IBM QRadar Vulnerability Manager

Improve security and compliance by identifying security gaps and risks for resolution

Highlights

- Help prevent security breaches by discovering vulnerabilities and risks from a single, integrated dashboard
- Prioritize remediation and mitigation activities by understanding network context
- Enable seamless integration with IBM® Security QRadar® SIEM to get dynamic, up-to-date asset information for proactive management of vulnerabilities and risks
- Conduct rapid network scans periodically or dynamically to find security weaknesses and minimize risks
- Visualize current and potential network traffic patterns with a network topology model based on security device configurations
- Quantify and prioritize risks with a policy engine that correlates network topology, asset vulnerabilities, and actual network traffic, enabling risk-based remediation
- Model threat propagation and simulate network topology changes to help improve security
- Centralize network security device management to help reduce configuration errors and simplify monitoring of firewall performance

For many organizations, managing network vulnerabilities and risks 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 Scan results are often a complex puzzle of misconfigured devices, unpatched software, and outdated or obsolete systems.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 and 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 of exposure of personally identifiable information has been increasing at an alarming rate.

IBM 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.

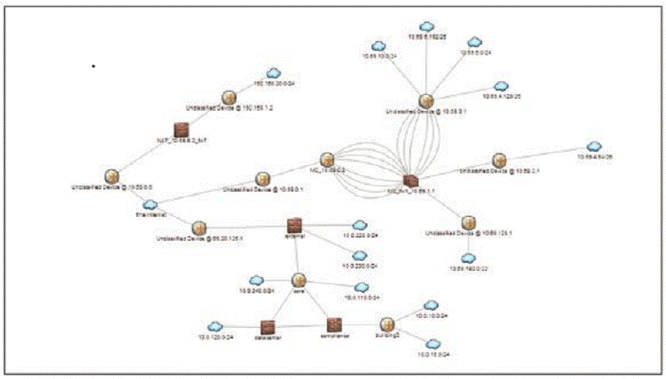
It also correlates network topology information using data from IBM QRadar SIEM including asset configurations, network events and flow patterns. This provides valuable insights revealing, for example, which assets and vulnerabilities are causing the most risk, so IT staff can prioritize their remediation tasks. QRadar Vulnerability Manager can also help identify firewall and intrusion prevention (IPS) misconfigurations that may allow attackers into the network and create inefficiencies in devices.

Many network attacks succeed simply due to inconsistent network and security configuration practices, highlighting the need for automated network configuration monitoring and alerts for policy breaches. QRadar Vulnerability Manager offers an integrated, automated, policy-based approach that can greatly improve an organizations' ability to assess information security risk through a single console shared with QRadar SIEM. It leverages a broad range of risk indicators including asset, network and security configuration data, network activity data, network and security events, and vulnerability scan results. It also provides other key capabilities that include the assignment of risk scores, vulnerability risk assessment, and correlation of known vulnerabilities with network topologies. It helps deliver a prioritized list of vulnerabilities to better assess which systems are most vulnerable to attack and should be remediated first. QRadar Vulnerability Manager also delivers advanced threat modeling , and the simulation and visualization of the potential spread of threats through the network by leveraging vulnerability, network topology and connection data.

QRadar Vulnerability Manager helps security 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, 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

- 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



The QRadar Vulnerability Manager topology viewer enables users to view network devices and relationships, including subnets and links

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 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 classified as nonthreatening. For example, applications may be installed on a server, but they may be inactive, 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 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 "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 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 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.

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 network scans 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.

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 deployed quickly and security teams do not need to learn a new interface. They can simply generate reports from within the familiar QRadar family user interface.

Apply Proactive Security

- High-speed internal scanning, which helps preserve network performance and availability
- Support for discovery, non-authenticated, uthenticated 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 this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

May 2017