January 2013

Delivering success that scales with the largest enterprises

IBM Security QRadar solutions power some of the world's largest, most successful security intelligence deployments

IBM

Powerful, comprehensive solutions across industries

The award-winning IBM® QRadar® Security Intelligence Platform collects, correlates and monitors even the highest data volumes and supports the rich customization that large organizations require—without the cost and complexity associated with first-generation security information and event management (SIEM) solutions. In order to support the demands of organizations across industries, IBM offers the geographic reach to serve global organizations and the partner ecosystem required to deliver powerful and comprehensive solutions.

Big capabilities built for big enterprise needs

The QRadar Security Intelligence Platform—which includes IBM Security QRadar SIEM, IBM Security QRadar Log Manager and IBM Security QRadar Risk Manager—excels in the areas that matter most to large organizations, offering scalability, high performance, centralized management, wizard-based customization and other advantages.

Scalability

The QRadar Security Intelligence Platform scales easily to meet the needs of some of the world's largest organizations. Its distributed, federated database architecture allows QRadar solutions to monitor, correlate and store high data volumes in real time. Unlike some competing products, the QRadar Security Intelligence Platform does not filter out data or write data to disk without correlation. With its inherently scalable architecture, there is no arbitrary limit on the volumes the platform can support. Organizations use QRadar solutions in real-world deployments to process more than 100,000 events per second, fully correlated. The platform's purpose-built databases support a centralized searching and correlation engine that enables users to transparently search data across distributed appliances. Correlation can be performed both locally and globally, without any impact on performance. This ability to monitor and manage activity from a single pane of glass, with both global and local correlation, is a key reason security operations centers rely on the QRadar Security Intelligence Platform as their strategic intelligence solution.

QRadar customers include industry leaders such as:

- Four businesses with more than USD100 billion revenue
- More than 100 members of the Global 2,400
- Top three global pharmaceutical company
- Top three global software company
- Top three US energy company
- Top three US drugstore chain
- Top three US media and entertainment company
- Top five global auto manufacturer
- Top five US airline
- Top 10 US defense contractor
- Top 10 US general merchandise retailer
- Top 15 US utility company
- One of the world's largest SAP customers

Search performance

As the size of a deployment grows, it becomes increasingly challenging to rapidly deliver results when searching, analyzing and reporting on data spread across multiple enterprise sites—and with today's advanced cyberattacks, speed is a critical requirement for threat management. The QRadar Security Intelligence Platform performs extremely fast searches of networking and security data residing anywhere within the enterprise using its high-performance indexing capabilities and a simple-to-use, free-text user interface.

Searches that can take alternative solutions minutes, if not hours, to complete are often performed by QRadar solutions in seconds. The result is virtually instant information access for more effective and efficient forensics, threat management and enterprise-wide network insight.

Customization and integration ability

Although the QRadar Security Intelligence Platform ships with thousands of out-of-the-box rules, report templates, dashboards and searches, it is also highly configurable to meet the needs of multidivisional, multinational organizations with numerous operational groups. It also easily integrates with dozens of third-party network, security and infrastructure products.

- **Dashboards:** Users can easily customize workspaces with critical views of security and networking data.
- **Correlation and workflow:** Rules can be developed and matched to specific use cases for threat management, policy monitoring, compliance and more. QRadar solutions offer embedded workflows that allow security operations teams to track and investigate evidence associated with an offense.
- **Reports:** An easy-to-use QRadar reporting wizard helps users develop their own customized reports, including multiple chart layouts, to create advanced reports.
- **Forensic and operational views:** Commonly used searches and views can be saved to help with detailed investigations navigating through both live and historical data.
- **Custom event and flow properties:** Custom properties can be created to extract data beyond the default fields and used for searching, filtering, reporting and correlation activities.
- **Custom events:** New custom events can be added to the standard QRadar taxonomy—for example, an intrusion detection system event based on a custom signature.
- **Integration:** QRadar solutions offer integrations with surrounding security, network and data-center technologies including ticketing systems, email systems, Fibre Channel, iSCSI and many other common technologies.

Reliable threat intelligence

The IBM X-Force® research and development team is one of the most renowned commercial security teams in the world. This group researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM products, and educates the public about emerging Internet threats using a database of more than 60,000 computer security vulnerabilities, a global web crawler and international spam collectors.

In addition, IBM has thousands of security clients around the world, many of whom use this security services organization to manage their network environments. Every day, the X-Force team manages 15 billion security events on various networks around the world, logging and analyzing that data to produce insights about different Internet attack activity.

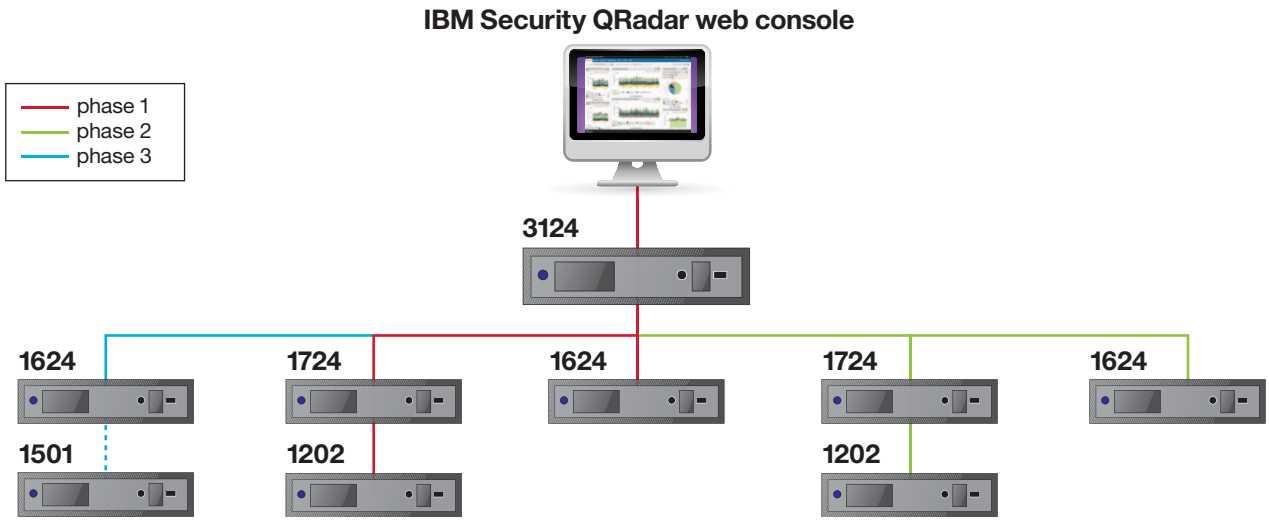
QRadar SIEM customers can enrich their existing threat-detection capabilities by purchasing a weekly subscription to X-Force threat intelligence data feeds. The content in these feeds is automatically incorporated into the correlation and analysis functions of QRadar SIEM, and any security event or network activity data that involves identified IP addresses will be automatically flagged—adding valuable context to security incident analyses and investigations.

Easily expand and upgrade your deployment

With QRadar products, organizations can easily expand the size and breadth of a deployment and upgrade to the newest product releases. No intrusive architectural changes, "rip-and-replace" migrations or expensive professional services engagements are required to keep pace with growing security needs.

The QRadar distributed appliance approach enables an organization to start with a small, midsize or large deployment and add new processing or functional capabilities on the fly. Event and flow processor appliances and flow collector appliances are easily inserted wherever required to support evolving network needs.

Because the QRadar Security Intelligence Platform is built upon a common architecture and user interface, it is easy for organizations to add new QRadar products to existing



The QRadar SIEM console configuration provides intelligence to keep users apprised of enterprise network activity. This architecture diagram also shows possible phase 2 and phase 3 expansion paths.

deployments. All software is pre-installed, enabling new products to be accessed through a simple license key activation. For example, some customers first deploy QRadar Log Manager and later upgrade to QRadar SIEM without touching any hardware.

When new versions of QRadar products are released, it is a simple process to upgrade existing QRadar products due to intelligent automation built into the QRadar Security Intelligence Platform.

Take advantage of high-availability and disaster-recovery features

Deploying QRadar solutions in a highly available configuration is straightforward. IBM provides a turnkey solution for high availability that provides fully automated failover and disk synchronization that removes guesswork, risk and complexity so users can focus on their security intelligence operations, not on their IT infrastructures.

You can further protect QRadar deployments against catastrophic physical damage by forwarding all collected event and flow data to secondary, disaster-recovery appliances hosted in a separate facility.

Leverage capabilities that support business security worldwide

In addition to offering a security intelligence platform that scales to the needs of large organizations, IBM also provides the geographic presence, expert services and broad partnerships that organizations need.

Geographic reach

IBM offers the geographic reach and experience necessary to serve national and multinational companies and government agencies around the world. With decades of experience and proven success across continents, IBM knows how to serve and support organizations worldwide. IBM maintains local teams in most countries, including world-class professional services and technical support resources. The IBM Business Partner network includes a wide set of partners well versed in local market needs, regulations and customs, and able to meet the needs of mid-market and small business clients.

Services and support capabilities

While product capabilities can define a solution's potential, the services that surround it help organizations realize that potential. IBM has developed exceptional capabilities in technical support, professional services and training—both in-house and throughout its global partner network.

IBM Software Services has the breadth, depth and reach to manage your service needs. You can leverage the deep technical skills of our lab-based software services team and the business consulting, project management and infrastructure expertise of the IBM Global Services team. Also, we extend our IBM Software Services reach through IBM Business Partners to provide an extensive portfolio of capabilities. Together, IBM provides the global reach, intellectual capital, industry insight and technology leadership to support a wide range of critical business needs.

Access to strong professional services offerings is key to the success of security intelligence solutions. IBM uses a proven methodology based on vast customer experience and provides a variety of support levels, from self-help to tiered levels of support services, enabling users to choose the one that best meets their needs.

These services are complemented by training courses that provide a comprehensive understanding of features and skills necessary to use QRadar solutions effectively. Courses include instruction on initial configuration, event and flow data collection, data searching and querying, report generation, and more.

Partner ecosystem

IBM maintains a global ecosystem of solution providers, resellers, distributors, services and integration partners to help organizations implement security intelligence deployments. Users benefit from these relationships to help ensure the success of installations ranging from the smallest to the largest security intelligence deployments in the world. The QRadar ecosystem is built upon partnerships of various types, including:

- **Strategic alliance, original equipment manufacturer (OEM) and technology partners:** These partnerships enable users to maximize the value of their existing network and security investments and vendor relationships. OEM partners provide private-label versions of solutions from IBM, while strategic alliance and technology partners have developed strong technology and business relationships with IBM that enable better product interoperability and improved solutions. Relationships are developed at the engineering, support and product levels for joint product testing, troubleshooting, superior documentation, faster data feeds and partner training.
- **Solution provider, reseller and distributor partners:** These partners participate in the IBM Security QRadar Alliance Partner Program and include many pre-eminent channel organizations in the security marketplace. They assist customers with requirements definition, purchasing, financing, deployment and support.
- **Services and integration partners:** These partners provide expert assistance in all phases of security intelligence deployments, using their own local and global expertise.

Learn from examples of customer success

Each customer uses QRadar platform products to address their unique security intelligence needs. The following use cases demonstrate how QRadar solutions have been deployed by some of the world's largest companies.

Fortune 500 defense contractor

Customer: The organization is a Fortune 500 defense and aerospace systems company with more than 70,000 employees worldwide.

Business challenge: This organization needed to protect its complex, geographically distributed network from advanced threats that targeted highly sensitive information. Because of the organization's size and the importance of detecting threats in real time, this customer required scalability for massive event volumes.

The QRadar solution: To meet these challenges, the organization deployed QRadar SIEM with QRadar QFlow Collector technology using 40 appliances across 25 locations worldwide to monitor and protect its critical network. The QRadar solution

provides enterprise-wide security intelligence to capture network activity and detect anomalies and threats. By not only aggregating all NetFlow protocol data but also performing content capture with QFlow data, the organization gained total visibility and the ability to correlate users, content, location and necessary telemetry to isolate the critical information from noise.

The organization relies on QRadar to process more than six billion events per day in one of the largest SIEM deployments in the world. The distributed QRadar solution processes 70,000 events per second, and can process bursts of more than 100,000 events per second—all fully correlated, not just written to disk. QRadar SIEM is an essential element of the organization's security operations center, providing 24×7 visibility and alerting for 20 security operations specialists located at the security operations center and in other locations worldwide.

Fortune Five energy company

Customer: This Fortune Five energy company has more than 50,000 employees worldwide.

Business challenge: This company needed to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), North American Electric Reliability Corporation (NERC) standards and numerous regulations in other countries. At the same time, it needed to monitor and analyze an average of two billion logs daily to protect itself from security threats.

The QRadar solution: The company addressed its regulatory compliance and security needs by deploying QRadar SIEM with QRadar QFlow Collector technology using 30 appliances globally. By correlating events, network activity, asset information and configuration data, the solution intelligently identified 25 to 50 high-priority offenses from the two billion daily events occupying 40 TB of aggregate storage. The solution serves 100 security users across four groups, while protecting 10,000 network devices, 10,000 servers and 80,000 user endpoints. Major technologies protected by QRadar SIEM include Oracle, SAP, Cisco and Juniper products. The company also uses the QRadar solution to monitor six million card swipes per day for PCI compliance and ensures the security of supervisory control and data acquisition (SCADA) systems for NERC compliance.

Fortune 200 retailer

Customer: The organization is a Fortune 200 retailer with more than 100,000 employees.

Business challenge: This organization needed to replace a failing competitive implementation quickly in order to ensure PCI DSS compliance for an upcoming audit. It also needed to identify security threats across its large network of stores and corporate computing assets.

The QRadar solution: The retailer rapidly implemented a QRadar solution and passed its PCI audit within 90 days of the start of implementation. The company deployed QRadar SIEM with QRadar QFlow and VFlow Collector appliances, using 15 appliances to monitor and correlate activity from 45,000 point-of-sale devices and 6,000 corporate IT assets. The distributed solution processes more than one billion logs per day, intelligently rationalizing this volume down to 30 high-priority offenses. QRadar was the only solution that met the organization's needs by analyzing NetFlow data and correlating it with security events via an easy-to-use console, while automatically creating tickets for their BMC Remedy IT Service Management Suite of products. QRadar SIEM is now used by the organization's security, operations and network engineering groups.

Conclusion

IBM provides organizations, businesses and government agencies with a security intelligence platform proven to deliver success at scale, backed by the business capabilities organizations demand for their unique critical security needs.

For more information

To learn more about the IBM QRadar Security Intelligence Platform, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2013

WGB03006-USEN-00