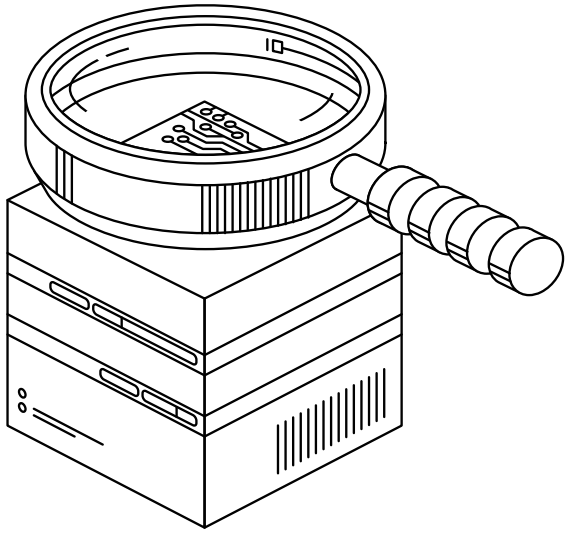
FIREMON

Security Manager

Establish control over complex security infrastructures with continuous, enterprise-wide visibility into network configurations.



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.

Three add-on modules extend the capabilities of the Security Manager platform to include change management, rule review and recertification and risk analysis.

Policy Planner

Automates the change workflow process from the change request to rule design, staging, implementation and verification.

Policy Optimizer

Automates rule review and recertification, linking security teams with policy owners and documenting rule justification for continuous assessments and audits.

Risk Analyzer

Analyzes vulnerabilities and their potential impact on assets using device configuration data and vulnerability feeds and then prioritizes them for remediation.

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 AUTOMATION OF MANUAL TASKS

Streamline compliance auditing and validation processes by using automation to demonstrate that net work access controls are in place at all times and are being tested frequently.

02 DASHBOARD-DRIVEN USER INTERFACE

Provides continuous management visibility into devices, complexity and compliance using web-based user interface that provides dashboard-driven, click-through reporting across the entire enterprise in a single pane of glass.

03 UNMATCHED IN-DEPTH ANALYSIS

Provides conclusive, in-depth assessment of network security infrastructure using Elasticsearch that filters and slices global rule base using any combination of over 200 filter criteria, returning results in sub-seconds with the capacity to query thousands of devices at a time.

04 UNMATCHED SCALABILITY

Security Manager distributes functions across multiple applications servers to perform simultaneous analysis and normalization across multiple platforms from multiple vendors, while splitting out reporting functions on a dedicated appliance.

05 UNMATCHED DATA RETENTION

Security Manager stores every piece of data received indefinitely without any system performance degradation.

06 DEEPEST VISIBILITY

Traffic Flow Analysis (TFA) features live traffic flow data and broader policy/rules search criteria, providing greater insight into the applications that are traversing a particular security rule.

07 REAL-TIME CHANGE ANALYSIS

We know the who, what, when of every change that happens to monitored devices in real time. No need to poll devices to determine configuration changes.

08 NGFW SUPPORT

Supports seamless migration support for application-centric policies for NGFW monitoring, policy implementation and management systems.

WHY SECURITY MANAGER?

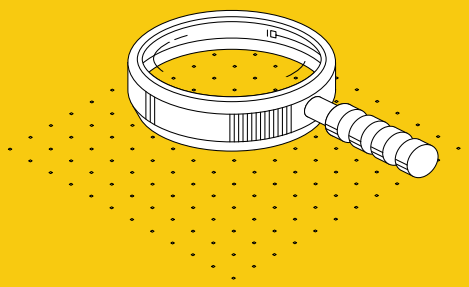
Maintain continuous visibility into existing network devices and security policies.

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 Assessment
- Network Map Visualization
- Advanced API Integration
- High-Speed, Comprehensive Search



FIREMON

Learn more about our solutions: www.firemon.com

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

REV 071917