DATA SHEET

POLICY OPTIMIZER

Automate Rule Review Workflows

As networks grow in size and complexity, policy maintenance and compliance becomes increasingly difficult. Manual review processes don't scale to enterprise networks, leaving expired, unused, and overly-permissive rules to expand the threat surface.

HIGHLIGHTS

- Automatic rule recertification
- Event-based triggers for rule reviews
- Keep, deactivate, or decommission rules
- Comprehensive audit trails
- Dashboards manage and prioritize workflows

Policy Optimizer:Automate Rule Review Workflows

By automating rule workflow management, the Policy Optimizer module for Security Manager ensures that existing firewall rules are reviewed then recertified or decertified in accordance with compliance, business, or security policies. Using event-based triggers or search query results generated within Security Manager, Policy Optimizer automatically creates and sends tickets to policy owners to take action.The result is an automated rule review workflow that minimizes attack surfaces, helps maintain continuous compliance, and simplifies the audit process for a range of standards, including PCI DSS 3.2.1 requirement 1.1.7.

Feature	Benefit
Automated Ticket Creation and Routing	Rule reviews are automatically triggered and assigned based on a range of criteria, including policy violations, control failures, dormancy, and expiration dates
Centralized Audit Tracking	Speed compliance audits using an automatically-generated, accurate register of all changes made to rules over time
Consolidated Administration and Reporting	Single, easy-to-understand dashboard of all workflows, color-coded by severity to prioritize mitigation
Rule Treatment Options	Certify or decertify rules quickly and seamlessly, with automatic rule decommissioning when used with Policy Planner

THE ONLY AGILE NETWORK SECURITY POLICY PLATFORM

FIREMON

Automate workflows to review and recertify security policies

Manual processes for reviewing and routing rules are inefficient and resource-intensive, making it nearly impossible to recertify rules complex enterprise environments. Policy Optimizer **automatically creates and routes tickets** based on a range of events including policy violations, control failures, policy expiration dates, rule dormancy, scheduled reviews, and more.

Rule search query results within Security Manager can be sent directly to Policy Optimizer to create new workflows. Tickets are automatically assigned to the rule owners by email, with any relevant attachments included for review. These workflows are highly customizable and can be adapted to meet a range of business and regulatory requirements.

> *"With FireMon we are able to continually audit our firewalls and flag any issues that would cause a problem with a security audit."*
>
> **Howard Wall**
> Senior Security Engineer,
> Alkami Technology
> Financial Services

Rule Treatment Options

Timely reviews of policies are only half the battle: establishing workflows to follow through on modifying or decommissioning rules is key to maintaining a strong security posture.

Policy Optimizer's automated ticketing makes it easy to designate which rules have been recertified to be kept active and which have been decertified for modification or decommissioning. Additionally, rule decommissioning is completely automated when paired with the Policy Planner module for Security Manager.

Centralized Audit Tracking

Audits are nerve-wracking and resource-intensive at the best of times, and they only get harder when there isn't an audit trail, or when that trail is made up of manually entered and inconsistent records.

Tamper-proof audit trails are created automatically, capturing pertinent details of all actions performed on a rule over time. Review stage, reviewer, start/end dates, completion, the duration of each ticket and more is all clearly displayed within Policy Optimizer tickets for easy access and review.

Full Visibility and Reporting

A lack of visibility is a lack of security, and the inability to assess the state of policy review at a glance allows for high-risk vulnerabilities to lurk in the backlog. Rule maintenance **administration and reporting is streamlined** with Policy Optimizer. The easy-to-understand dashboard shows all workflows in process and color-codes them for severity to simplify mitigation prioritization. When a specific ticket or policy needs to be found, FireMon's SIQL search tools allow for easy location of any Policy Optimizer ticket. Every aspect of the policy change workflow is easily documented with sub-second reporting for every policy and rule, with reports that can be customized to meet business and compliance requirements.

DS0053-EN-20211007-1