FireMon's Security Manager V7.0 Release Expands Value to Enterprises and Service Providers

Abstract

Network complexity is one of the biggest threats to IT security assurance, and nowhere is this threat more evident than in the enterprise, nor more significant than in assuring confidence in network security systems themselves. With the introduction of Security Manager 7.0 and Policy Planner 3.0 announced in February 2013, FireMon specifically targets enterprise and Managed Security Service Provider (MSSP) concerns. Building on the combination of risk analysis and network security posture management developed through Security Manager versions 6.0 and 6.1 released in 2012, this latest FireMon release introduces the continuous assessment capability needed in complex networks, best-practices modeling that embraces a control-oriented rather than device-oriented approach, business process technology standards for integrating with change management and service support, and other features that give enterprises and MSSPs a platform aligned with the more strategic approach required to manage large or complex environments. Enterprise Management Associates (EMA) summarizes these new capabilities in light of the value that complex network security configuration control brings not only to enterprise security, but also to the reliability and performance of IT in delivering business priorities at scale.

Background and Context

As enterprise networks have grown in complexity, so too has the complexity of network security. Firewalls, intrusion prevention systems (IPS), unified threat management (UTM) appliances and other network security tools do more than guard the perimeter. Security today demands compartmentalization and zoning of networks to contain threats and isolate areas of high sensitivity.

As this complexity has grown, so too has the challenge of management. Without tools that can bring order to potential chaos, well-intentioned efforts to protect sensitive IT content and functionality can add to the problem rather than help. Complex configurations can actually introduce risk exposures if not evaluated carefully and in detail—and not only on any individual device, but also in the context of how one device handles traffic relative to others in the network. The mis-ordering of rules, for example, can expose risk that administrators believe they have resolved. Vulnerabilities that cannot be patched or reconfigured may be protected by network security point products—but only if administrators are aware that the exposure exists.

These factors have given rise to the market of tools that automate the assessment of complex network security configuration, providing insight into exposures that help organizations better protect their networks and create device policies that are more effective, with fewer conflicts or unintended exposures. These tools do more than reduce risk. They can also reduce the number of network availability and performance issues resulting from security configuration problems, enhancing their value by increasing IT's performance in serving the business.

FireMon has become a recognized name in this growing market. Its founders bring their insight into complex network security configuration from experience with recognized security service providers such as IBM, HP, CSC, Symantec, and Dell. This experience has given FireMon its distinctive focus on meeting enterprise-class needs, in a market driven by the complexity that grows with scale.

In 2011, FireMon broadened its capabilities with the acquisition of Saperix, expanding its assets into the domain of security risk assessment and attack path identification. Today, the FireMon portfolio includes products such as Security Manager, Risk Analyzer and Policy Planner, delivering deep and detailed visibility into network policy and configuration issues, security risk exposures, pre- and post-change rule analysis, rule and object documentation and usage analysis (including the ability to reveal hidden rules), security topology awareness, traffic flow analysis, audit and reporting support, and other features that distinguish FireMon's enterprise-class approach. The ability of this approach is further demonstrated in capabilities that appeal to large-scale service providers as well, such as analysis of permissions in multi-tenant environments and distributed data collection needed to deliver cloud computing.

In mid-2012, FireMon introduced its sixth major version of its Security Manager software that married its security policy management capabilities with the risk analysis ability to identify network access paths that expose vulnerabilities and measure their impact, acquired with Saperix. With the late 2012 release of Security Manager version 6.1, FireMon expanded these capabilities with a new Access Path Analysis (APA) feature that analyzes the traversal of packets through a device, from source interface and route through destination route and interface, with analysis of NAT and security policy applied. Results include an assessment of whether the packet reached its destination, and how the firewall handled it in transit.

Version 6.1 also expanded FireMon's ability to visualize and analyze network security configuration with FireMon Insight. Insight is a core capability of Security Manager provided in a Web portal to enable quick, broad access to the operational analysis capabilities. Insight delivers an intuitive visualization of network configuration information across a diversity of point products, unifying the representation of configuration data in a REST-based Web dashboard. Insight also introduces the FireMon Query Language (FMQL) that exposes a consistent syntax for understanding devices and device properties, rules and policies, regardless of supported vendor.

Announcement Highlights

With the seventh release of Security Manager announced in February 2013, FireMon further targets enterprise concerns with new capabilities designed to align with the strategic approach essential to focusing the management of security in large and complex networks.

Best Practice Modeling and Continuous Assessment

Security practices and regulatory requirements alike often highlight the need for assessing the adherence of networks to expected security policy and configuration requirements. The problem with such requirements, however, is that one-time assessments or snapshots in time may miss transient exposures or leave the organization vulnerable until a subsequent assessment identifies a gap. Continuous assessment has arisen as a strategy for closing such gaps, but in large or complex networks, change may happen so frequently that important exposures may be overlooked unless they can be identified in detail and remediation prioritized whenever important issues arise. In truly large/complex environments, this may be all but impossible without automation.

In Security Manager 7.0, FireMon introduces capabilities that enable organizations to achieve both conformity with recommended practices and continuous monitoring of adherence to security objectives.

With FireMon's built-in Controls library, businesses can define policy, analyze environment-specific risks and maintain records of previous mitigations. The FireMon knowledgebase equips organizations with pre-packaged assessments, enabling organizations to move immediately to a higher level of maturity leveraging the experience of FireMon at a wide array of enterprise deployments. Custom assessments can also be defined when needed. These capabilities equip organizations with a more comprehensive focus on consistency in practices that make a difference, rather than a device-by-device approach that may lead to discrepancies in policy definition and deployment – and resulting risk exposures.

The Continuous Assessment capability introduced in Security Manager 7.0 allows organizations to monitor adherence to these objectives and track progress toward greater environment security. With the selection of an assessment and identification of devices or device groups to be monitored, version 7.0 automates continuous assessment, providing organizations with detailed reports via dashboards and individual notifications delivered as frequently as required. The realities of enterprise policy management are evident in capabilities such as exemption whitelisting when needed, and the ability to trend findings such as common control failures by device, assessment or severity over time. This supports a more strategic approach to security management, by revealing where efforts to enhance security may best be applied.

Business Process Standardization

A comprehensive approach to environment management must integrate the various capabilities involved. Assessment must be united with the ability to effect change when needed. In the enterprise, specialized tools for these functions are not uncommon – particularly when organizations require best-of-breed solutions in specific domains, or in the frequent case where established approaches have become well defined. Enterprises simply cannot discard tools that have proven their worth to accommodate new capability.

FireMon has recognized this reality in this latest release, in its embrace of the Object Management Group's (OMG) Business Process Model and Notation (BPMN) standard. According to FireMon the newly announced Policy Planner 3.0 is the first policy and risk management platform to embrace the BPMN 2.0 standard. Embracing this standard for business process definition recognizes an additional reality of enterprise network and security management: Security, compliance or audit teams may conduct assessments, but making changes to the production environment typically falls under the direct control of IT operations. There are valid reasons – for operational as well as security and compliance purposes – for maintaining these distinctions. Separation of Duties (SoD) requires that those who evaluate security should be distinguished from those who make actual changes. Preserving the reliability and performance of IT, meanwhile, requires operational expertise. By supporting integration through business process standardization, FireMon recognizes these realities that foster greater adoption of strategic security monitoring and assessment in the enterprise.

Standardization also enables easy modification of FireMon Policy Planner 3.0 to integrate with existing enterprise workflow solutions. Custom workflows can be developed from BPMN 2.0-compliant task types, with support for parallel approval path forks, escalation timers, decisions, notifications and user inputs. Changes can be assessed for policy conformity as well as potential operational issues prior to implementation – a key advantage of network assessment technology. Adherence to the BPMN standard further supports adaptability, enabling capabilities from the correlation of ad hoc queries to ticket-related fields, to the development of dashboard widgets that reveal open ticket counts and technician assignments for more efficient resource management.

Enhanced Domain and Authentication Support

Enterprises are not the only organizations likely to value features of this latest FireMon release. Service providers, for example, must manage *multiple* client environments – and must keep those environments distinct from each other. FireMon Security Manager 7.0 provides new Domain configurations that support the management of segregated environments in parallel, keeping each domain's vulnerability data, custom assessments, zone definitions and device configurations isolated from each other.

FireMon's authentication capabilities further support Domain isolation. Users with appropriate privileges can share "global" assessments across domains, but each domain's custom values remain hidden from others. Users and groups can be limited to specific domains, giving a service provider's customers the latitude to manage their own environments as needed.

Additional authentication features introduced in Security Manager 7.0 include the mapping of Security Manager group mappings to LDAP groups, supporting the correlation of LDAP-native user and group memberships to FireMon privileges by simply adding LDAP groups to an existing Security Manager role.

EMA Perspective

The market of tools for complex network security policy and configuration assessment has become very active in recent years. Its momentum has attracted participation from those focused on risk, such as RedSeal Networks and Skybox Security, and given rise to direct FireMon competitors such as Tufin and AlgoSec. FireMon has maintained its strength in this space with a focus on scalability and performance for the enterprise born out of the practical experience of its founders—a strength needed to tackle the complexity of enterprise networks that drives this market.

This discipline could not be more fundamental to security. In EMA analyses of enterprise security and IT operations management practices, those who demonstrate a high degree of maturity in configuration and change control also show measurably better performance in security outcomes—as well as superior performance in improved IT change outcomes, more efficient IT staff performance, more IT projects completed on time and within budget, and other business benefits. In one such study of more than 200 organizations worldwide, EMA found that those that achieved all four milestones of:

- Defining their configuration and change control processes,
- Actually implementing those processes in operation,
- Monitoring the environment for adherence to those priorities and detecting deviations when they occur, and
- Responding quickly to address these deviations and assure their remediation

also reported half the median incidence of "disruptive" security incidents—those requiring unplanned resources to resolve.[1] If configuration is this critical to IT security, how much more so the configuration of devices and systems deployed specifically to keep the network safe?

FireMon has been a pioneer in technologies that not only recognize the importance of this challenge, but the scale of complexity in enterprise networks and the variety of security point products that substantially increase risk. With this latest release of its platform, FireMon challenges its growing range of competitors on both the risk and complexity management fronts, with new features that make the most of the distinctive commitment to the enterprise that has characterized the FireMon approach.

[1] *IT Risk Management: Five Aspects of High Performers that Set Them Apart*, EMA Advisory Note, July 2011.