IBM Security QRadar Vulnerability Manager for Government

Improve security and compliance by prioritizing security gaps for resolution through Continuous Diagnostics & Mitigation

Highlights

- Help prevent security breaches by discovering and highlighting high-risk vulnerabilities from a single, integrated dashboard
- Prioritize remediation and mitigation activities by understanding the complete network context
- Enable seamless integration with IBM® Security QRadar® SIEM to get dynamic, up-to-date asset information for proactive vulnerability management for Continuous Diagnostics & Mitigation (CDM)
- Conduct rapid scans across the network—periodically or dynamically—to find security weaknesses and minimize risks
- Automate regulatory compliance with collection, correlation and reporting

For many governmental Departments and Agencies, managing application, database, host and network vulnerabilities is a lesson in frustration. Vulnerability scans are typically conducted in response to compliance mandates, and they can reveal up to tens of thousands of exposures—depending upon network size. Scan results are often a complex puzzle of misconfigured devices, unpatched software, and outdated or obsolete systems. And security administrators must struggle to quickly identify, assess, determine operational risk, and provide security operations with respective courses of action to remediate or mitigate the exposures that pose the greatest risk.

At the same time, security breaches are dramatically increasing for all kinds of organizations. From e-commerce and social-networking giants to healthcare, universities, banks, governments and gaming sites, the breadth of breach targets is vast. While the number of disclosed vulnerabilities continues to rise, the number of incidents that result in the loss, theft or exposure of personally identifiable information has been increasing at a rate of nearly 40 percent.[1]

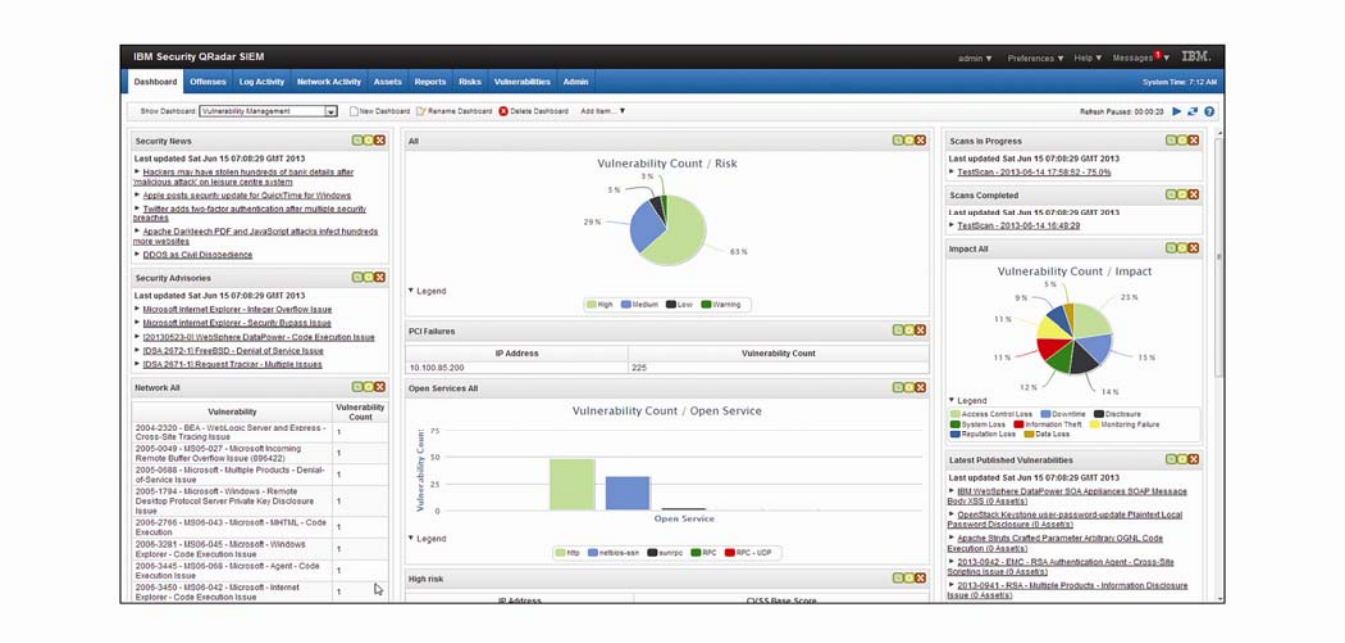
IBM Security QRadar Vulnerability Manager can help organizations minimize the chances of a network security breach by using a proactive approach to finding security weaknesses and minimizing potential risks. It uses a proven vulnerability scanner to collect up-to-date results, but unlike other solutions, it leverages the capabilities of IBM QRadar Security Intelligence Platform to present the data within the overall context of the network usage, security and threat posture. Designed to consolidate results from multiple vulnerability scanners, risk management solutions and external threat intelligence resources, QRadar Vulnerability Manager operates like a centralized control center to identify key security weaknesses that need to be addressed to help thwart future attacks.

QRadar Vulnerability Manager helps security and operational teams identify resource configuration issues, understand the impact of software patching schedules, coordinate with intrusion prevention systems to block open connections, and establish continuous monitoring of systems that can't otherwise be remediated—all from a single, integrated dashboard. By correlating vulnerability data with QRadar SIEM event and threat analysis, IBM Security QRadar Risk Manager device configuration and network traffic analysis, and external databases, including IBM X-Force® threat intelligence, QRadar Vulnerability Manager can help organizations build actionable plans for deploying their often constrained IT staffing resources. And since it is already integrated with QRadar Security Intelligence Platform, security teams have one less system to install, configure and manage.

Get a single, prioritized view of potential vulnerabilities

QRadar Vulnerability Manager is helping redefine how IT security and operational teams collect and use vulnerability assessment data—transforming a tedious monthly or quarterly scanning and reporting activity into an insightful, continuous monitoring program. Its intuitive user interface provides complete visibility across dynamic, multi-layered networks. Departments and Agency's can now:

- Select a dashboard view and click through related tabs to review security offenses, log events, network flows, asset statuses and configurations, reports, risks and vulnerabilities
- Create, edit and save asset searches and scans for more intelligent monitoring
- Make faster, more informed decisions with a prioritized, consolidated view of scan data
- Help coordinate patching and virtual patching activities, and direct intrusion prevention systems (IPSs) to block potential attack paths for maximum impact



IBM Security QRadar Vulnerability Manager provides a single, integrated dashboard for viewing multiple vulnerability assessment feeds and threat intelligence sources. This way, security teams can quickly identify the exposures that pose the greatest risk.

QRadar Vulnerability Manager includes an embedded scanning engine that can be set up to run both dynamic and periodic scans, providing near real-time visibility of weaknesses that could otherwise remain hidden. Leveraging the passive asset discovery capabilities of IBM Security QRadar QFlow and Log Collector appliances, any new asset appearing on the network can be immediately scanned. As a result, organizations can reduce their exposure to advanced threats between regular scanning cycles and help ensure compliance with the latest security regulations.

Using the same rules-based approach as QRadar SIEM, QRadar Vulnerability Manager helps minimize false positives and filters out vulnerabilities already defined as non-threatening. For example, using risk mitigation controls, applications may be installed on a server, but they may be disabled, and therefore not a security risk; devices that appear exposed may actually be protected by a firewall; or endpoints that have vulnerabilities may already be scheduled for patching.

QRadar Vulnerability Manager maintains a current network view of all discovered vulnerabilities, including details such as when the vulnerabilities were found, when they were last seen, what scan jobs reported the vulnerabilities, and to whom the vulnerability is assigned for remediation or mitigation. The software also presents historic views of daily, weekly and monthly trends, and it can produce long-term trending reports, such as the month-by-month trend of Payment Card Industry (PCI) failure vulnerabilities discovered over the past year.

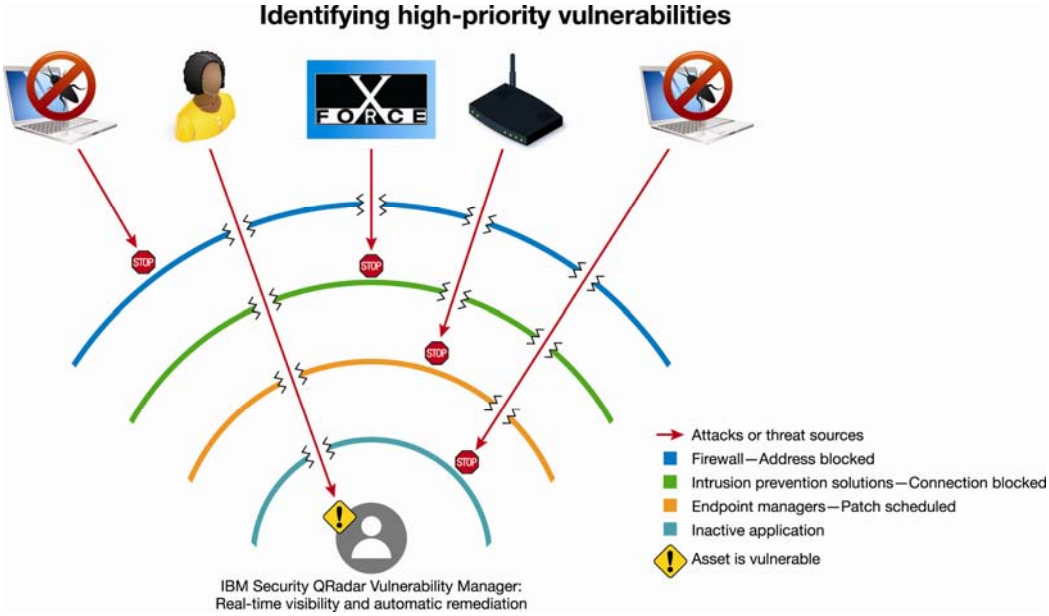
Stand-alone, independent vulnerability-scanning solutions can take considerable time to scan large address

spaces for assets, servers and services, and their scan results can be out of date quickly. These point solutions also require additional infrastructure and include different technologies for network, application and database scanning—all requiring additional and sometimes manual administration. And after identifying an often incomplete sea of vulnerabilities, the point solutions do not include any contextual information for helping security teams prioritize their tasks for remediation.

Thwart advanced threats

Unlike the random, brute-force attacks of the past, today's organizations must guard against sophisticated targeted attacks, so called "advanced persistent threats"—that is, a complex series of attacks that often take place over a prolonged timeframe. Using a range of tactics from zero-day exploits to custom malware to simply trolling for unpatched or misconfigured systems, these attackers consistently probe their targets using a "low-and-slow" approach until they find a security gap. Organizations can use more intelligent tools like QRadar Vulnerability Manager to improve their defenses by regularly scanning and addressing as many high-impact vulnerabilities as possible.

Most vulnerability scanners simply identify large numbers of exposures and leave it up to security and operational teams to understand the severity of risks. These tools are often not integrated with the existing security infrastructure and require additional manual effort to align with the current network topology, usage information and security processes. Many of these tools are used simply for compliance, rather than as an integral part of a threat and security management program. QRadar Vulnerability Manager simplifies security operations by integrating the scanning and remediation efforts into the security risk and mitigation efforts.



QRadar Vulnerability Manager uses security intelligence to help filter vulnerabilities. This enables organizations to understand how to prioritize their remediation or mitigation activities.

With QRadar Vulnerability Manager, organizations can:

- Leverage existing appliance infrastructure and security intelligence data to seamlessly conduct automated scans for network vulnerabilities
- Detect when new assets are added to the network, when assets start behaving abnormally, or when assets might be potentially compromised—using log events and network flow data—and perform immediate scans to help ensure protection and improve visibility
- Help improve productivity by enabling security and operational teams to focus on a small, manageable number of high-priority events, eliminating false positives and correlating results with network-blocking activities

Address compliance mandates

Regulatory requirements are forcing organizations of all sizes to develop vulnerability management programs to help ensure proper control of sensitive IT assets. QRadar Vulnerability Manager helps organizations facilitate compliance by conducting regular scans across the network and maintaining detailed audit trails. It categorizes each vulnerability with a severity rating and an exposure score. In addition to scanning assets both internally and externally, QRadar Vulnerability Manager enables security teams to create tickets to manage remediation activities and specify exceptions with a full audit trail.

With QRadar Vulnerability Manager, organizations can:

- Orchestrate a high volume of concurrent assessments without disturbing normal network operations—multiple stakeholders can scan and rescan the network as needed for remediation verification
- Summarize vulnerability assessments by day, week and month for effective reporting and visibility of trends
- Run scans from both inside and outside the network
- Capture an audit trail of all vulnerability management activities, including discovery, assignments, notes, exceptions and remediation

Extend your security intelligence

QRadar Vulnerability Manager combines the real-time security visibility of QRadar Security Intelligence Platform with the results of proven vulnerability-scanning technology. As part of the QRadar SIEM architecture, QRadar Vulnerability Manager can be quickly activated via a licensing key—requiring no additional hardware or software. This can result in considerable cost savings, since security teams do not normally have to deploy new technologies or learn a new interface. They can simply generate reports from within the familiar QRadar product family user interface.

Key integrations for QRadar Vulnerability Manager include:

- **QRadar SIEM:** Provides the appliance infrastructure for conducting network scans, the asset database for logging and tracking vulnerability management activities, the passive network detection capabilities for discovering newly added assets, and all the contextual security intelligence data needed to build and execute actionable vulnerability management plans
- **QRadar Risk Manager:** Reveals current and historical network connection data to show how vulnerabilities relate to the overall network topology—including how firewall and IPS rules affect the exploitability of specific assets from internal and external threat sources
- **IBM Security SiteProtector™ System:** Provides virtual patching capabilities using network IPS signatures to protect against exploits of identified vulnerabilities by blocking associated connections
- **X-Force threat intelligence feed:** Supplies up-to-date information on recommended fixes and security advice for active vulnerabilities, viruses, worms and threats
- **IBM Endpoint Manager:** Streamlines remediation tasks by automatically managing patches to hundreds of thousands of endpoints, including the latest mobile devices; provides integrated reporting for real-time monitoring of patch progress
- **IBM Security AppScan®:** Supports web application vulnerability assessments, enabling QRadar Vulnerability Manager to provide visibility and prioritization of web application vulnerabilities within its integrated dashboard
- **IBM InfoSphere® Guardium® Vulnerability Assessment:** Supports scanning of database infrastructure, enabling QRadar Vulnerability Manager to provide visibility and prioritization of database vulnerabilities within its integrated dashboard

Apply proactive security

In a world where no networks are truly secure, QRadar Vulnerability Manager enables organizations to more effectively protect their environments using an extensive line of proactive defenses, including:

- High-speed internal scanning, which helps preserve network performance and availability
- Support for discovery, non-authenticated, authenticated and Open Vulnerability Assessment Language (OVAL) scans
- External scanning capabilities to see the network from an attacker’s viewpoint and help facilitate compliance

- Single-click investigations from dashboard screens and deep, rules-based, rapid searching capabilities to learn more about specific events or identify long-term trends
- Suppression of acceptable, false positive or otherwise non-mitigated vulnerabilities from ongoing reporting
- Vulnerability assignment and remediation lifecycle management
- Full audit trail for compliance reporting

Why IBM?

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 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information

To learn more about IBM Security QRadar Vulnerability Manager, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/software/products/us/en/category/SWI60

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, June 2013

“IBM X-Force 2012 Trend and Risk Report,” *IBM Security Systems,* March 2013. http://www-03.ibm.com/security/xforce/downloads.html