IBM Software
Thought Leadership White Paper

October 2014

Success that scales: Delivering security intelligence for organizations of all sizes

Meet your changing needs for security intelligence with fast, easy, cost-effective deployments of IBM Security QRadar solutions

Introduction

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. Whether motivated by financial gain or just the opportunity to wreak havoc, attackers are also increasingly sophisticated in their methods. In fact, many security breaches go completely undetected for months. A recent report found that 63 percent of organizations learn they are breached from an external source, and 38 percent of targets were attacked again once the original incident was remediated.[1]

Meanwhile, as attacks grow more advanced, it's increasingly important for organizations to be sure they have the right security tools in place. In addition to the costs associated with a potential data breach, IT and operational expenses can escalate when organizations don't have the flexibility and scalability to meet changing security requirements. And replacing ineffective, legacy tools can involve costly migrations.

Security information and event management (SIEM) tools provide a powerful way for organizations to detect the latest threats *before* they can cause damage. The right SIEM tools can combine massive amounts of data from network traffic, flows, logs, user behavior, security events and numerous other sources to automatically identify unknown or previously undetected threats. Using analytics, these tools can help find attackers lurking within the organization, as well as predict and prioritize security weaknesses for breach prevention, mitigation and remediation.

However, not all SIEM tools are created equal. For effective security that can last for the long term, your organization needs an integrated platform of security intelligence solutions that can adapt to your changing needs. The platform should enable your organization to:

- **Scale out:** Expand the solution 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, such as integrated risk management, vulnerability management and incident forensics

This white paper explains how IBM® QRadar® Security Intelligence Platform can meet all of these scalability needs. Whether you want to support a growing organization, add new capabilities or expand storage capacity and performance, IBM offers integrated solutions that can be deployed quickly, easily and cost-effectively for rapid time to value.

The state of the security landscape

Although large-scale security breaches get the most media coverage—and many others go unreported—the risks of attack are growing for organizations of all sizes. Today's threats are more sophisticated than ever. And even small organizations have increasingly complex IT environments, where large amounts of security data must be quickly collected and analyzed to help detect breaches, respond to them and prevent them from happening in the future.

The unfortunate truth is that the longer it takes to resolve an attack, the more financially devastating that attack can be. In a review of attacks on US-based organizations, the Ponemon Institute found that the average time to resolve a cyber attack was 32 days, with an average cost to organizations of more than

USD1 million; malicious insider attacks were found to take more than 65 days on average to contain, at a cost of approximately USD2.1 million.[2]

Meanwhile, IT organizations have increasingly limited budgets. They must deploy more effective prevention, detection and response capabilities in the most cost-effective manner possible. Rather than deploying another point solution, organizations need an integrated platform that can provide out-of-the-box security intelligence with rapid time to value—while also providing the scalability to quickly and easily meet new requirements.

Protection for today and tomorrow

IBM Security QRadar solutions provide a fast, easy, cost-effective way to meet your changing needs for security intelligence—without the cost and complexity of disparate compliance reporting, application monitoring and vulnerability scanning products. QRadar solutions offer integrated capabilities for log management, SIEM, data storage, incident forensics, full-packet capture, and risk and vulnerability management.

Featuring a single, highly scalable architecture, QRadar solutions are 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. Most software is pre-installed, enabling new solutions to be accessed through a simple license key activation. Plus, all QRadar solutions use the same integrated, intuitive, web-based user interface.

Real-time visibility

QRadar solutions are designed to monitor, correlate and store large volumes of data in real time. This next-generation SIEM technology 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.

With the centralized SIEM engine, QRadar users can transparently search data across distributed environments. Correlation can be performed both locally and globally, helping small organizations implement sophisticated analytics and large organizations stay a step ahead of the latest threats.

Search performance

As the size of a deployment grows, QRadar solutions have the processing power to enable rapid searches, analysis and reporting on security data spread across multiple locations. And with today's advanced threats, speed is a critical requirement for threat management. QRadar solutions provide high-performance indexing capabilities for extremely fast searches from within an intuitive user interface.

Plus, IBM Security QRadar Data Node is designed to cost-effectively add long-term data storage and expanded search processing capacity for QRadar deployments. Organizations can easily scale data storage and analysis performance on demand—without any complex disk or file reconfiguration. QRadar Data Nodes help organizations avoid the cost, complexity and potential performance issues of traditional storage area network (SAN) solutions. And the searches of historical data can result in more effective and efficient security insights.

Flexible deployment

QRadar Security Intelligence Platform also supports a variety of cloud-based deployment models. Organizations can start by deploying QRadar event collectors within the cloud to capture activities and alerts associated with hosted services and send them back for on-premises analysis. If connectivity and bandwidth issues are a concern, QRadar event and flow processors can be placed inside the cloud environment to perform the correlation analysis and send only offense conditions back to on-premises systems. Organizations with limited IT staff can also choose a complete cloud-based QRadar deployment with external access to the centralized management console.

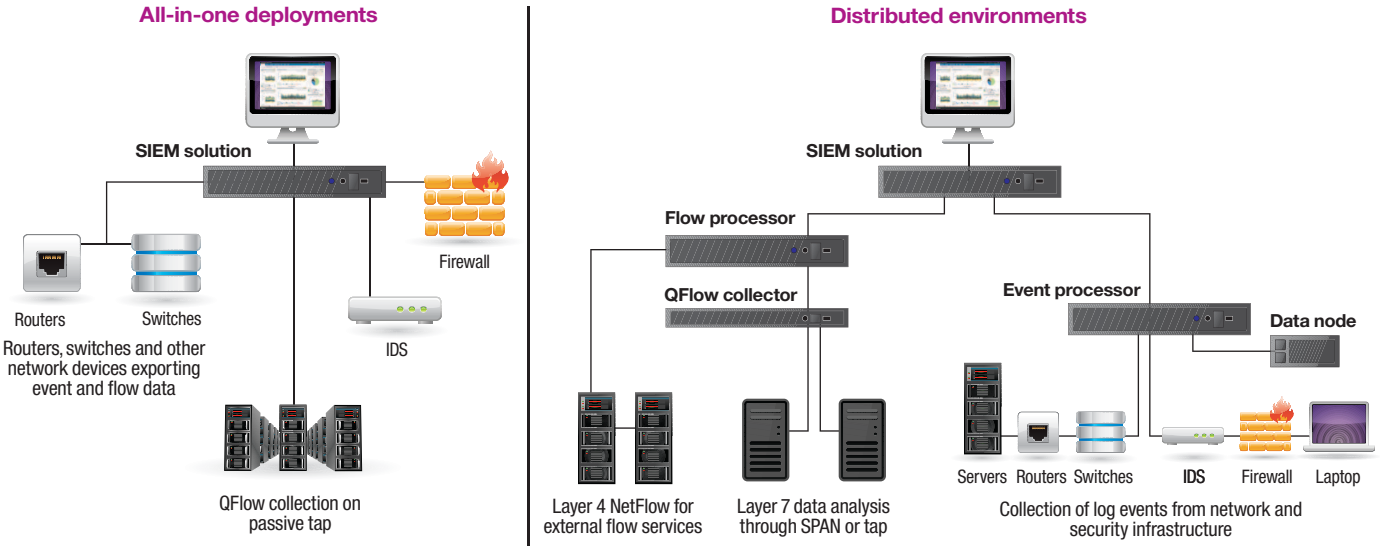
Scale out, from small to large

With QRadar solutions, 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.

QRadar solutions empower organizations with an incremental deployment approach. Security teams can begin with a single, all-in-one turnkey appliance and grow it over time into a highly distributed, console-based solution by adding multiple event processors, event collectors, flow processors, flow collectors and data nodes (for low-cost storage and search performance). In addition, QRadar flow collectors can be added for Layer 7 application-layer visibility and network flow analysis—even across virtualized and cloud deployments. The collectors can be deployed wherever required to support evolving network requirements.

QRadar can also scale to, and support, cloud deployments. For example, QRadar can be installed for cloud environments where the IT infrastructure has been moved to the cloud, but the QRadar console and event and flow processors all remain *on premises*. Application-specific QRadar modules can transfer events and flows in real time from the cloud workload through a secure connection to the customer data center. QRadar can then consolidate and analyze the data from both the cloud and on premises. In contrast, QRadar event and flow processors can also be located in the cloud, while the console remains on premises. In this scenario, data is transferred in real time through a secure connection to the client's data center for consolidation and analysis.

Scalable deployments with IBM Security QRadar



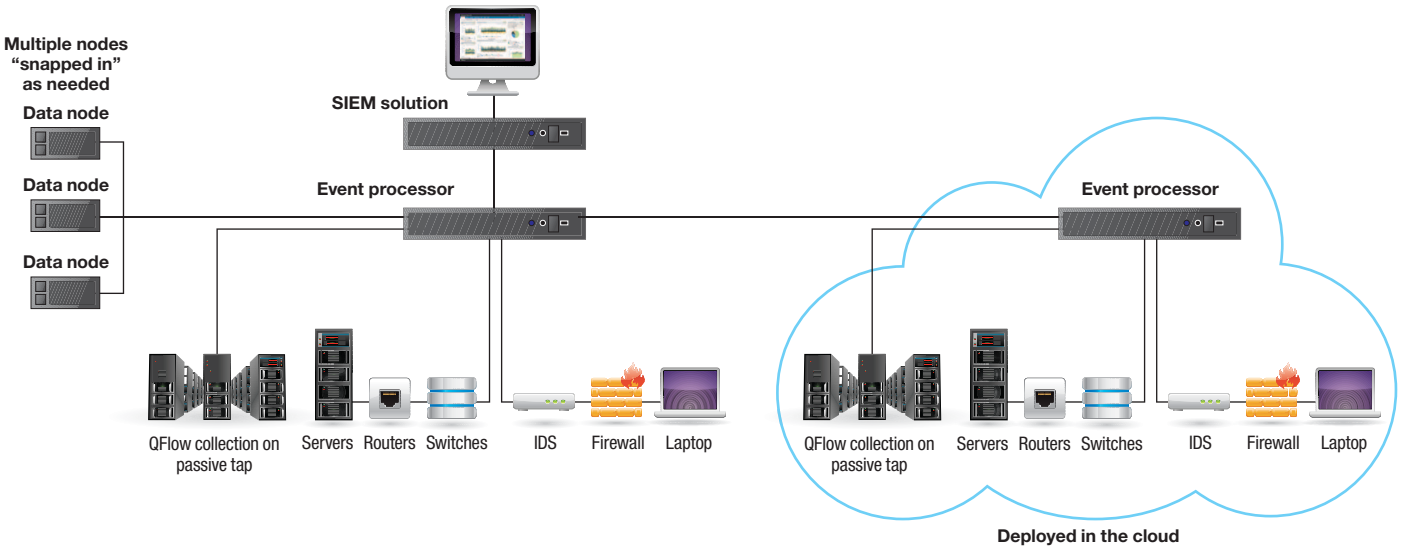
QRadar can also scale and be delivered *from* the cloud. For this type of deployment, QRadar is installed and configured in a cloud infrastructure, such as SoftLayer. QRadar event and flow processors reside both in the cloud and on-premises (the console is in the cloud), and they collect events and flows from applications running in both locations. Events and flows from the on-premises workload are forwarded on a real-time basis to QRadar in the cloud through a secure channel for consolidation and analysis.

Because QRadar solutions are built upon a common architecture, database and user interface, organizations can easily scale out their existing deployments. Security teams can access new capabilities from within the existing interface, after a simple license key activation. Intelligent automation also means that product upgrades are completely transparent, so staff can focus on more strategic activities.

Scale up for speed and capacity

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. Attackers are lurking within networks for longer periods of time, and security teams need to have fast access to historical data to help defend against these stealthy threats. To help boost the storage capacity and analytical processing performance of QRadar deployments, organizations can now use QRadar Data Node solutions for virtually unlimited, dedicated and cost-effective storage scalability. In fact, QRadar Data Node solutions can easily support up to petabytes worth of data for long-term retention.

Scalable SIEM storage with IBM Security QRadar Data Nodes



Here's how they work. QRadar event and flow processors store data and conduct searches on that data. QRadar Data Nodes can be added directly to those QRadar event and flow processors to add both low-cost storage and search processing capacity. QRadar Data Nodes receive and store events and flows, and they can actively participate in query operations, providing additional processing power and increased search performance. QRadar Data Nodes provide real-time data interpretation, correlation and alerts. Plus, they can transfer SIEM data at potentially millions of events per second without impacting normal operations.

Importantly, there is almost no limit to the number of QRadar Data Nodes that can be added to a QRadar deployment. In addition, intelligent algorithms automatically balance data across QRadar event and flow processors when a new data node is added, or rebalance when one is removed, in a manner that optimizes search performance and storage.

Basically, QRadar Data Node solutions enable organizations to keep data longer and add more querying horsepower—completely transparently. Unlike SAN solutions, no reconfigurations are required; log sources can stay the same; no changes are needed for correlation rules, reporting or SIEM integrations; and the user interface is unchanged.

Scale functionality within the same interface

In addition to expanding the size, speed and capacity of a SIEM deployment, organizations can also scale QRadar solutions along another dimension—functionality. This provides them with another way to get more value from an existing investment. Some key capabilities that can be added to the core SIEM solutions include:

- **Risk management**—for collecting configuration and topology data to proactively identify risks, simulate offenses and take corrective action *before* an attack occurs
- **Vulnerability management**—for identifying and prioritizing weaknesses so security personnel can take corrective action *before* an attack occurs
- **Incident forensics**—for quickly and easily investigating the step-by-step actions of an attacker, and supporting quick and effective remediation after an attack occurs

Risk management

IBM Security QRadar Risk Manager can be added onto an existing QRadar solution, enabling organizations to proactively manage network device configurations, improve compliance and manage risks. 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. And with automated monitoring, organizations can quickly discover configuration errors that may leave them exposed for attack. Additional capabilities include multi-vendor configuration audits, risk/compliance policy assessments and advanced threat simulation.

Vulnerability management

IBM Security QRadar Vulnerability Manager is another way to expand the proactive security capabilities of an existing QRadar solution—enabling security teams to view vulnerability data within the context of network usage, security and threats. Designed to consolidate results from IBM and non-IBM vulnerability scanners, risk management solutions and external threat intelligence sources, QRadar Vulnerability Manager provides a centralized control center for prioritizing security gaps and weaknesses for resolution. It supports periodic and dynamic network security scans, filtering of false positives and a full audit trail for compliance reporting.

Incident forensics

IBM Security QRadar Incident Forensics gives IT security professionals additional visibility into the "who, what, when, where and how" of a security incident. It helps eliminate the need for expensive, specialized forensics training, and offers an intuitive user interface capable of rapidly searching terabytes of network

flow data. 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.

Scalability success in the real world

Organizations of all sizes have successfully deployed QRadar solutions to meet their immediate security requirements, and the flexible QRadar architecture provides them with the room to grow to meet future needs. For example:

- **A small university in Virginia needed a scalable solution to help manage its escalating security events. Using QRadar solutions, the school was able to distribute processing across multiple appliances for performance scaling, use out-of-the-box correlation rules for rapid deployment and simplified administration, and utilize flow analysis to help detect and prevent suspicious network activity.**
- **A large financial services firm needed to help improve security across its different geographic locations. By deploying QRadar solutions, the firm gained centralized logging for billions of events per day, the ability to proactively manage risks and vulnerabilities, and easy-to-use incident forensics for investigating incidents and understanding how to prevent them in the future.**
- **A major telecommunications company needed to help ensure fast searching and access for more than 90 sites. Using QRadar solutions, the company benefited from a single, global view of its distributed environment, the ability to correlate massive amounts of security data, and scalable performance for searching, analysis, reporting and corrective action.**

Conclusion

As security threats grow increasingly sophisticated, organizations need to have the right tools in place for predicting and prioritizing security weaknesses for mitigation or remediation. Deploying multiple, independent security tools and disparate point solutions 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.

QRadar solutions are designed to provide the fast, easy, cost-effective way to meet changing security needs. The integrated solutions can scale over time in size, functionality and performance to help organizations stay a step ahead of attackers for many years to come.

For more information

To learn more about IBM Security QRadar solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/qradar

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM 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.

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
October 2014

[1] "M-Trends 2013: Attack the Security Gap," *Mandiant*, March 2013. https://www.mandiant.com/resources/mandiant-reports/

[2] "2013 Cost of Cyber Crime Study: United States," *Ponemon Institute*, October 2013. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

Please Recycle

WGW03073-USEN-00