Data Sheet

Juniper Secure Analytics Vulnerability Manager

Product Overview

As a member of the JSA Series of Secure Analytics Appliances family, Juniper Secure Analytics Vulnerability Manager helps organizations minimize the chances of a network security breach by using a proactive approach to finding security weaknesses and mitigating potential risks. Using Juniper Secure Analytics Vulnerability Manager, organizations can conduct rapid network scans, discover and highlight high-risk vulnerabilities from a single integrated dashboard, and automate regulatory compliance with powerful collection, correlation, and reporting tools.

Product Description

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 Scan results are often a complex puzzle of misconfigured devices, unpatched software, and outdated or obsolete systems.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

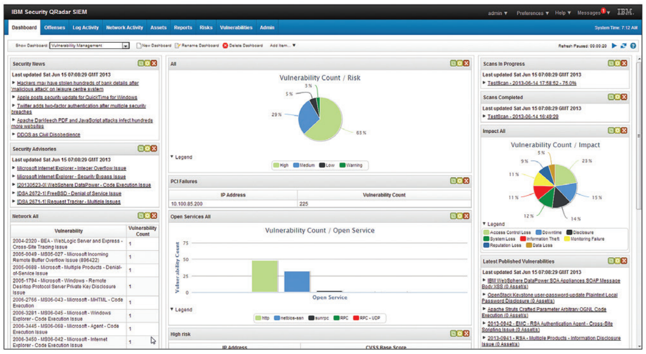
Juniper Secure Analytics Vulnerability Manager consolidates results from multiple vulnerability scanners, risk management solutions, and external threat intelligence resources, operating like a centralized control center to identify key security weaknesses that need to be addressed to prevent future attacks. It uses a proven vulnerability scanner to collect up-to-date results, but unlike other solutions, it leverages the capabilities of Juniper Networks® JSA Series Secure Analytics Appliances to present the data within the overall context of the network usage, security, and threat posture.

Juniper Secure Analytics Vulnerability Manager helps security teams identify resource configuration issues, understand the impact of software patching schedules, and coordinate with intrusion prevention systems (IPS) 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 the JSA Series Secure Analytics family's event and threat analysis capabilities, Juniper Secure Analytics Risk Manager device configuration and network traffic analysis, and external databases, including IBM X-Force threat intelligence, Juniper Secure Analytics Vulnerability Manager can help organizations build actionable plans for deploying their often constrained IT staffing resources. And since it is already integrated with the JSA Series Secure Analytics portfolio's security intelligence platform, security teams have one less system to install, configure, and manage.

Architecture and Key Components

Juniper Secure Analytics 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. Because its intuitive user interface provides complete visibility across dynamic, multilayered networks, organizations 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 (IPS) to block potential attack paths for maximum impact



Security News

Last updated Sat Jun 15 07:08:29 GMT 2013

- Hackers may have stolen hundreds of bank details after 'malicious attack' on leisure centre system
- Apple posts security update for QuickTime for Windows
- Twitter adds two-factor authentication after multiple security breaches
- Apache Darkleech PDF and JavaScript attacks infect hundreds more websites
- DDOS as Civil Disobedience

Security Advisories

Last updated Sat Jun 15 07:08:29 GMT 2013

- Microsoft Internet Explorer - Integer Overflow Issue
- Microsoft Internet Explorer - Security Bypass Issue
- [20130523-0] WebSphere DataPower - Code Execution Issue
- [DSA 2672-1] FreeBSD - Denial of Service Issue
- [DSA 2671-1] Request Tracker - Multiple Issues

Network All

Vulnerability	Vulnerability Count
2004-2320 - BEA - WebLogic Server and Express - Cross-Site Tracing Issue	1
2005-0049 - MS05-027 - Microsoft Incoming Remote Buffer Overflow Issue (896422)	1
2005-0688 - Microsoft - Multiple Products - Denial-of-Service Issue	1
2005-1794 - Microsoft - Windows - Remote Desktop Protocol Server Private Key Disclosure Issue	1
2006-2766 - MS06-043 - Microsoft - MHTML - Code Execution	1
2006-3281 - MS06-045 - Microsoft - Windows Explorer - Code Execution Issue	1
2006-3445 - MS06-068 - Microsoft - Agent - Code Execution Issue	1
2006-3450 - MS06-042 - Microsoft - Internet Explorer - Code Execution Issue	1

All

PCI Failures

IP Address	Vulnerability Count
10.100.85.200	225

Open Services All

High risk

IP Address	CVSS Base Score

Scans In Progress

Last updated Sat Jun 15 07:08:29 GMT 2013

- TestScan - 2013-06-14 17:58:52 - 75.0%

Scans Completed

Last updated Sat Jun 15 07:08:29 GMT 2013

- TestScan - 2013-06-14 16:49:29

Impact All

Latest Published Vulnerabilities

Last updated Sat Jun 15 07:08:29 GMT 2013

- IBM WebSphere DataPower SOA Appliances SOAP Message Body XSS (0 Asset(s))
- OpenStack Keystone user-password-update Plaintext Local Password Disclosure (0 Asset(s))
- Apache Struts Crafted Parameter Arbitrary OGNL Code Execution (0 Asset(s))
- 2013-0942 - EMC - RSA Authentication Agent - Cross-Site Scripting Issue (0 Asset(s))
- 2013-0941 - RSA - Multiple Products - Information Disclosure Issue (0 Asset(s))

Figure 1. Juniper Secure Analytics Vulnerability Manager provides a single, integrated dashboard for viewing multiple vulnerability assessment feeds and threat intelligence sources; security teams can quickly identify the exposures that pose the greatest risk.

Juniper Secure Analytics 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 passive asset discovery capabilities of the QFlow and Log Collector features in JSA Secure Analytics 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 is used across the JSA Series Secure Analytics product family, the Vulnerability Manager helps minimize false positives and it 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.

Juniper Secure Analytics 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 quickly become out-of-date. 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 Juniper Secure Analytics 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.

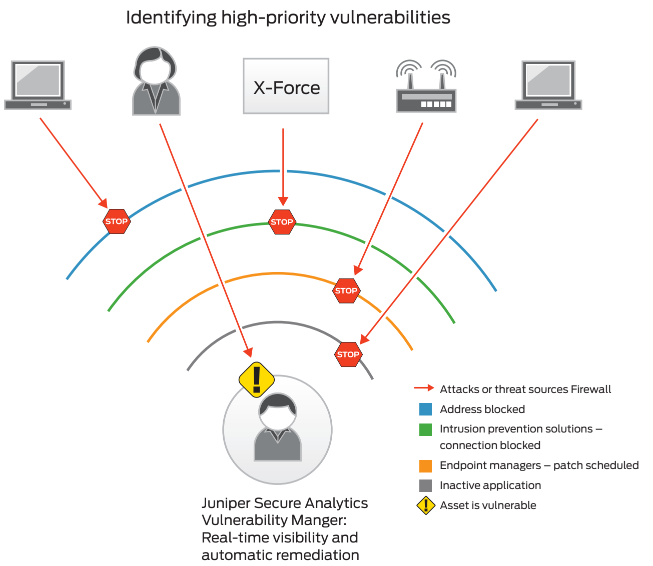


Figure 2. Juniper Secure Analytics Vulnerability Manager uses security intelligence to help filter vulnerabilities; this enables organizations to understand how to prioritize their remediation and mitigation activities.

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

With Juniper Secure Analytics 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 Security Intelligence

Juniper Secure Analytics Vulnerability Manager combines the real-time security visibility of JSA Series Secure Analytics Appliances with the results of proven vulnerability scanning technology. As part of Juniper's Secure Analytics architecture, Juniper Secure Analytics 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 JSA Series Secure Analytics product family user interface.

Key integrations for Juniper Secure Analytics Vulnerability Manager include:

- JSA Series Secure Analytics Appliances: 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
- Juniper Secure Analytics 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
- 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, Juniper Secure Analytics 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 life cycle management
- Full audit trail for compliance reporting

Features and Benefits

- Helps prevent security breaches by discovering and highlighting high-risk vulnerabilities from a single, integrated dashboard
- Prioritizes remediation and mitigation activities by understanding the complete network context
- Enables seamless integration with JSA Series Secure Analytics Appliances to get dynamic, up-to-date asset information for proactive vulnerability management
- Enables rapid network scans—periodically or dynamically—to find security weaknesses and minimize risks
- Automates regulatory compliance with collection, correlation, and reporting

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

To learn more about how Juniper Secure Analytics Vulnerability Manager can benefit your organization, please contact your Juniper Networks representative and visit www.juniper.net.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPer NETWORKS