FIREMON

WHITE PAPER

AUTOMATED, REAL-TIME RISK ANALYSIS AND REMEDIATION

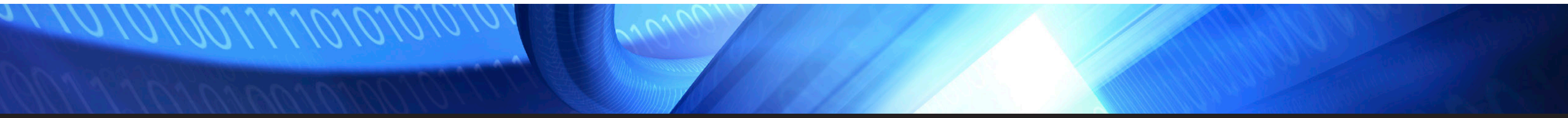
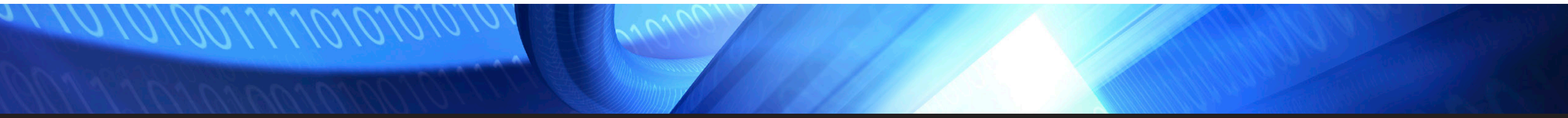


Table of Contents



Executive Summary

Managing risk within today's enterprise network environments represents a significant challenge. Enterprises have more IP addresses, servers, mobile phones, partners, applications and data than ever before. Since each of these target systems can be vulnerable, enterprises have more vulnerabilities than ever before. This increased exposure has been reflected in the press coverage of breaches over the last 24 months, with 2011 and 2012 seeing the most significant media coverage of high profile breaches in years.

In their 2012 annual Chief Information Security Officer Assessment, IBM noted that external threats are now viewed by the majority of CISO respondents as the primary security challenge they face. The traditional reactive approach to risk is no longer effective in mitigating the vulnerabilities within an enterprise. A real-time, proactive approach that automates risk management is needed to empower today's enterprises to effectively identify and remediate the actual assets that are subject to risk within their networks.

Vulnerability Scanners Alone Are Not Enough

Traditionally, when enterprises have wanted to address the risk posture of their networks, vulnerability scanners have been the "go to" solution. Vulnerability scanners are a key tool within the security toolbox, and a valuable resource all organizations should leverage.

Vulnerability Scanners can produce a significant list of vulnerabilities within enterprise environments, with customers seeing 10,000 vulnerabilities or more identified in the scan results. These results can be an overwhelming amount of risk to attempt to address and mitigate, causing many organizations to either ignore the vulnerabilities or to engage in an attempt to identify the most serious vulnerabilities and remediate them, with the hopes that lesser vulnerabilities will not be exploited.

As Verizon Business noted in its white paper, "Data-centric Vulnerability Management," there are too many vulnerabilities to remediate with vulnerability scanners, noting, "With traditional vulnerability management assessments, organizations are generally provided with lengthy reports listing vulnerabilities, and too many are identified as "high" or "critical." Because of the overwhelming number of identified vulnerabilities, it's extremely challenging to determine how to handle so many issues, when the potential impact of each vulnerability is unclear."

Vulnerability Scanner providers have reacted to the overwhelming amount of data that scanners can generate. Most commercial scanners today allow organizations to identify the value of their internal assets, and will then rank the scan results based on the highest value assets that have the most severe vulnerabilities. While this somewhat improves the ability of an organization to attempt to prioritize their remediation efforts, it lacks a critical element in identifying what assets are truly at risk. The scanners lack the full context of the network topology, how data flows through the network and what mitigating security controls might be in place.

With this perspective, consider the following scenario:

- An organization designates a web server that processes credit card transactions as a high value asset, and an internal windows database server running a one-off database specific to the workgroup using it as a low value asset.
- The vulnerability scanner identifies a severe SQL vulnerability on the web server, and lists it as one of the top vulnerabilities within the network based on its asset value. Conversely, the scanner identifies an UPnP vulnerability on the Windows Server, and lists it as a low value vulnerability.
- Based on these rankings, an organization may determine that it should immediately remediate the SQL vulnerability on the web server, and possibly remediate the Windows Server if time permits.

In the above scenario, there are several factors that the vulnerability scanner is unable to process. The scanner is not aware that a firewall sits in front of the web server, and denies all SQL traffic to the web server from any external or internal resource. The scanner is also not aware that a firewall administrator pushed a new policy to the firewall that controls access to the Windows Server, and due to a mistake by the firewall admin, the Windows Server is now reachable from external sources using any service, including UPnP.

Without incorporating the awareness of the network security controls in place, vulnerability scanners alone are unable to identify what specific assets are truly at risk, and which assets require immediate remediation actions. Combining the full context of the network topology and network security controls with the results of the vulnerability scanner greatly improves the accuracy of the risk picture. However, there is one more key to truly enabling proactive, real-time automated risk analysis and remediation.

Real-Time Change Configuration Notification is the Key to Risk

Change happens. In today's enterprise network environments, change happens continuously. Change requests for applications, hardware, software, network or partner connections can result in both network and security teams constantly having to make changes to the topology of the network and the associated security controls. Getting real-time notification of these changes is the key to identifying the true risk posture of any environment. Risk solutions that either manually import the device configurations or poll the devices on an hourly or daily basis to detect configuration changes are unable to provide true real-time risk analysis.

Consider the previous example of the Windows Server running a one-off database with a UPnP vulnerability. The firewall admin pushes the new policy that accidentally enables external sources to connect with the database server with any service, including UPnP, at 9:10am. If a risk tool that polls the devices on an hourly basis were deployed, it would not detect the change to the firewall policy and update the risk state accordingly until 50 minutes later. Without real-time notification of changes to network and security devices, real-time risk analysis can not be achieved.

FireMon Security Manager with Risk Analyzer: Risk Solved

FireMon's Security Manager version 6.0 with the patented Risk Analyzer module provides the world's first complete Security Posture Management Solution that provides real-time risk analysis and remediation. Security Manager connects to your organization's firewalls, routers, switches and load balancers, and provides real-time configuration change detection and alerting that is automatically fed into the Risk Analyzer module.

As changes occur they update the risk assessment, which provides real-time analysis and prioritized remediation recommendations. This real-time topology and network security configuration is combined with the output of vulnerability scanners to highlight exactly what assets are currently at risk, and provides a prioritized list of remediation actions that is based on what reduces the greatest amount of risk with the least amount of effort.

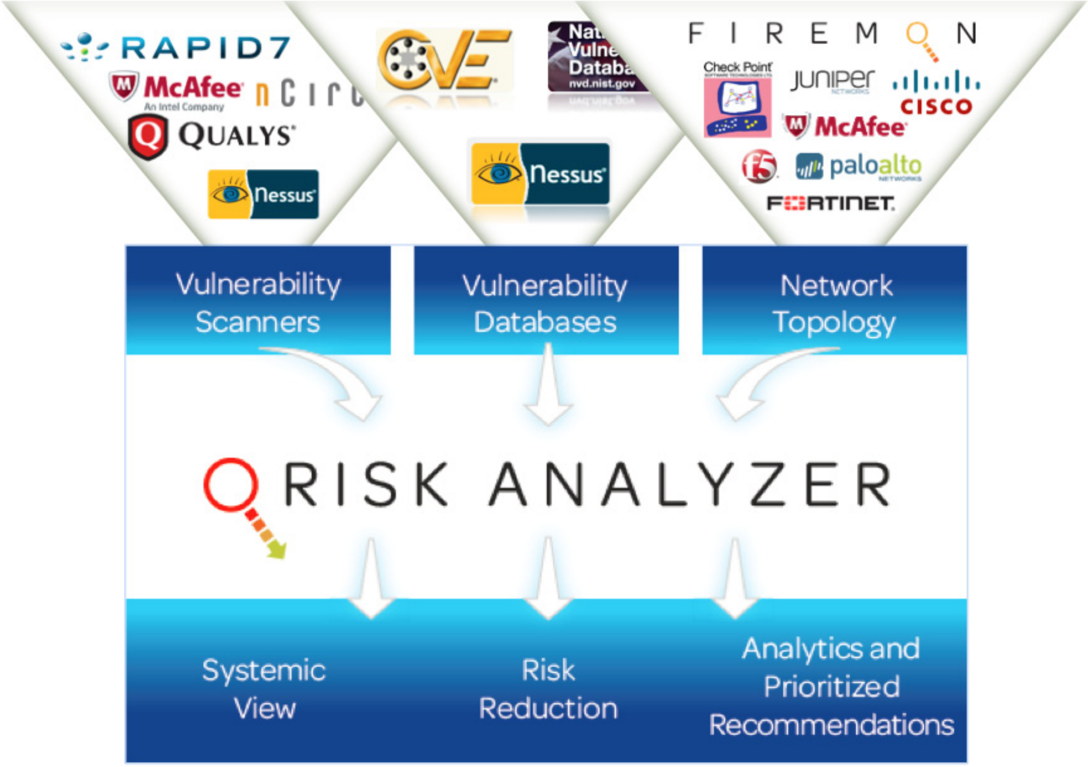


Image 1: Risk Analyzer System Architecture

Risk Analyzer reduces your organization's risk exposure in several ways, providing a proactive defense that allows the security team to stay one step ahead:

- It shows network security managers how attacks propagate throughout the network and where best to stop them at the perimeter.
- It helps vulnerability managers to prioritize their efforts and eliminate the greatest risk with the least effort.
- It helps CIOs to measure current exposure, direct the department's work effectively and decrease an organization's risk.

Security Manager with Risk Analyzer can also proactively alert security teams to the risk that requested changes could create within the network. By integrating Risk Analyzer with FireMon's Policy Planner tool, organizations can learn what risk a new firewall rule would introduce to the network before actually deploying the rule, enabling security teams to provide factual, data-based reasons as to why a change request should or should not be allowed.

Security Manager with Risk Analyzer provides a graphical attack path that enables organizations to see the possible paths an attacker might use across the network layout. See quickly where you can stop an attack with the least amount of time and effort.

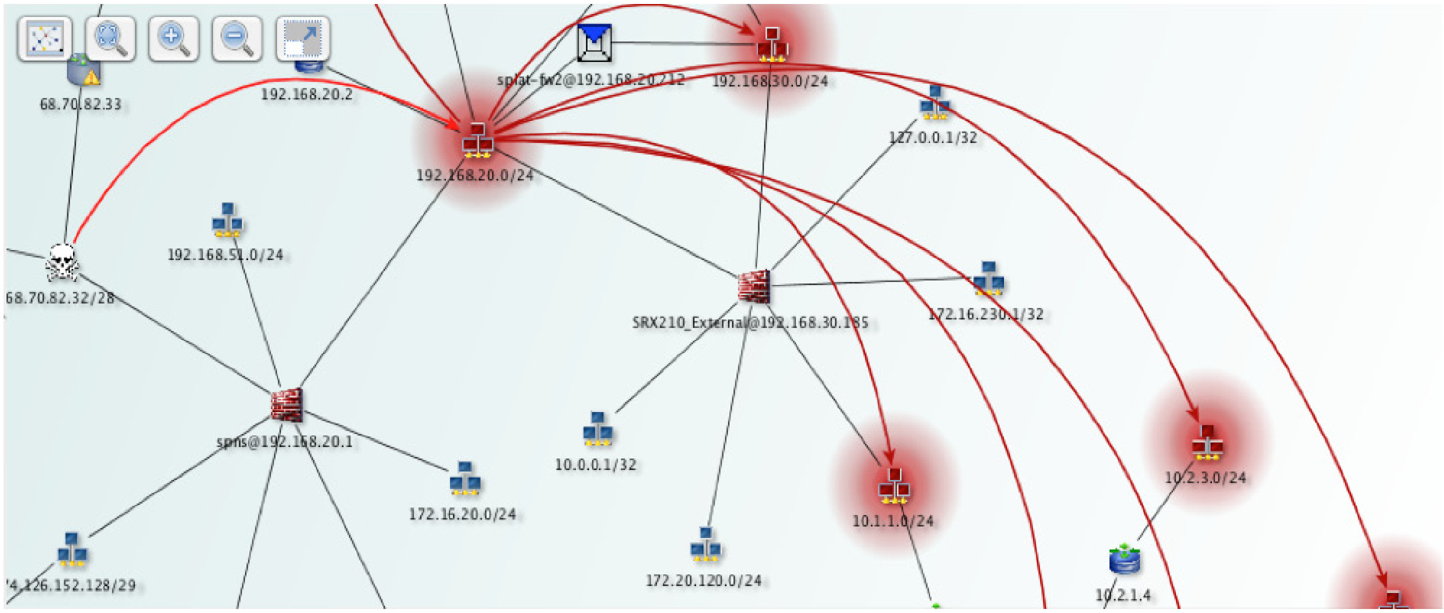


Image 2: Visualize real-time enterprise network risks

STOP ATTACKS FROM PROPAGATING

Multi-level attacks are difficult to identify and prevent. A Risk Analyzer attack graph shows how an attacker can penetrate the network and where on the perimeter to stop the attack.

PRIORITIZE VULNERABILITIES

Risk Analyzer provides a segmented and prioritized list of the vulnerabilities that present the greatest risk and will reduce danger most when they are countered.

MEASURE RISK

Risk Analyzer provides a concrete measurement of network risk based on simulated attacks. It gives decision makers the high-level data needed to take decisive action.

INTEGRATE PENETRATION TESTING

In combination with Metasploit from Rapid7, Risk Analyzer identifies and visualizes critical security holes and maps them against known exploits to demonstrate meaningful threats to specific environments. Security Operations Center analysts can use this closed-loop system for identifying, modeling and validating specific risks to work effectively and reduce operating costs.

PROACTIVE “WHAT IF” SCENARIOS

A powerful analysis engine lets you patch systems virtually and re-run a complete analysis in seconds. Compare various patch scenarios to ensure that your patch efforts have the most impact.

MAINTAIN NETWORK PERFORMANCE

Risk Analyzer scales as the number of hosts increases to maintain network performance even as threats multiply.

Conclusion

As the threat landscape explodes due to increasing infrastructure complexity and sophisticated attack vectors, organizations need to leverage tools that can automate the identification of what assets are truly at risk in real-time. John Sawyer, in an article for Dark Reading entitled “Tech Insight: Practical Threat Intelligence” noted that “Being able to keep up with changing technology, emerging threats, and information overload that goes with managing thousands to tens of thousands of systems requires proactive efforts on the part of security pros.” Sawyer also highlights that “security teams are being forced into developing threat intelligence operations to react quickly and mitigate new vulnerabilities as they crop up.”

FireMon Security Manager 6.0 with Risk Analyzer is the only solution on the market today that provides the required threat intelligence to identify exactly what assets are at risk, and what remediation actions will reduce the greatest amount of risk. Security Manager’s real-time configuration change detection ensures that the risk analysis is never in an out-of-date state, and provides organizations the assurance that their efforts are focused on what is truly at risk within their environment.

For more information on FireMon’s complete product portfolio, please visit the company’s website at www.firemon.com or email FireMon at info@firemon.com.