management. The IBM security intelligence solution provides organizations with crucial visibility into what is occurring within their networks, data centers, and applications to better protect IT assets and meet regulatory requirements.

By using IBM security intelligence solutions, organizations can achieve the following objectives:

► Detect threats that other solutions miss.

Internet-based threats and fraud continue to get more sophisticated. Intelligence is hidden in an organizations' data, which can be used to detect alarming problems. Such problems range from employees stealing proprietary information to botnets trying to break in and steal credit card information or international espionage. IBM security intelligence solutions can help identify the high priority offenses against your corporate data and detect anomalies in user, application, and network behavior.

► Consolidate data silos.

With many companies generating millions or billions of records of events every day, a wealth of information exists in the event and log data that is generated by existing network devices. Unfortunately, this information is frequently stored in silos, often ignored, and most always under-used. IBM security intelligence solutions can converge the previously distinct network, security, and operations views of the infrastructure into a sensible yet scalable intelligence solution. By using this method, an organization can quickly respond to what is important. It can distill network and security information down to the identity and application awareness level to better and more efficiently resolve network threats and policy infractions.

- Detect insider fraud.

Some of the biggest threats to an organization come from the inside. Organizations often lack the intelligence that is necessary to accurately link individuals to incidents of malicious behavior. With user and application monitoring, organizations can set a baseline for normal user activity, making it easier to identify abnormal or risky behavior and weaknesses.

- Predict risks against your business.

Security and IT teams are constantly challenged to better manage risk across an ever-growing spectrum of vulnerabilities before a breach occurs. IBM security intelligence solutions can provide a preliminary solution that allows for assessing what risks exist during and after an attack. It can also answer many “what-if” questions ahead of time, which can greatly improve operational efficiency and reduce network security risks.

- Exceed regulation mandates.

Companies today are under growing executive pressure to comply with mandates, such as Sarbanes-Oxley, Good Practice Guide 13 (GPG-13), Financial Services Authority (FSA), Garante, HIPAA, FISMA, GLBA, PCI, and NERC. The massive amounts of data and events that are being generated in an organization provide the keys to the audit trail. The collection correlation and integration of all surveillance feeds for IBM security intelligence solutions yields the following information:

- More accurate data for an operator
- More granular forensics for an incident response manager
- More complete reporting for auditors

IBM security intelligence product family

The IBM security intelligence product family is based on a long planned and carefully developed strategy to build an operating system approach to security intelligence. The IBM *security intelligence operating system* powers the IBM Security QRadar® product family of IBM security intelligence solutions.

Figure 10 illustrates the IBM security intelligence operating system as the foundation of the IBM security intelligence solutions.

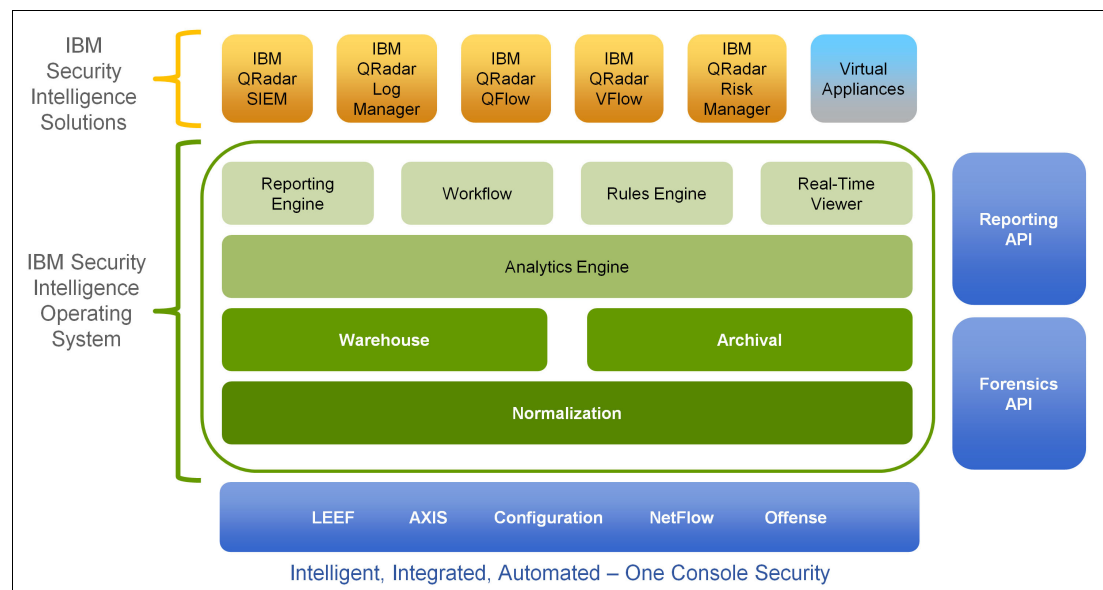


Figure 10 IBM security intelligence product family built on a common foundation

This framework is common for collecting, warehousing, filtering, analyzing, and reporting on all security intelligence telemetry. This integrated solution is the platform for risk management, security information and event management, log management, and network and application activity monitoring.

The IBM security intelligence operating system approach includes the following benefits:

- ▶ Convergence provides consolidation of previously siloed monitoring and analysis capabilities.
- ▶ Simplicity provides multiple functions delivered with a common user experience.
- ▶ Scalability provides simplified expansion capabilities for the largest infrastructures.

The IBM Security QRadar product family consists of the following solutions:

- ▶ IBM Security QRadar Log Manager
- ▶ IBM Security QRadar SIEM
- ▶ IBM Security QRadar Risk Manager
- ▶ IBM Security QRadar QFlow for network and application activity monitoring
- ▶ IBM Security QRadar VFlow for virtual activity monitoring

IBM Security QRadar Log Manager

IBM Security QRadar Log Manager is a comprehensive solution for organizations that are looking to implement a distributed event log manager to collect, archive, and analyze network and security event logs. Log management has emerged as a required part of an organization's ability to deliver security best practices and to meet specific auditing and reporting requirements of various government regulations.

For example, it helps to meet the following government requirements:

- ▶ Federal Information Security Management Act
- ▶ Health Insurance Portability and Accountability Act
- ▶ North American Electric Reliability Corporation
- ▶ Payment Card Industry Data Security Standard
- ▶ Sarbanes-Oxley

IBM Security QRadar Log Manager provides numerous advantages, including the following examples:

- ▶ Fast and efficient deployment
- ▶ Distributed log collection and archival
- ▶ Policy-driven event log manager correlation
- ▶ Effective reporting and compliance auditing
- ▶ Reliable and tamper-proof log storage
- ▶ Possible upgrade to full IBM Security QRadar SIEM

IBM Security QRadar SIEM

IBM Security QRadar SIEM delivers the SIEM system solution that can give security professionals the visibility that they need to protect their networks. The advanced SIEM technology of IBM Security QRadar can protect IT assets from a growing landscape of advanced threats and can meet current and emerging compliance mandates.

The IBM Security QRadar next-generation SIEM is an intelligent, integrated, and automated SIEM system. It delivers the following benefits:

- ▶ Unified, turnkey deployments and more efficient administration and management
- ▶ Distributed correlation that can allow for billions of log entries and records to be monitored per day

- ▶ Single log archival capacity that ensures seamless reporting and comprehensive searching within the SIEM system
- ▶ Centralized command and control functions that reduce acquisition costs of the security management solution and improve IT efficiency
- ▶ Advanced threat and security incident detection that reduces the number of false positives and detects threats
- ▶ Compliance-centric workflow that enables the delivery of IT best practices that support compliance initiatives
- ▶ Distributed appliance architecture scales to provide log management in any enterprise network

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager can provide organizations with a preliminary solution that network security professionals can use to assess which risks exist during and after an attack. These network security professionals can also answer many what-if questions ahead of time, which can greatly improve operational efficiency and reduce network security risks. Powerful security analytics, simulation, and visualization tools can give network security professionals the ability to move away from day-to-day security fire fighting and to adopt a proactive, risk-based methodology that can improve network security and minimize the risk of exposures.

With IBM Security QRadar Risk Manager, network security teams have the tools they need to achieve the following objectives:

- ▶ Automate compliance tasks and assess compliance risk, using the broadest set of risk indicators.
- ▶ Simplify multivendor configuration audits to ensure consistency of device configuration and assess the risk of configuration changes.
- ▶ See the risk impact of network changes, including new application and infrastructure deployments through enhanced security modeling and simulations.
- ▶ Use powerful network security visualizations to gain insight into when traffic can and does occur on your network, helping to pinpoint security risks that make exist.

IBM Security QRadar QFlow for network and application activity monitoring

The IBM Security QRadar QFlow appliance performs network and application activity monitoring. Network and application activity monitoring is a security fundamental that some organizations do without, at their peril. Effective analysis of network session activity, or flow data, involves the collection and detailed classification of network and application behavior. It also involves the ability to correlate network and application activity with log events and other security activities across your entire network.

Application-aware network monitoring enables stateful information about all conversations at the application layer. It also provides a more thorough understanding of complex applications including voice over IP (VoIP), multimedia, enterprise resource planning (ERP), and database.

IBM Security QRadar QFlow gathers knowledge from a deep examination of every packet within a conversation and provides a more detailed application level context. This information, when correlated with network and security events, enables a more advanced analysis of the overall security posture of the network. Furthermore, the application content that is captured can provide key forensic data and evidence for analyzing the true impact of threats, notably those threats that can include potential data leakage.

IBM Security QRadar VFlow for virtual activity monitoring

Because virtual servers are just as susceptible to security vulnerabilities as physical servers, organizations now must define and implement appropriate precautionary measures to protect their applications and data that reside within the virtual data center.

With the Security QRadar VFlow for virtual activity monitoring, IT professionals can increase visibility into the vast amount of business application activity that appears across their virtual networks. The Security QRadar VFlow offering helps organizations to better identify these applications for security monitoring, application-layer behavior analysis, and anomaly detection. IBM Security QRadar VFlow can also enable operators to capture application content for deeper security and policy forensics.

What's next

Many organizations have recognized and embraced the value of business intelligence and analytics technology, because their success is predicated on the ability to analyze and act upon the essential information that is derived from staggering volumes of data. Similarly, security intelligence is essential because information security is integral to doing business in the 21st century. Powerful, automated analytics of centralized data from sources that cover the entire spectrum of the IT infrastructure make a high level of cost-effective security possible and indispensable.

Analyzing information for a security-related context should include looking at the *typical security data*, such as access or network traffic logs. The analysis must also extend to other, often *business-related* areas to produce more meaningful and accurate reports.

IBM security intelligence, analytics, and big data

Sophisticated cyber crimes and advanced persistent threats are occurring at an alarming rate. Aided by new attack techniques, increased financial support and the ease of exposing social connections, attackers are having more success than ever before. Traditional security solutions are no longer sufficient to defend against these escalating threats.

IBM Security QRadar uses big data capabilities to help keep pace with advanced threats and to help prevent attacks before they happen. It helps uncover hidden relationships within massive amounts of security data, by using proven analytics to reduce billions of security events to a manageable set of prioritized incidents.

Forward-looking organizations explore custom analytics that use additional big data technologies on various unstructured data sources. Such data sources include email, social media feeds, business transactions, and full network packet payloads. To meet this demand, IBM is integrating industry-leading security intelligence capabilities with the world-class analytics capabilities of IBM InfoSphere® BigInsights™ or IBM Netezza® solutions and related big data software and services (Figure 11 on page 17). This combination offers a comprehensive solution. A security intelligence platform is designed to detect and prioritize threats in real time, with a mature solution that is based on Hadoop for custom data mining and analytics.



Figure 11 IBM Security QRadar and big data for security intelligence

A big data security analytics solution must ingest data that is provided by a large variety of security data feeds from within the enterprise, in addition to unstructured and semistructured data from inside and outside the enterprise. It must also adapt to the changing threat landscape, provide a holistic view of the enterprise environment, and drive intelligence that can be acted upon to protect against both known and unknown threats.

By using IBM security intelligence solutions with big data, security organizations can analyze more data, more flexibly and can gain more accurate results. By analyzing structured, enriched security data alongside unstructured data from across the enterprise, IBM security intelligence solutions can help find malicious activity that is hidden deep in the masses of an organization's data, for advanced threat and risk detection.

Use case

In this use case, a large financial services firm uses the IBM security intelligence solutions to meet regulatory compliance, detect frauds and threats, and improve network visibility. The financial firm, with a growing customer base, employs over 10,000 people with 1000+ offices throughout the North America, Europe and Middle East, Africa, and Asia-Pacific regions.

The financial services firm supports internal-facing and external-facing websites and has integrated dedicated applications and network connections with multiple offices and the firm's various business partners. The corporate data center houses all the core application servers and databases that are used to conduct business, including web servers, email servers, and servers that process credit card transactions.

The financial services firm has identified so many separate locations that need access to the data center and to the internet that the network perimeter has become blurred. This situation demands the need to protect the various parts of the organization from external and internal threats. To achieve this objective, this services firm understands the requirement to have visibility across its entire network. This way, it can detect any threat and deal with it swiftly, without impacting the ability to meet customer needs and timelines.

The Chief Information Security Officer (CISO) has tasked the organization with the following arduous assignments:

- ▶ Ensuring that the company complies with PCI DSS requirements
- ▶ Ensuring that the company implements a security intelligence solution that can scale its security operations to have complete visibility into their network architecture

The following network devices and applications are defined as the key assets to monitor:

- ▶ Active Directory
- ▶ Database
- ▶ DHCP servers
- ▶ Firewalls
- ▶ Load balancers
- ▶ Mail servers
- ▶ Microsoft workstations
- ▶ Reverse proxies
- ▶ Routers
- ▶ Switches
- ▶ VPN
- ▶ Web application servers

The financial services firm can use an IBM Security Intelligence solution to fulfill these requirements and to protect the various assets that are defined by the office of the CISO. Multiple IBM Security QRadar SIEM appliances can be deployed throughout the IT environment to gather sets of data to use for analysis and security intelligence.

Figure 12 shows the high-level architecture of the deployment.

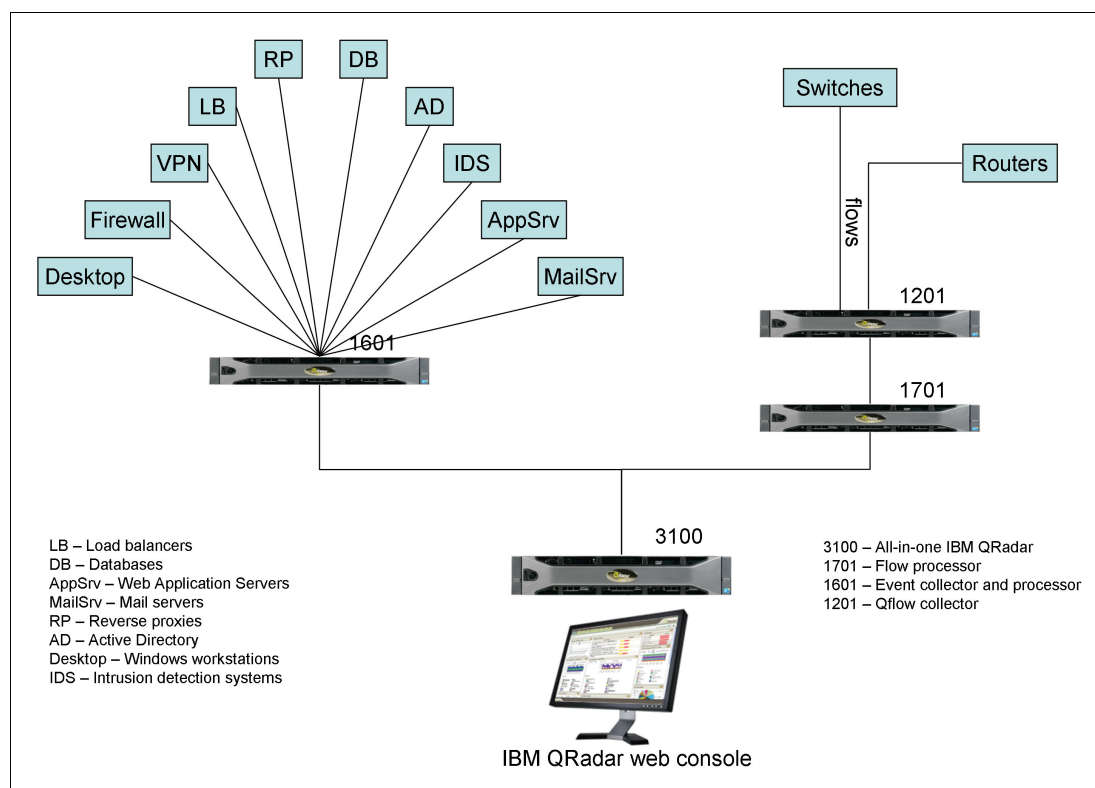


Figure 12 High-level architecture of IBM Security QRadar deployment

The IBM Security QRadar SIEM product was the only product that provided the financial services firm with all the features and functions that the firm was looking for within one solution.

- Finding the real threats in a heap of logs and messages

By using the IBM Security QRadar SIEM, enterprise IT professionals can centralize separate network security management functions from various operational silos into a single, cohesive framework. This unique and highly cost-effective approach delivers an unparalleled monitoring and auditing capability that is network, security, application, and identity aware. IBM Security QRadar profiles the behavior of systems, applications, and users, learns normal patterns, and recognizes anomalies, whether they originate from security breaches, internal network misuse, or operational inefficiencies. By isolating an anomaly's source as a network issue or a security threat, IBM Security QRadar provides a head start for dealing with suspect activity before real damage is suffered.

- Finding the threats fast to remediate immediately

By using the IBM Security QRadar SIEM log management capabilities, the financial firm can perform forensic research to evaluate where a problem occurred and can deal with it right away. For example, the IBM Security QRadar SIEM dashboard delivers a prioritized list of potential threats and network abnormalities that can be remediated instantly, rather than after an incident occurs. A security team can now monitor real-time attacks with the ability to drill down to the packet level or previous offense activity. This way, the team can gain substantially more insight as to the type of attack, the payload of the packets, and the hosts that are involved in the attack.

Rules can be created to alert security specialists and ticket tracking tools so that problems can be dealt with efficiently and remediation can be tracked.

- Reporting capabilities

The financial services firm began its search for a network security management solution to address its needs while adhering to specific external compliance and internal policy mandates. Standard regulatory reports, which are shipped with the product, gave the firm a jump-start on its compliance reporting needs so that the firm can monitor compliance in an ongoing fashion.

- Improving business processes with security intelligence

Overall, the network services team of the financial services firm successfully achieved its goals with IBM Security QRadar SIEM. The IBM Security QRadar architecture provides the team flexibility to scale its solution and to turn on more robust incident and event collection without incurring exponentially higher costs. With the security intelligence that IBM Security QRadar SIEM provides, the firm's security and administrative teams improved their security posture both internally and externally.

As the team continues to scale up its security operations with IBM Security QRadar, the firm can effectively streamline its overall security process. It relies on IBM Security QRadar SIEM to pull the necessary actionable information from logs, events, and network traffic data. Smaller teams can be used by centralizing their program through IBM Security QRadar by saving the time it took to manually collect and analyze logs, event data, and network traffic from multiple sources and across multiple silos. The financial services firm also improved overall business and decision-making processes by applying the contextual information from log and event collection to its everyday activities.

Summary

The job of delivering an effective security intelligence program is not trivial for organizations. The motivation for improving an organization's overall IT security posture comes from many directions, including operational improvements and compliance mandates. However, all directions lead in the same direction, protecting assets from those attackers who want to harm them. Historically, organizations have invested in many point solutions in an attempt to mitigate specific IT risks. Moving forward, organizations need to look at ways to capitalize on their existing investments and to integrate the value from the information that these individual solutions already provide.

IBM security intelligence solutions provide organizations with improved operational efficiencies and the ability to lower costs through an integrated approach to network security intelligence. They provide unique and differentiated values in the areas of detecting threats that other solutions miss, exceeding compliance mandates, discovering insider fraud, predicting risks, and consolidating data silos.

Other resources for more information

For more information, see the following resources:

- ▶ The latest IBM X-Force Trend Reports
<https://www.ibm.com/services/us/iss/xforce/trendreports>
- ▶ The IBM Security QRadar product family
<http://q1labs.com/products.aspx>
- ▶ Security Intelligence and Compliance Analytics
<http://www.ibm.com/software/products/us/en/subcategory/SWI60>

The team who wrote this guide

This guide was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).

Nilesh Patel is a senior identity and access management and security intelligence professional in the IBM Security System division. Nilesh is a solution advisor for IBM security and compliance management solutions and is an accredited IBM Redbooks® Master Author. He has extensive experience in design and implementation of identity and access management solutions with security intelligence and compliance solutions. Nilesh has published many technical papers within the IBM developer domain and customized integration modules on the IBM Open Process Automation Library for identity and access management and security intelligence products. He has delivered many technical webcasts to educate customers on new features and integration of IBM Security products.

Arun Madan is a Senior Technical Staff Member (STSM), Certified Information Systems Auditor (CISA), Associate Director, and Chief Architect for IBM Global Technology Services® - Strategic Outsourcing in IBM India/South Asia. Arun is a security expert writer at the ITSO, Austin Center. He has been with IBM for the past 6 years and has over 30 years of experience in the Information Technology industry. He has designed and led implementations of organization-wide security frameworks, and published and presented papers at various security forums.

Sridhar Muppidi is a Senior Security Architect for IBM Software Group. As a Senior Technical Staff Member, he drives security architecture and design activities across IBM

security products. He is responsible for SOA security architecture and SOA security solutions. He is a lead architect for the IBM Security Policy Management solution. His responsibilities include providing secure solutions to enterprises, working on new product development, and representing IBM in standards activities. Sridhar holds a Ph.D. degree in computer science and has published extensively.

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He has 26 years of experience in various areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture. Axel writes extensively and teaches IBM classes worldwide about areas of software security architecture and network computing technologies. He has a degree in computer science from the University of Bremen, Germany.

Thanks to the following people for their contributions to this project:

Rick Cohen
Randy Forlenza
Raghu Kalyanaraman
Miguel Sang
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new IBM Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4956-00, was created or updated on May 9, 2013.



Trademarks


IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>



The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

BigInsights™
Global Technology Services®
IBM®

InfoSphere®
Redbooks®
Redguide™

Redbooks (logo) ®
X-Force®

The following terms are trademarks of other companies:

Netezza, and N logo are trademarks or registered trademarks of IBM International Group B.V., an IBM Company.

QRadar, and the Q1 logo are trademarks or registered trademarks of Q1 Labs, an IBM Company.

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.