

Security Manager

Comprehensive firewall rule management to reduce risk, manage change, and enforce compliance

As networks become more complex with the ever-growing number of new devices, applications and cloud services, it becomes nearly impossible to manage firewall policies and rules. A typical enterprise environment has millions of rules and just one simple misconfiguration in any one of them can lead to devastating consequences such as compliance violations, outages, and even data breaches.

Reduce Risk

Manage risk with real-time visibility and control

Organizations often face challenges with managing security policies, including a lack of visibility into policy-related risk, poorly configured policies, complexity, inability to detect changes, and lack of documentation. The best way to combat cybersecurity attacks and breaches is to identify and address vulnerabilities before they are exploited.

FireMon reduces risk by providing real-time risk evaluations, prioritizing rules that violate custom business rules, industry best practices, and rules that are identified as critical vulnerabilities. It also offers risk and threat modeling, recommends patches for identified problems and provides tools to prevent attacks before they happen. Additionally, FireMon's risk prevention guardrails evaluate every new rule and change in real-time to ensure they don't create new policy-related vulnerabilities.

Manage Change

Avoid misconfigurations, accelerate business, and improve security

Changing firewall rules and security policies isn't a glamorous task, but the consequences of getting it wrong can be quite severe. A simple misconfiguration can block legitimate users to mission critical services or can let the wrong folks in, exposing the organization to attack.

FireMon manages change by monitoring policy changes across the entire environment, on any device, on-premises or in the cloud, and identifies any potential impact on the organization. Its workflows streamline the process of new rule creation and changes to existing policies, reducing the time it takes to deploy rules and does it accurately the first time around. FireMon also fully automates the deployment of policy changes with its best-in-class automation tools allowing changes to happen at the push of a button and be fully implemented in a matter of minutes.

Enforce and Maintain Compliance

Avoid violations, avoid risk, and avoid fines

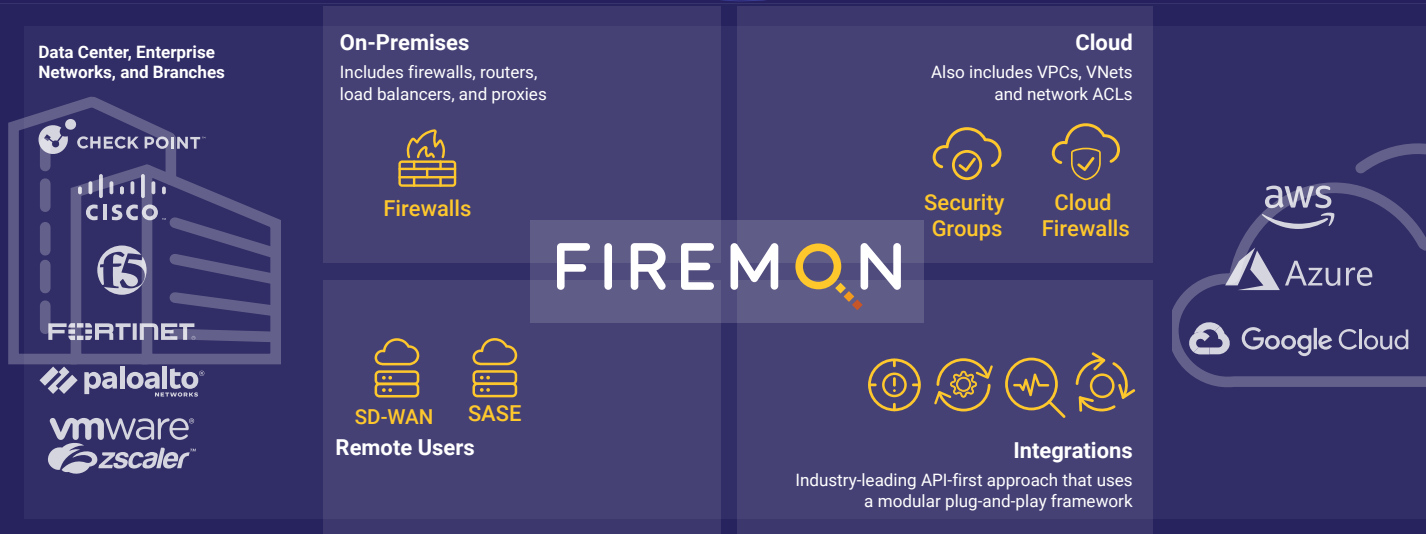
Ever-changing regulatory and internal security policy requirements make it a struggle to maintain compliance, especially for large organizations with complex, multi-vendor firewall and hybrid cloud environments. Manual processes introduce errors, slow audits, and increase the risk of fines and lawsuits.

FireMon helps organizations enforce and maintain compliance by offering highly customizable compliance reporting that can

Automate Firewall and Cloud Security Policy Management

FireMon's Security Manager is a purpose-built network security policy management (NSPM) platform that automates the management of firewall and cloud security policies to eliminate policy-related risk, accurately and quickly change rules, and meet internal and external compliance requirements.

generate reports in minutes, saving your team time and headaches. Additionally, FireMon provides the only real-time violation detection solution for policy compliance, alerting users before any violations are deployed. FireMon also automates the process of recertifying or decertifying firewall rules, ensuring continuous monitoring and removal of rules that are no longer needed or serve no purpose according to compliance, business, or security policies.



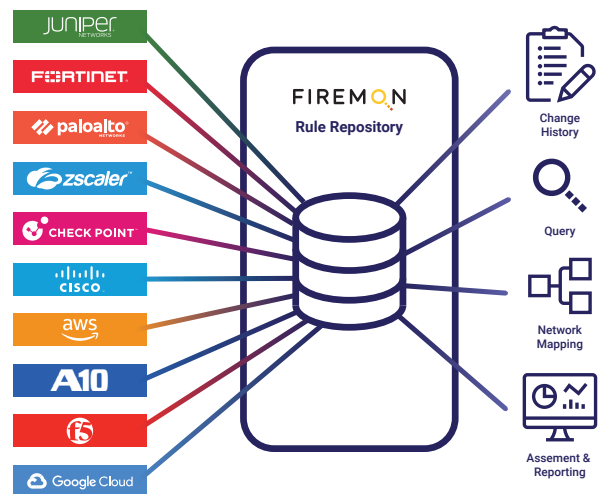
FireMon's Security Manager integrates across the entire environment from the data center to the cloud.

Security Manager Features

FireMon's Security Manager was purpose-built with the key features needed to support complex enterprise environments.

Real-Time Inventory of Devices and Rules

Rule repository is at the core of FireMon's Security policy management platform. This critical component serves as the centralized warehouse for every device, policy, and rule across the entire environment. It automatically identifies and imports information into a rule repository and supports over 80 vendors and versions. The platform translates this information into a common, normalized rule database that powers various functions such as audit tracking, change management, network mapping, and reporting.



FireMon gathers devices, policies, and rules from across the entire environment and normalizes them into a single rulebase.

Search Across the Entire Environment

FireMon enables you to search policies across your entire environment from a single console using the same structure and naming conventions. Our proprietary Security Intelligence Query Language (SiQL) enables searching network policies across various elements in the platform, including workflows and users, and returns real-time results in less than 10 seconds. SiQL is comprehensive, customizable, granular, and fast, making it suitable for highly complex enterprise environments.

Consolidated Compliance and Risk Assessments

With over 20 preconfigured compliance and assessment reports that can be customized, or new ones created using over 500 preconfigured criteria checks, FireMon's reporting capabilities are unmatched. FireMon's unified dashboard provides a real-time assessment of risk posture across the entire environment and highlights potential and actual compliance violations and vulnerabilities. The platform also offers access path analysis, "what if" attack assessments, and integrations with vulnerability scanners like Qualys, Rapid7, and Tenable for deeper insight on policy-related risks. Vulnerability scanner and risk/threat modeling is an optional add-on for enhanced security.

Simplify Rule Creation and Updates

FireMon's rule management tools simplify rule creation and updates with insights and visibility across the network space. The platform provides a detailed recommendation on device changes needed to successfully deploy new rules or update existing ones, and automatically evaluates them for risk and compliance violations before deployment. FireMon's workflow management system integration with leading ITSM systems allows changes to be made manually or deployed automatically to affected devices immediately or during approved change windows.

Rule Review and Recertification

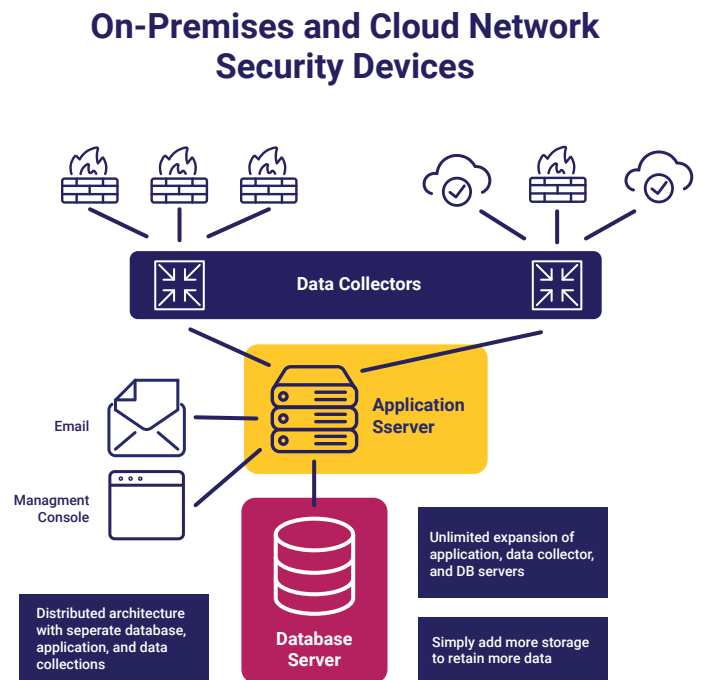
FireMon's optional policy lifecycle management feature ensures existing rules are assessed regularly with automated workflows that send rules to policy owners for review. Whether it's periodic reviews every 6 months for PCI-DSS compliance, or reviews triggered by our SiQL searches, the platform sends rule review emails asking owners to review the rule. The owner then has the option to recertify or decertify the rule at hand. Flexible workflows adapt easily to the needs of any business and track all information needed to make compliance audits a breeze.

API-First for Maximum Integration Flexibility

FireMon offers native and API-based integrations with various security vendors, such as IBM, Rapid7, AWS, and Azure, and our API-first approach exposes all platform elements and functionality via Swagger-based APIs. With FireMon, the need for professional services to set up our platform in your environment is significantly reduced.

Architecture Built for Scale

FireMon's Security Manager is designed to meet the needs of complex enterprise environments. Supporting up to 15,000 devices and 25 million rules in less than 10 seconds response time is simply what we do. This is achieved through a distributed architecture that separates the application, database, and data collectors on separate servers, allowing for seamless scalability as enterprise needs change.



A distributed architecture allows easy expansion of any FireMon element enabling the platform to scale to the needs of any organization.

Features At-a-Glance

	Security Manager Base	Change Management Add-on	Rule Recertification Add-on	Vulnerability Management Add-on
Centralized rule repository	X			
Multi-vendor rule normalization	X			
Rule usage summary	X			
Security Concern Index to measure risk over time	X			
Control failure summary	X			
Vulnerability assessments	X			
Change history and documentation	X			
SIQL search	X			
Preconfigured assessments	X			
Customizable reporting	X			
Preconfigured controls	X			
Customizable controls	X			
Access Path Analysis	X			
What-if attack scenario simulations				X
Vulnerability scanner integration, (Qualys and Rapid7)				X
Customizable rule creation/change workflows		X		
Intelligent rule design recommendations		X		
Pre-deployment compliance/risk assessments		X		
Automatic rule deployment to devices		X		
Customizable rule review workflows			X	
Event-driven review triggers			X	
ITSM integration; including ServiceNow	X	X	X	
SIEM integration	X			
SOAR integration	X	X		
Swagger-based API integrations	X	X	X	X

9X

Improvement with Security Manager

FireMon's Security Manager offers a robust and flexible solution to address enterprise network security challenges to help ensure organizations are protected against security risks. FireMon customers can expect a 90% reduction in time to create and deploy new firewall rules, 90% less time needed to manage rule changes and conduct compliance audits, and 90% faster time to block threats. Security Manager saves time, money, and more importantly protects enterprises from compliance violations, unplanned outages, and accidentally creating policy-related vulnerabilities.

FIREMON

FireMon is the only real-time security policy management solution built for multi-vendor hybrid enterprise environments. FireMon provides policy automation for the latest network security technologies helping organizations achieve continuous compliance while minimizing firewall policy-related risk. Only FireMon delivers complete visibility and control across an organization's entire IT landscape. [Firemon.com](https://www.firemon.com)

© 2023 FireMon, LLC.

All rights reserved. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

DS0027-EN-20230523-03