DATA SHEET

Extreme Networks Security Analytics G2 – Vulnerability Manager

Improve security and compliance by prioritizing security gaps for resolution

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 Extreme Networks SIEM to get dynamic, up-to-date asset information for proactive vulnerability management
- Conduct rapid network scans—periodically or dynamically—to find security weaknesses and minimize risks
- Automate regulatory compliance with collection, correlation and reporting

For many organizations, managing 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 Scan results are often a complex puzzle of misconfigured devices, unpatched software, and outdated or obsolete systems.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 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 organizations, 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.

Extreme Networks Security 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 Extreme Networks Security Analytics 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, Vulnerability Manager operates like a centralized control center to identify key security weaknesses that need to be addressed to help thwart future attacks

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 SIEM event and threat analysis, Risk Manager device configuration and network traffic analysis, and external databases, Vulnerability Manager can help organizations build actionable plans for deploying their often constrained IT staffing resources. And since it is already integrated with Security Analytics Platform, security teams have one less system to install, configure and manage.

Get a Single, Prioritized View of Potential Vulnerabilities

Vulnerability Manager is helping redefine how IT security 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. Organizations can now:

Vulnerability Manager provides a single, integrated dashboard for viewing multiple vulnerability assessment feeds and threat intelligence sources

- 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

Vulnerability Manager includes an embedded scanning engine that can be set up to run both dynamic and/or periodic scans, providing near real-time visibility of weaknesses that could otherwise remain hidden. Leveraging the passive asset discovery capabilities of Flow 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.

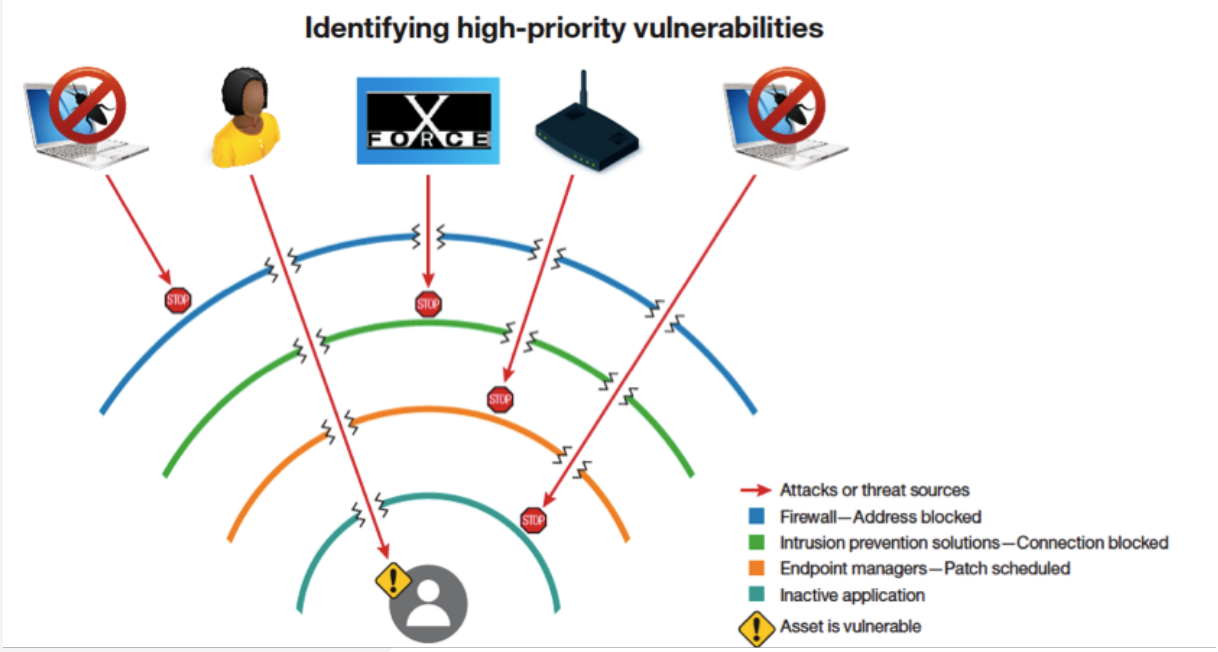
Using the same rules-based approach as SIEM, Vulnerability Manager helps minimize false positives and filters out vulnerabilities already classified as non- threatening. For example, applications may be installed on a server, but they may be inactive, and therefore not a security risk; devices that appear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

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



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

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 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 With 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 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. 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, Vulnerability Manager enables security teams to create tickets to manage remediation activities and specify exceptions with a full audit trail.

With 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

Vulnerability Manager combines the real-time security visibility of Security Analytics Platform with the results of proven vulnerability-scanning technology. As part of the SIEM architecture, 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.

KEY INTEGRATIONS FOR VULNERABILITY MANAGER:

Security Information & Event Management (SIEM) & Log Management: 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.

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.

Extreme Networks Security Threat Protection G2 Site Manager: 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.

Apply Proactive Security

In a world where no networks are truly secure, 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

Technical Specification for Extreme Networks Security Vulnerability Manager

MODEL	VIRTUAL	APPLIANCE
Description	Extreme Networks Security Vulnerability Manager G2 VM	Extreme Networks Security Vulnerability Manager G2 Appliance
Form Factor	-	2 RU Appliance
Processor	2 vCPU minimum required	Intel Xeon E5-2620 V2, 2.6GHz, 6 Core, 15MB Cache (x2)
Memory	16 GB minimum required	64 GB
Hard Disk	500 GB minimum required	6.2 TB usable

Ordering Information

PART NUMBER	NAME	DESCRIPTION
89067	SVMG2-SA-APL	Extreme Networks Security Vulnerability Manager G2 Standalone Appliance (Base 255 scanning assets + 50 EPS Log Management) (No Integration with other SIEM or LM products)
89068	SVMG2-SA-VIR	Extreme Networks Security Vulnerability Manager G2 Standalone VM License (Base 255 scanning assets + 50 EPS Log Management) (No Integration with other SIEM or LM products)
89069	SVMG2-ONBOX	Extreme Networks Security Vulnerability Manager G2 ON BOARD for Console or All-in-One SW License
89070	SVMG2-OFFBOX-APL	Extreme Networks Security Vulnerability Manager G2 OFF BOARD for Console or All-in-One Appliance (Base 255 scanning assets)
89071	SVMG2-OFFBOX-VIR	Extreme Networks Security Vulnerability Manager G2 OFF BOARD for Console or All-in-One VM SW License (Base 255 scanning assets)
89072	SVMG2-ADD256	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 256
89073	SVMG2-ADD1K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 1024
89074	SVMG2-ADD2K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 2048
89075	SVMG2-ADD4K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 4096
89076	SVMG2-ADD8K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 8192
89077	SVMG2-ADD16K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 16384
89078	SVMG2-ADD32K	Extreme Networks Security Vulnerability Manager G2 Scanning Assets Increase by 32768

POWER CORDS
In support of its expanding Green initiatives as of July 1st 2014, Extreme Networks will no longer ship power cords with products. Power cords can be ordered separately but need to be specified at the time order. Please refer to www.extremenetworks.com/product/powercords/ for details on power cord availability for this product.

Warranty

As a customer-centric company, Extreme Networks is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Extreme Networks Security Analytics Appliances come with a one-year warranty against manufacturing defects. For full warranty terms and conditions please go to: http://www.extremenetworks.com/support/warranty.aspx.

Service & Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs.

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800