FIREMON

# Policy Manager

**Control and validate security policy to reduce risk, manage change, and maintain continuous compliance.**

Enterprise network security is incredibly powerful, but also incredibly complex. As organizations invest in firewalls, cloud platforms, and segmentation technologies, policy becomes harder to control across environments.

A typical enterprise operates with millions of rules, and a single misconfiguration can lead to compliance violations, outages, or breaches. The challenge is not the tools themselves, but ensuring the policy they enforce behaves as intended.

## Enforce and Maintain Compliance

### Avoid violations, avoid risk, and avoid fines

Ever-changing regulatory and internal security policy requirements make it difficult to maintain compliance across complex, multi-vendor firewall and hybrid cloud environments. As policy spans firewalls, cloud platforms, and segmentation systems, ensuring consistent enforcement becomes increasingly challenging. Manual processes introduce errors, slow audits, and increase the risk of fines and compliance failures. Over time, exceptions accumulate and policy drifts from original intent, leaving teams uncertain whether deployed controls actually meet regulatory requirements.

## Policy is Power. Control It End-to-End.

FireMon, the founder of Network Security Policy Management (NSPM), is the control plane for security policy across enterprise networks. It sits above firewalls, cloud platforms, and segmentation systems, continuously validating that policy operates as intended across the entire environment.

Trusted by Global 2000 organizations, FireMon turns policy into a controlled, measurable system. It detects drift, quantifies exposure, and ensures that security policy remains aligned as environments evolve.

- **Firewalls enforce**
- **Visibility tools observe**
- **FireMon governs**

FIREMON

FireMon continuously validates policy against compliance requirements, ensuring that security policy remains aligned and audit-ready at all times. It provides real-time violation detection so teams are alerted before non-compliant changes are deployed, while automated reporting generates audit-ready documentation in minutes. Policy recertification workflows enforce ownership and accountability, ensuring rules are regularly reviewed and aligned with business and regulatory intent. By embedding compliance into daily operations, FireMon eliminates manual audit preparation and ensures continuous alignment with internal and external standards.

## Manage Change

### Avoid misconfigurations, accelerate business, and improve security

Changing security policy is constant, and the consequences of getting it wrong can be severe. As environments scale, policy changes become more frequent, more complex, and more difficult to validate across firewalls, cloud platforms, and segmentation systems. A single misconfiguration can block legitimate access to mission-critical services or introduce unintended exposure. Without a clear understanding of how changes will impact the environment, teams rely on manual processes that slow operations and increase the likelihood of errors.

FireMon enables teams to validate every policy change before it is deployed. It simulates the impact of proposed changes and performs real-time risk and compliance assessments, ensuring updates align with security intent and do not introduce unnecessary access or violations. Automated workflows streamline rule creation and modification, while integrations with ITSM platforms support structured approvals and controlled execution. Once validated, changes can be deployed consistently across environments, allowing organizations to accelerate policy updates while maintaining control and reducing operational risk.

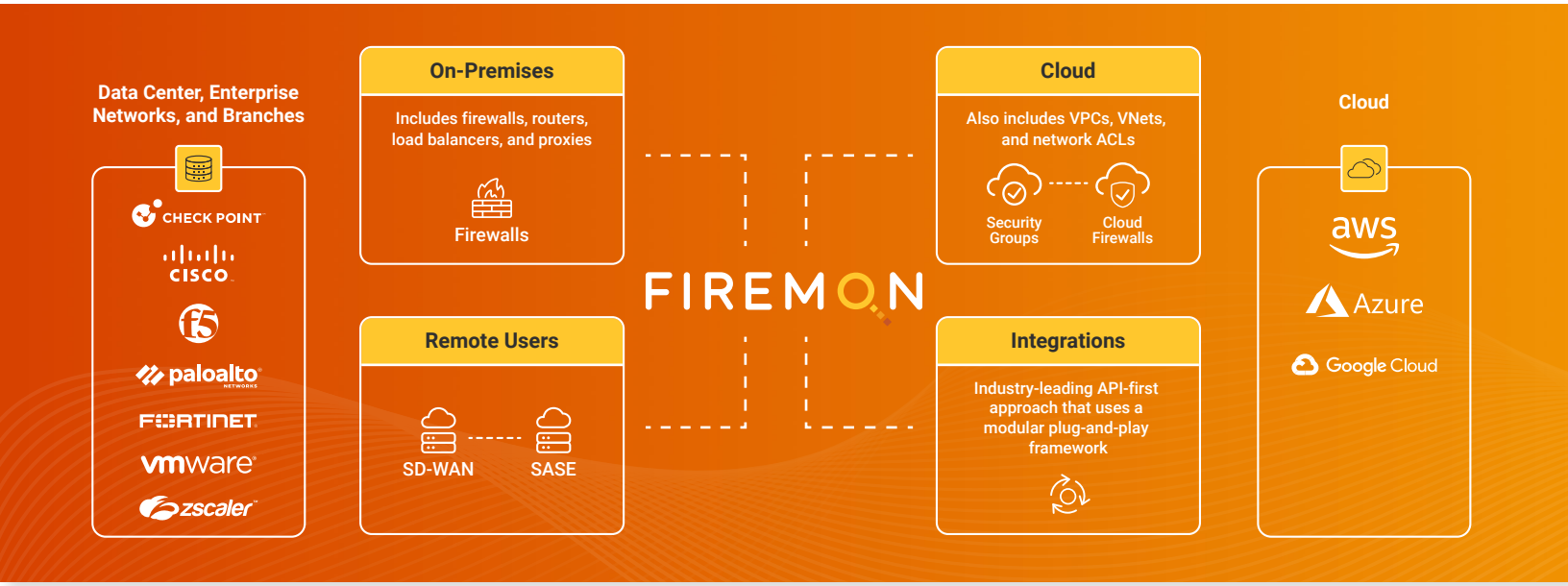
## Reduce Risk

### Manage risk with continuous validation and control

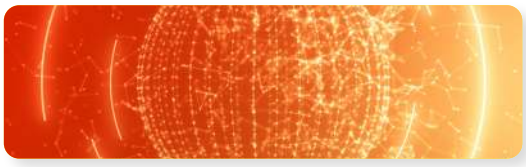
Organizations often struggle to understand how policy actually behaves across their environments. As complexity increases, risk becomes harder to identify, measure, and control across firewalls, cloud networks, and segmentation platforms. Misconfigurations, overly permissive rules, and policy drift create hidden exposure that can lead to outages or breaches. Without a centralized approach to evaluating policy, teams lack a clear view of how access is granted and where vulnerabilities exist.

FIREMON

FireMon continuously evaluates policy to identify misconfigurations, excessive permissions, and exposure paths across the entire environment. It applies real-time analysis, risk scoring, and threat modeling to quantify risk and prioritize the most critical issues. Predictive attack path simulation helps organizations understand how vulnerabilities could be exploited, while AI-powered insights provide clear remediation guidance. Guardrails enforce validation on every new rule and change, ensuring additional risk is not introduced. By continuously validating policy and measuring risk over time, FireMon enables a proactive, risk-aware approach to network security.




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



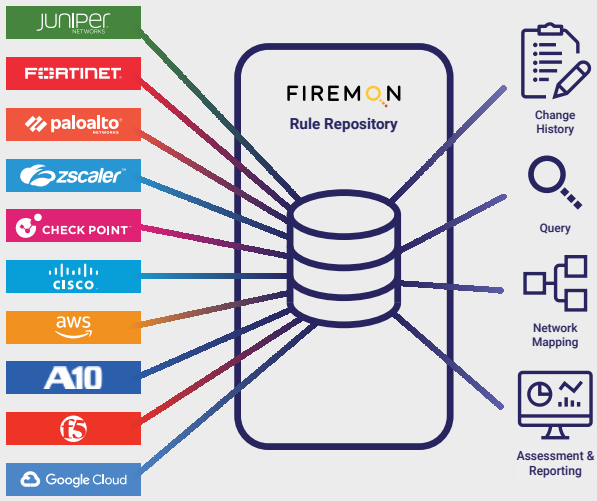
FIREMON

# Policy Manager Features

FireMon's Policy 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 offers comprehensive, real-time visibility across firewall policies, cloud security groups, and hybrid infrastructure. Supporting 120+ security platforms, it ensures organizations maintain full control over their security landscape. 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. By leveraging AI-powered analytics, FireMon allows users to benchmark security posture against industry peers, providing actionable intelligence to optimize firewall policies and strengthen overall risk management. 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.

FIREMON

## 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.

## Industry Benchmarking

Compare your organization's firewall policy KPIs with industry peers to identify areas of weakness and potential risk. By providing real-time benchmarks across all critical metrics, FireMon Insights helps you understand where you stand and where to focus your efforts.

## Trending Metrics

Track KPI progress over time to evaluate whether your management practices are driving improvement. Gain insights into key areas like reducing policy risks, cleaning up unused rules, and ensuring compliance.

## AI-Driven Insights

Powered by nearly fifty KPIs and enriched with benchmarking and trending data, FireMon Insights' AI engine identifies and prioritizes critical areas of concern. Each recommendation is backed by detailed analysis, helping teams address vulnerabilities and optimize policies with confidence.

## AI Chatbot

Simplify interactions with firewall data using natural language. FireMon Insights' chatbot enables users to troubleshoot issues, validate access policies, and gain insights instantly, reducing bottlenecks and improving productivity.

## 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.

FIREMON

## Architecture Built for Scale

FireMon's Policy 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.

FIREMON

## Features At-a-Glance

| | Security Manager Base | Policy Planner Add-on | Policy Optimizer Add-on | Risk Analyzer Add-on | FireMon Insights Add-on |
|---|---|---|---|---|---|
| Centralized rule repository | X | | | | |
| Multi-vendor rule normalization | X | | | | |
| Rule usage summary | X | | | | |
| Security Concern Index to measure risk | 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 | | | | |
| Security Posture Benchmarking | | | | | X |
| Executive Dashboards and KPIs | | | | | X |
| AI Chat Interface | | | | | X |
| What-if attack scenario simulations | | | | X | |
| Vulnerability scanner integration, including Qualys and Rapid7 | | | | X | |
| Customizable rule creation/change | | X | | | |
| Intelligent rule design recommendations | | X | | | |
| Pre-deployment compliance/risk | | 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 | |

## Policy Manager Delivers 10X Faster Results

FireMon's Policy 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. Policy Manager saves time, money, and more importantly protects enterprises from compliance violations, unplanned outages, and accidentally creating policy-related vulnerabilities.

FIREMON | Policy is **Power**

FireMon is the founder of Network Security Policy Management (NSPM) and the control plane for security policy across modern enterprise networks. FireMon provides an authoritative layer above enforcement technologies, continuously validating that deployed rules, segmentation, and access controls operate as designed across firewalls, cloud networks, and microsegmentation platforms.

The FireMon platform combines firewall policy management, a Zero Trust control plane, AI-powered policy control, and risk-aware policy change management to detect policy drift, quantify exposure, and drive prioritized corrective action. Global enterprises, government agencies, and service providers rely on FireMon to reduce measurable risk and maintain continuous compliance.

info@firemon.com firemon.com





DS0364-EN-20260512-04