

# F I R E M N

**Website:** [www.firemon.com](http://www.firemon.com)

**Price:** Avg. of \$5,625/year for base product suite

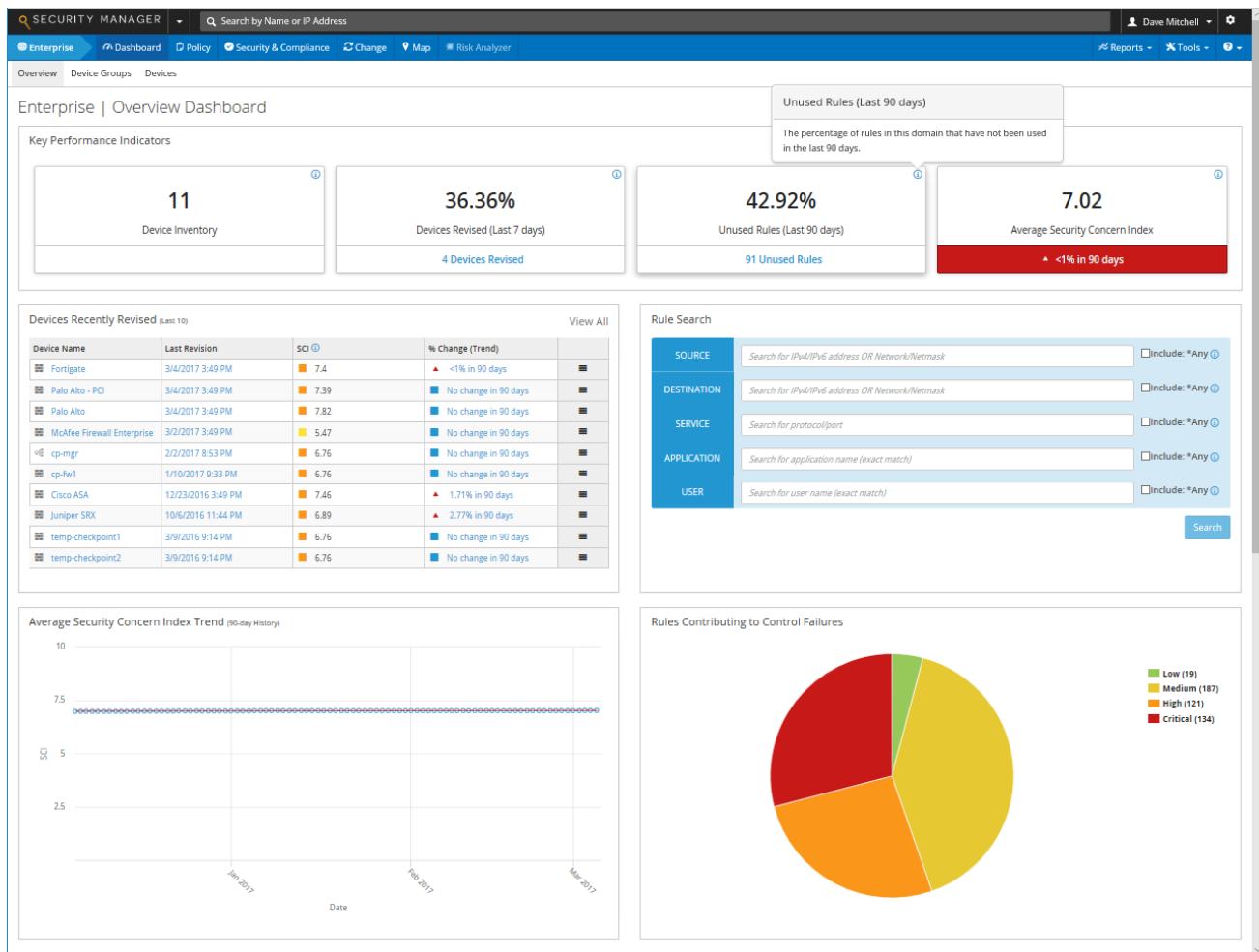


**Verdict:** Worried about GDPR compliance? Don't be as FireMon's Intelligent Security Management (ISM) Platform keeps you ahead of the game with sophisticated firewall monitoring, risk analysis and automated change management

IT security professionals already faced with a mountain of data protection regulations will find their jobs are about to get a lot tougher. The EU GDPR (general data protection regulations) come into force in May 2018 and that means businesses of all sizes must protect against security breaches involving personal data or be hit hard with punitive fines.

Firewalls are the first line of defense and it's now imperative that administrators start working on compliance with clear and effective configuration and change management policies. This will be challenging in geographically distributed, multi-vendor environments and FireMon's Intelligent Security Management Platform lightens the load by providing a suite of tools for firewall and network device visibility, compliance audits, risk analysis and change management.

The complete suite is seamlessly integrated into a web-based management console that provides a single pane of glass view of your entire security infrastructure. ISM runs on FMOS (FireMon Operating System) - a hardened Linux OS based on CentOS which provides a highly scalable, distributed architecture capable of delivering real-time security intelligence and event analytics across thousands of firewalls.



The Security Manager dashboard keeps you in the loop on all your security vulnerabilities

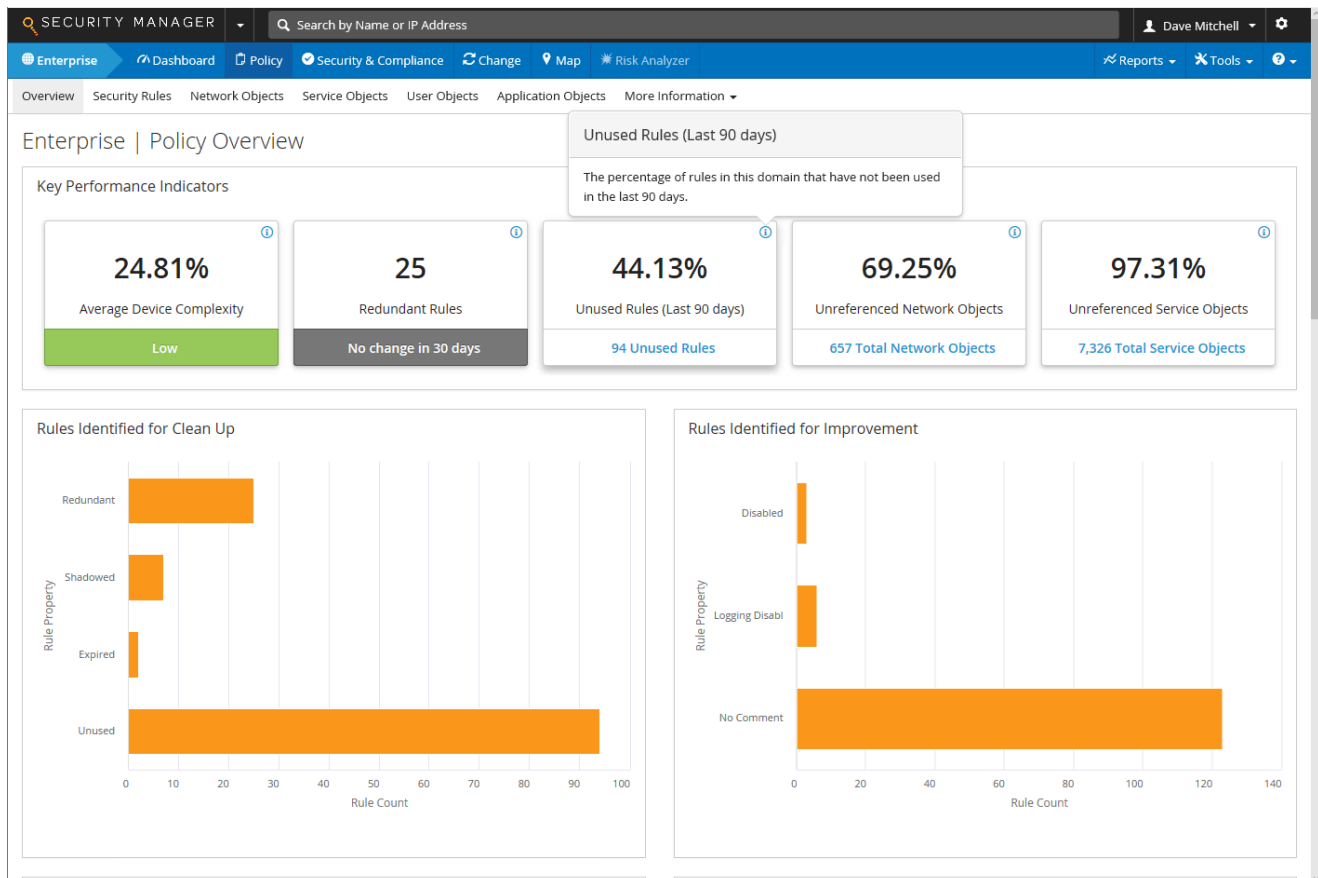
## FireMon Intelligent Security Management

The ISM suite comprises five products and in this review we look at FireMon's three star players - Security Manager, Policy Planner, and Policy Optimizer. Security Manager is the driving force behind ISM and provides continuous firewall configuration analysis, rule assessment, real-time change detection and policy compliance auditing.

We were impressed with the Security Manager console as it delivers a wealth of information in an easily digestible format. The main dashboard provides widget-based views with graphs and tables clearly showing main areas of interest including unused rules, those contributing to assessment failures, the most active firewalls and traffic flow analysis.

Tabs provide quick access to in-depth views of policies, security and compliance or change analysis and a smart feature is FireMon's Key Performance Indicators (KPIs). Located at the top of each screen, KPIs offer at-a-glance performance measurements that deliver critical security information avoiding the need to drill down.

The dashboard view provides four KPIs for firewall inventory, device revisions in the last seven days, the percentage of unused rules and an average Security Concern Index (SCI) - a ranking of firewall policy severity. The last two KPIs are unique to FireMon as Security Manager provides a global number across multiple firewalls whereas competing products can only do this on a per-device basis.



The Policy view highlights all rules that need attention and provides sage advice on tightening them up

## Policies, Compliance and Change

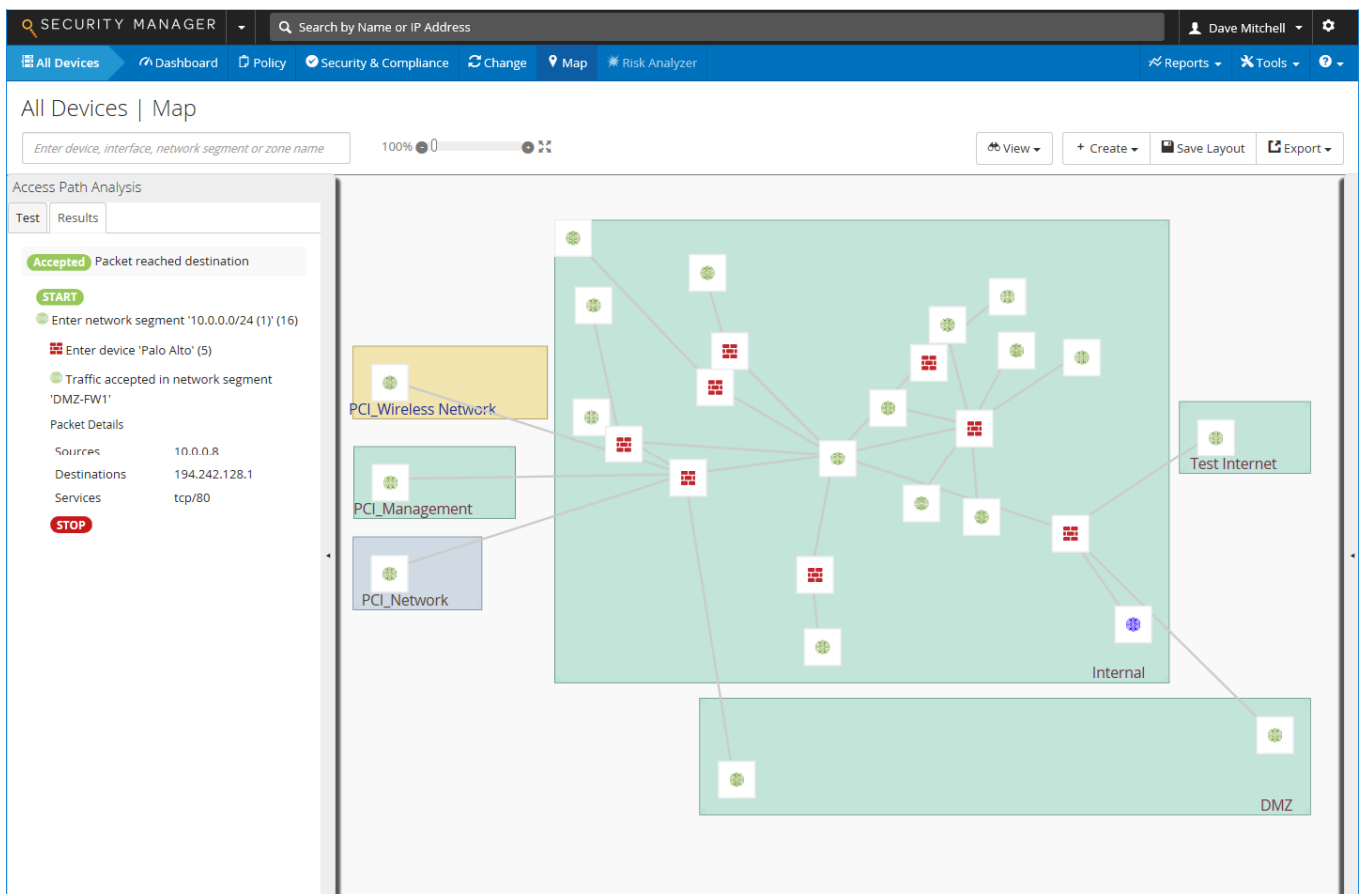
Security Manager is capable of presenting a remarkable amount of information as its Policy view provides five KPIs and identifies unused, redundant, shadowed, expired and failed rules. It showed us precisely which rules needed improving or cleaning up and we could drill down deeper and see those devices they applied to.

The Security Rules page showed us all rules that had tripped an alert with them sorted neatly into groups for cleanup or improvement operations, those that had failed and any changed in the past seven days. Each rule is listed in the standard firewall format where we could see sources, destinations, services, actions, hit counts, severity grades and who made the last revision.

FireMon includes four preconfigured assessment modules for Best Practices, DISA STIG, NIST and PCI-DSS plus you can create your own using the administration console's Assessment Builder tool. They all use sets of Controls which define eleven different type of criteria for functions such as device interrogation, allowed rules, searches using FireMon's SIQL (Security Intelligence Query Language) and rule usage checks.

Libraries of pre-defined controls are provided and they start analyzing all monitored devices the moment Security Manager is activated. We viewed the results from the Security and Compliance tab which opens an overview with more KPIs and detailed reports for assessment and control results.

Along with the Device Map which shows how devices relate to each other, we particularly like the Access Path Analysis feature which performs tests to see how firewalls react to traffic. This can be used to test whether a user can reach an application and if not, see precisely which device has blocked its traffic and why.



The Device Map can be used to analyse paths to see if data is getting through to end users

## **FireMon Policy Planner and Optimizer**

Available as separately licensed options, the Policy Planner and Policy Optimizer modules snap neatly into the main console. Policy Planner provides workflow and change management processes allowing security managers to track security policies and plan, authorize and audit changes.

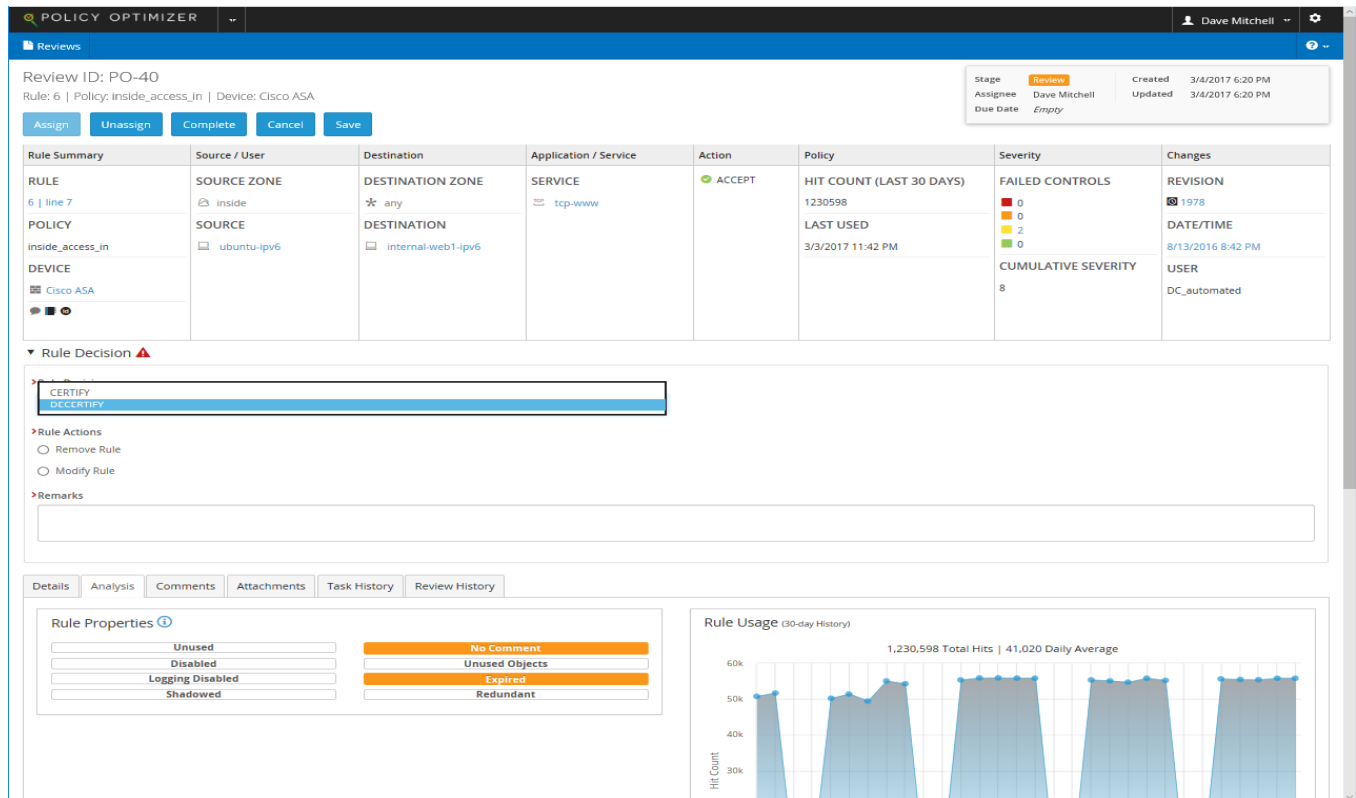
Workflow packs are used to create tickets for access requests, creating, modifying or removing connections and rule reviews. These can be modified or added to in the Administration console where Active Directory, LDAP, RADIUS and SAML authentication servers are also defined and users assigned specific console access rights.

Ticket creation is fairly straightforward as its workflow controls the entire process from initial request through design, user assignment, review, verification and on to implementation. Policy Planner analyses tickets, makes recommendations for rule changes and its risk assessments highlight issues such as rules that would expose vulnerabilities in the target firewall.

Businesses managing hundreds of thousands of rules will find Policy Optimizer a boon as it removes the need for inefficient and time-consuming manual review processes. It's designed to identify stale, overly complex and risky rules and can be used as part of a compliance drive by ensuring certain rules are regularly reviewed.

We found this the least intuitive part of the ISN suite as it requires new controls and assessments to be created from the administrator console which are then used to route control failures through to the Policy Optimizer console. We could also view rules flagged in the Security Manager Policies page and route them directly to the Policy Optimizer with one click.

Workflow tickets are assigned to selected users for review and analysis where they can decide to decertify a rule and either remove or modify it or choose to certify it and set a new review date. Overall, we recommend this module as it takes the daily drudgery out of security policy reviews, will make compliance a lot easier and can be linked in with a number of third-party change management systems.



**POLICY OPTIMIZER**

Reviews

Review ID: PO-40  
Rule: 6 | Policy: inside\_access\_in | Device: Cisco ASA

Stage: Review  
Assignee: Dave Mitchell  
Due Date: Empty

Created: 3/4/2017 6:20 PM  
Updated: 3/4/2017 6:20 PM

Rule Summary	Source / User	Destination	Application / Service	Action	Policy	Severity	Changes
<b>RULE</b> 6   line 7	<b>SOURCE ZONE</b> inside	<b>DESTINATION ZONE</b> any	<b>SERVICE</b> tcp-www	ACCEPT	<b>HIT COUNT (LAST 30 DAYS)</b> 1230598	<b>FAILED CONTROLS</b> 0	<b>REVISION</b> 1978
<b>POLICY</b> inside_access_in	<b>SOURCE</b> ubuntu-ipv6	<b>DESTINATION</b> internal-web1-ipv6			<b>LAST USED</b> 3/3/2017 11:42 PM	<b>CUMULATIVE SEVERITY</b> 8	<b>DATE/TIME</b> 8/13/2016 8:42 PM
<b>DEVICE</b> Cisco ASA							<b>USER</b> DC_automated

**Rule Decision**

CERTIFY  
DECERTIFY

**Rule Actions**

☐ Remove Rule  
☐ Modify Rule

**Remarks**

Details | Analysis | Comments | Attachments | Task History | Review History

**Rule Properties**

Unused  
Disabled  
Logging Disabled  
Shadowed

No Comment  
Unused Objects  
Expired  
Redundant

**Rule Usage (30-day History)**

1,230,598 Total Hits | 41,020 Daily Average

Hit Count

The Policy Optimizer module does away with tedious manual review processes by automating it

## Conclusion

With fines for data breaches about to get very serious, enterprises can't afford to have their IT security staff engaging in daily firefights as they struggle to maintain compliance. FireMon's Intelligent Security Management Platform is an ideal solution as it delivers a rapid response team for automating security policy configuration in line with laid down compliance practises.

FireMon takes the pain out of compliance by delivering joined up firewall auditing and change management while tight integration across the suite members ensures security isn't compromised at any stage. It's capable of providing a wealth of information about your security infrastructure, its modular design means you only purchase what you need and it's compatible with all major firewall vendors.

**Reviewed by: Dave Mitchell, Binary Testing, for the IT Security Guru**