Automate At Your Pace and Confidence Level with the Power of Continuous Adaptive Enforcement™

THE CHALLENGE

Many enterprises are embarking on digital transformation initiatives, while simultaneously dealing with a sophisticated and volatile threat environment. Their increased focus on incident response and hybrid cloud visibility, coupled with the growing impact of governance, risk, and compliance on security operations, is further compounded by the inability to hire and retain skilled security professionals, putting additional strain on lean security teams and increasing their security risk.

These challenges are magnified as the gap between the urgency to innovate and ensuring a secure network widens as security teams struggle to keep up using outdated, manual processes. With an increasing number of policy changes triggered by either an active security event or by business-driven initiatives like deploying new services or applications, the lack of security process automation can lead to misconfiguration errors, accidental exposure, or service disruptions. Enterprises need to be confident in their ability to reduce security risk and achieve business agility without sacrificing one for the other.

THE SOLUTION

Drive Innovation at the Speed of Business with FireMon Multi-Level Security Automation

FireMon Automation delivers a comprehensive blueprint of security policy automation capabilities that drive smart security process automation to effectively address your unique use case, infrastructure, or compliance requirements. Our multi-level approach to security automation drives efficiency, agility, and efficacy by aligning automated tasks to your specific requirements across your on-premise, hybrid, and multi-cloud environments; and gives you the flexibility to manage your automation journey at your pace and confidence level. The levels of FireMon Automation include:

**AUTOMATED DESIGN**

A basic level of automation with:
- Design recommendations
- Auto-generated compliance and risk scoring reports

**Time:** Weeks to Days

**AUTOMATED IMPLEMENTATION**

Adds:
- Automated rule implementation
- Automated rule verification
- Automated change documentation

**Time:** Days to Hours

Operator monitors and reacts to environment changes

**ZERO-TOUCH AUTOMATION**

Adds automated compliance evaluation and approvals of:
- Per-app Security Intent
- Golden Rules guardrails
- Hands-off automation while the operator remains in control of the policies
- Integration with external systems (SOAR, CI/CD)

**Time:** 5-15 Minutes

System monitors and reacts to environment changes

**CONTINUOUS ADAPTIVE ENFORCEMENT™**

Adds:
- Auto-detection of infrastructure, network and platform changes
- Transparent recalibration of global security policies - not stopping at policy deployment
- Automatic fixes of out-of-band rogue changes

FireMon’s Compute Engine with exclusive Continuous Adaptive Enforcement™ brings real A-Z Zero-Touch Security Automation

**Time:** Immediate
Zero-Touch Automation
At the Zero-Touch Automation level, the system is now able to monitor and react to environment changes. Policies can be automatically pushed and activated on all of your devices without logging into different consoles or connecting to individual devices. You can define global, as well as per-application, access rules with abstraction, and alleviate the burden of time-consuming routine changes with Golden Rules guardrails. You can also enhance your automation at this level by using FireMon’s REST API to integrate with third-party security orchestration, automation and response (SOAR) and continuous integration and continuous deployment (CI/CD) solutions.

Automated Implementation
Additional capabilities are included at the Automated Implementation level, where implementation rules are now automated for the various devices in your network. Rule verification and change documentation are also automated, while you and your security team are still responsible for monitoring and executing on any changes.

Automated Design
Automated Design offers a baseline structure to your security processes with a basic level of automation that includes design recommendations, as well as auto-generated compliance and risk scoring reports. At this level, you and your security team are monitoring for any environment changes and responding to them as needed.

Continuous Adaptive Enforcement™
With Continuous Adaptive Enforcement™, FireMon introduces the defining benchmark for security policy automation. At this level, FireMon Automation goes beyond just push deployments to deliver ongoing contextual awareness, policy recalibration, and continuous policy deployment based on specified compliance requirements, and as defined in templates and Golden Rules guardrails. Rogue, out-of-band changes are fixed automatically to prevent unauthorized access or a potential data breach.

Who Is Firemon?
FireMon is the #1 security automation solution for hybrid cloud enterprises. FireMon delivers persistent network security for multi-cloud environments through a powerful fusion of real-time asset visibility, compliance and automation. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world.

For more information on FireMon Automation, visit www.firemon.com/automation

©2019 FireMon, LLC. All rights reserved. 11.19.2019