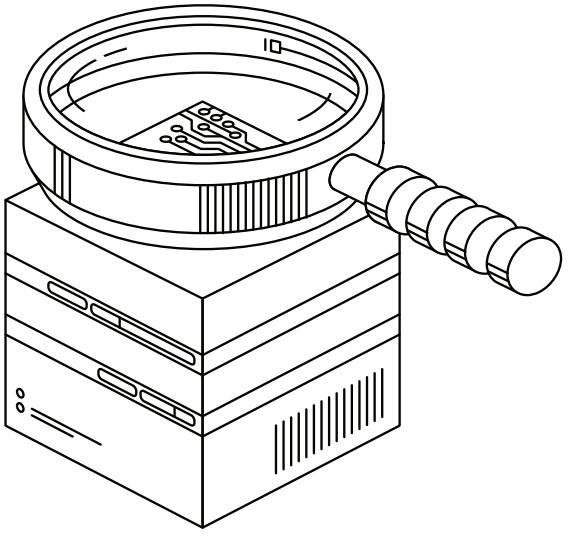
FIREMON

Security Manager

Optimizing Network Security Management through Continuous Assessment

Enterprise networks continue to increase in complexity, and threats to networks are more severe than ever

> Protecting these environments takes more than great technology; it takes effective and continuous management. Without the right systems in place, that can be a costly and time-consuming undertaking. FireMon Security Manager addresses the inherent complexity and changing requirements of today's enterprise networks by providing continuous visibility into network security devices and policies



What Is Security Manager?

FireMon Security Manager offers real-time visibility into network security infrastructure, including key indicators of device complexity, policy change and related risk. A scalable architecture and intuitive user interface ensure that security practitioners in any enterprise have the actionable data they need to quickly adapt network defenses to changing business demands and emerging threats.

Security Manager allows you to see your network at a dashboard-level glance with analysis, trending and key performance indicator widgets on a customizable dashboard and monitor network traffic behavior – down to the application level – to isolate overly permissive configurations. You can trace every available access path across the network and visualize relationships between network devices to identify risk access points and visualize and interact with highly complex network security environments or segmentations. With Security Manager, you can effectively isolate, document and alert on every ongoing change implemented throughout your existing firewall policies while defining and employing unique security controls for customized, repeatable analysis and reporting on your firewall policies.

The Security Manager platform was designed to address the three biggest challenges in firewall monitoring and management:

Clean Up

Analyze firewall configurations to identify hidden, unused, shadowed or overly permissive rules.

Compliance

Validate policies against regulatory requirements including PCI DSS 3.2, and against custom-defined policies - test what's important to you.

Change

Automate policy change workflow and scope the impact of proposed changes.

Solution Overview

The core capabilities of the Security Manager platform provide detailed, customizable network security analytics and real-time assessment of policy enforcement from an easy–to–understand dashboard to the entire network infrastructure.

01 FIREWALL RULE ASSESSMENT & OPTIMIZATION

Track utilization, effectiveness and efficiency of every rule on every firewall to eliminate complexity and optimize performance.

02 GRAPHICAL ATTACK PATHS

Trace the possible paths an attacker might use across the network and identify where you can stop an attack with the least amount of time and effort.

03 AUTOMATED CHANGE MANAGEMENT

Speed up root-cause analysis and improve effectiveness of initial change with automated change alerts, stakeholder assignment, impact analysis and full documentation

04 ACCESS PATH ANALYSIS

Trace every available access path across the network and visualize relationships between network devices to identify risky access points and adjust related rules and configurations.

05 POLICY COMPLIANCE AUDITS

Validate firewall configurations and report on compliance for internal audits and controls, as well as regulatory requirements, including PCI DSS 3.0, HIPAA, NERC-CIP and SOX. Custom-design assessments based on network segment, firewall type, and geographic locations.

06 NETWORK SECURITY VISUALIZATION

Maintain detailed visibility into current network security infrastructure via detailed dashboards, reports, maps and automated alerts.

NEW IN SECURITY MANAGER:

Omni Search
Quickly search all devices, policies and rules within the enterprise from a single place in the application

NGFW Support
Account for NGFW capabilities with application-level awareness and reverse application engineering.

Device Pack SDKs
Create device packs to integrate emerging technologies directly into Security Manager.

WHY SECURITY MANAGERT?

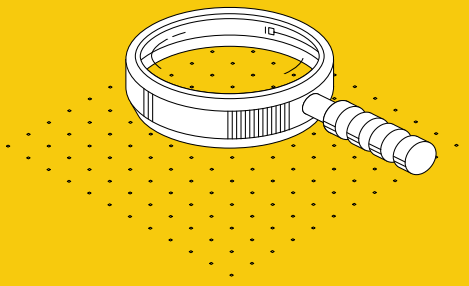
Maintain continuous visibility into existing network devices and security policies.

USE SECURITY MANAGER TO:

- Optimize firewall policy rule sets
- Map network-wide policy and access
- Validate and report on policy compliance
- Detect and report on policy changes
- Ease migration to next-generation firewalls

FEATURES:

- Traffic Flow Analysis
- Access Path Analysis
- Customizable Reporting
- PCI DSS 3.0 Assessment
- Network Map Visualization
- Advanced API Integration



FIREMON

Learn more about our solutions: www.firemon.com

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA

P: 1.913.948.9570
E: info@firemon.com