IBM Security

The power to protect at scale

Organizations of all sizes get collaborative security intelligence using IBM QRadar, with IBM Sense Analytics Engine

IBM Security White Paper

For today's security needs, deploy up-to-date analytics tools

Today's organizations are besieged by security threats. Like kids in a candy store, cybercriminals can't wait to get their hands on confidential information and sell it to the highest bidder.

And as attacks grow more advanced, it's increasingly important for organizations to have flexible, scalable and collaborative security tools in place to meet changing security requirements. Security information and event management (SIEM) tools provide a powerful way for organizations to prevent, detect and respond to the latest threats before they can cause damage. But it is important to choose the right SIEM solution. A solution you can fully deploy in weeks and never outgrow. A solution that doesn't require an advanced degree in search query specifications.

Detecting subtle differences in the environment—and understanding the context of security events—requires the power of advanced analytics. Security teams need an analytics engine that can match user behavior with log events, network flows, threat intelligence, vulnerabilities and business context. This can help them find attackers lurking within the organization, as well as prioritize issues for remediation.

In addition, the right security tools collect insights from beyond your organization. They empower your security teams to collaborate with experts from around the world and quickly incorporate their insights into URL blacklists, malware detection scripts, email subject lines for phishing attacks and more.

Companies face a 26% likelihood of a data breach in the next 24 months.[1]

Learn more from IBM® X-Force® about the latest security threats.

1 "2016 Cost of a Data Breach Study: Global Analysis," *Ponemon Institute,* June 2016.

IBM QRadar scales in all the ways security requirements demand

IBM QRadar® Security Intelligence Platform, powered by IBM Sense Analytics™ Engine, can not only meet the needs of today's security environment, it also scales to meet those needs as cyber threats and enterprise requirements grow.

Whether you want to support a growing organization, add new capabilities or expand storage capacity and performance, QRadar can be deployed and expanded quickly, easily and cost-effectively. You can start with a single appliance solution handling fewer than 10,000 log events per second, and grow it to support billions of daily events.

The integrated QRadar platform is designed to enable you to:

- **Scale out:** Expand the deployment over time as the business grows, and as the threat environment becomes increasingly hostile
- **Scale up:** Add event processing power and low-cost storage that can retain data for months, years or even decades
- **Scale functionality:** Deploy new capabilities through integrated risk management, vulnerability management, incident forensics, incident response and third-party applications
- **Scale for cloud:** Use on-premises infrastructure to collect security information from the cloud, deploy a hybrid environment with on-premises and cloud components, leverage security infrastructure in the cloud and deploy SIEM as a service
- **Scale through collaboration:** Integrate use cases and applications from other developers, business partners and your peers without adding unnecessary complexity

QRadar can collect log events and network flows from more than 450 applications and devices.[1]

Watch this video to learn how Sense Analytics improves response to threats.

1 "Introducing the IBM Security App Exchange," *IBM Corp.,* December 2015.

In today's threat landscape integrated security is critical

The unfortunate truth is that data breaches have increased in both frequency and cost—now averaging as high as USD4 million per enterprise breach.[1] Meanwhile, IT organizations have limited budgets, requiring prevention, detection and response to be as cost-effective as possible.

Rather than deploying another point solution, organizations need an integrated platform that can provide out-of-the-box security intelligence with advanced analytics. They must also be able to expand the platform by quickly adding new applications that conquer the latest security threats, without having to wait for the next product release.

The QRadar platform provides a fast, easy, cost-effective way to meet changing security intelligence and analytics needs. It offers integrated capabilities for log management, SIEM, data storage, incident forensics, full-packet capture, risk and vulnerability management, and incident response. It's an end-to-end solution, from prevention and detection to coordinated response and remediation.

Government presents a big target—more than 200 million records were compromised worldwide from January to October 2016. That's nearly 60 million more than in 2013, 2014 and 2015 combined.[2]

With its highly scalable architecture, QRadar is ideal for growing organizations that seek maximum security and compliance. Organizations can begin with a small, midsized or large deployment and add new processing or functional capabilities on the fly. Some modules are even pre-installed, enabling new capabilities to be accessed through a simple license key activation.

QRadar also scales through integration with other IBM and third-party products. It enables security teams to collaboratively take action against threats by integrating IBM X-Force Threat Intelligence feeds, as well as new, approved applications from the IBM Security App Exchange.

▶ Watch this demo to learn more about IBM QRadar Security Intelligence Platform.

1 "2016 Cost of a Data Breach Study: Global Analysis," *Ponemon Institute,* June 2016.

2 "The changing face of IT security in the government sector," *IBM X-Force Research,* December 2016.

Find and combat threats with real-time and historical visibility

QRadar with Sense Analytics is designed to monitor, correlate and store large volumes of data in real time, transforming raw security data into meaningful patterns of related activity. Data correlation can be performed both locally and globally, and can include questionable events that happened months ago.

The Sense Analytics Engine helps security teams detect potentially malicious activity, including behavioral changes that deviate from regular patterns, anomalies in network traffic (such as new traffic or traffic that suddenly ceases), and any user or asset activities that exceed a defined threshold. QRadar can also ingest the latest threat intelligence data from the IBM X-Force Exchange to detect emerging threats from across the globe, and generate alerts to help your security teams take action.

70% of organizations lack the visibility to report on end-user entitlements for data access.[1]

Then, as the size of a deployment grows, QRadar has the processing power to enable rapid searches, and to analyze and report on security data spread across multiple locations. QRadar provides high-performance indexing capabilities for extremely fast searches from within an intuitive user interface.

Plus, IBM QRadar Data Nodes can be added to any collector appliances, doubling and tripling search processing performance and data storage capacities using an automatic load balancing technology.

▸ Read more in this IBM blog about the importance of security visibility.

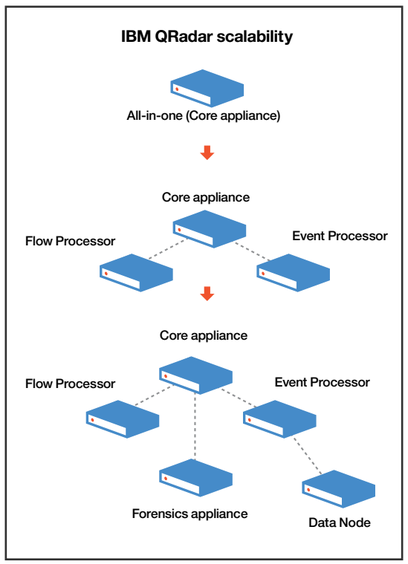
1 "Privileged Access: Manage the Potential Risk to Safeguard Your Data," *UBM,* May 2016.

Scale out, from small to large. Scale up for speed and capacity

With QRadar, organizations can easily expand the size and breadth of a deployment and upgrade to the newest product releases. And their security can grow incrementally as security needs change. Security teams can begin with a single, turnkey appliance and grow it over time into a highly distributed, console-based command center by adding multiple event and flow processors, collectors and data nodes.

Because QRadar functions are built upon a common architecture, database and user interface, security teams can easily scale out their existing deployments and access new capabilities. For example, IBM QRadar QFlow Collectors can be added for application-layer (Layer 7) visibility using deep-packet inspection technology—even across virtualized and cloud deployments. QFlow helps security teams automatically identify the content of traffic payloads, flag new anomalistic services, register legitimate assets in a configuration database and kick-off real-time scans.

Click image to enlarge. Click again for original size.



IBM QRadar scales to enable adding functions.

One of the biggest challenges organizations face today is the need to keep more and more security data available for quick analysis—for months, or even years. To help boost the storage capacity and analytical processing performance of QRadar deployments, organizations can use QRadar Data Nodes.

Here's how nodes work: QRadar event and flow processors are the components that collect, process and store real-time security data. They also perform ad hoc historical searches. If query performance degrades to an unacceptable level, QRadar Data Nodes can be added to QRadar event and flow processors to restore performance. All future incoming data is automatically balanced across the expanded processing resources and data storage capacities.

- Learn more in this IBM blog about the need for updated security solutions to outthink threats.

QRadar security capabilities scale for cloud deployments

QRadar also scales to support a variety of cloud-based deployment models. For example, QRadar can collect security information from cloud-based applications and integrate it with your on-premises data for comprehensive insights. The QRadar management console and event and flow processors all remain on-premises, while application-specific data gateways transfer events and flows in real time from the cloud workload. As a result, you have global visibility across the entire environment.

Alternatively, QRadar can collect, analyze and store data from the cloud *in the cloud*. In this hybrid environment, QRadar event processors and flow collectors are deployed in the cloud, while the management console remains on-premises. Data is transferred in real time through a secure connection to your data center for consolidation and analysis. Again, you get a complete picture of your security posture across on-premises and cloud infrastructure.

The QRadar on Cloud infrastructure is monitored 24x7 by trusted IBM service professionals.[1]

QRadar can also be deployed in the cloud and the infrastructure can be managed as a service by IBM. Called IBM QRadar on Cloud, this solution can help address funding issues and staff shortages by outsourcing basic tasks—while leaving you in full control of monitoring events, incidents and offenses. QRadar on Cloud can also provide you with more predictable and flexible monthly costs. It helps you move from a model based on capital expenditures to one based on operating expenses.

- Learn more on the web about QRadar on Cloud.

1 "IBM Security Intelligence on Cloud," *IBM Corp.,* April 2015.

Scale QRadar functionality within the same interface

IBM X-Force has identified more than 97,000 unique security vulnerabilities.[1]

In addition to expanding the size, speed and capacity of a SIEM deployment, organizations can also scale QRadar along another dimension—functionality. Some key capabilities that can be added to the platform include vulnerability and risk management, forensic analysis, user behavior analytics, incident response and numerous downloaded applications.

- **Vulnerability and risk management**—IBM QRadar Vulnerability Manager is another way to expand the proactive security capabilities of an existing QRadar deployment—enabling security teams to collect configuration and topology data to proactively identify risks, simulate offenses and take corrective action before an attack occurs and for identifying and prioritizing device and application vulnerabilities. As a centralized control center for prioritizing security gaps and weaknesses for resolution, the solution supports periodic and dynamic network security scans, and delivers a full audit trail for compliance reporting.

QRadar Vulnerability Manager also helps proactively manage network device configurations. For example, security professionals can pinpoint which firewall rules are firing, which are not, and which ones could be removed to improve firewall performance and security. The solution's automated policy monitoring service helps quickly discover configuration errors that may leave organizations exposed to attack or network traffic that fails to comply with one or more industry or governmental mandates.

▶ Read the IBM interactive white paper to learn more about QRadar Vulnerability Manager.

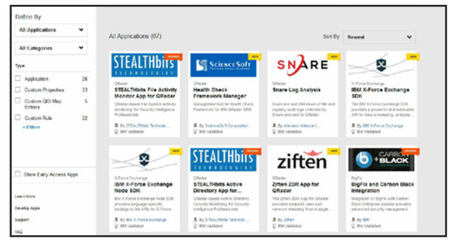
1 "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.,* February 2016.

More scalable functionality within QRadar

Scaling QRadar not only improves enterprise security, it helps organizations get more value from their existing QRadar investment. Additional capabilities that can be added include:

- **Forensics analysis**—IBM QRadar Incident Forensics provides additional visibility into the "who, what, when, where and how" of a security incident. With an intuitive user interface, the solution incorporates an Internet-style search engine interface to help provide clarity around what happened. It also uses full-packet capture capabilities to obtain and reconstruct the data that was accessed or transferred. As a result, QRadar Incident Forensics helps to quickly investigate and remediate a network breach, and it can reduce the chances of data exfiltration or the recurrence of past breaches.
- **Deep packet inspection**—IBM QRadar Network Insights is a real time packet inspection technology that helps security teams look for suspicious content hidden deep in data transmissions—from application level analysis of emails, files, chat sessions and web activity to invalid SSL certificates or protocol obfuscations. It provides administrators with the information and real-time alerts needed to not only spot attacks in progress, but also determine what damage may have already been done.
- **Incident response**—IBM QRadar Security Intelligence Platform senses, detects and analyzes events that can be signs of an advanced threat. Integration with IBM Resilient Systems® enables the automation of response processes, and allows the generation of a playbook that makes security alerts instantly actionable, provides valuable intelligence and incident context, and allows security teams to quickly take action.

Click image to enlarge. Click again for original size.



With IBM Security App Exchange, IBM customers, developers and business partners can share applications, security app extensions and enhancements to IBM Security products.

▸ Visit the IBM Security App Exchange.

Scale your efforts by collaborating with peers and experts

Cybercriminals share tactics on the dark web and beyond, so shouldn't the "good guys" collaborate too? The QRadar open framework enables you to scale your security measures through collaboration with the global security community. Using QRadar application programming interfaces (APIs), you can easily integrate IBM and third-party solutions.

The IBM Security App Exchange allows you to scale your QRadar deployment by downloading applications that have been tested and approved by IBM and that integrate with the QRadar management console. The site enables IBM, business partners and customers to collaborate and share best practices, applications, dashboards, and application extensions and enhancements to IBM Security products—helping improve response to the latest security threats.

IBM Security App Exchange is the first place to find validated application extensions and enhancements for QRadar. Your security teams can download and install the solutions independently—outside of official product release cycles. It's a great way to find industry-, threat-, device- and vendor-specific content for QRadar.

What's more, the X-Force Exchange enables your security teams to collaborate with X-Force researchers and other security experts on the latest threat information. You can use the site to research threat indicators to see if they represent malicious activity, track and share evidence, and interact in private communities to develop stronger defenses.

Click image to enlarge. Click again for original size.

With IBM X-Force Exchange, you can rapidly research global security threats, aggregate actionable intelligence and collaborate with your peers.

- Learn more about IBM Security App Exchange and X-Force Exchange on the web.

Why IBM?

As security threats grow increasingly sophisticated, organizations need to have the right analytics platform for predicting and prioritizing security weaknesses for mitigation or remediation. Deploying multiple, independent security tools and disparate point solutions is inefficient, costly and can leave dangerous gaps in security. And as an organization grows or new security intelligence capabilities are needed, security teams need technology that can adapt to the new requirements—rather than having to manage a costly rip-and-replace migration.

IBM capabilities for collecting information; automating corrective actions; continuously enforcing security policies; and monitoring, analyzing and auditing records provide the enterprise-wide view of threat activities that organizations need to sustain ongoing system and data security as well as regulatory compliance.

QRadar Security Intelligence Platform, powered by Sense Analytics, is designed to provide the fast, easy, cost-effective way to meet changing security needs. This integrated platform can scale over time in size, functionality and performance, giving you the power to act—at scale. With QRadar, you can stay ahead of attackers for years to come.

IBM Security solutions are trusted by organizations worldwide for identity and access management. Intelligent and integrated for improved effectiveness, the broad IBM portfolio of proven technologies enables organizations to protect their most critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

- Learn more on the web about IBM Security.

For more information

Find out how the integrated capabilities in IBM QRadar can meet your changing needs, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/qradar

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

WGW03267-USEN-00