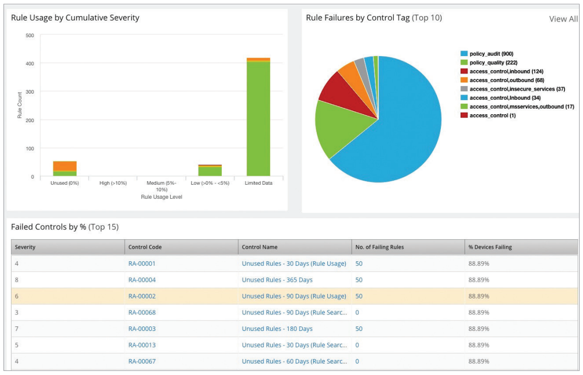
Rule Usage by Cumulative Severity
500
400
300
200
100
0
Rule Count
Unused (0%)
High (>10%)
Medium (5%-10%)
Low (>0% - <5%)
Limited Data
Rule Usage Level
Rule Failures by Control Tag (Top 10)
View All
🟦 policy_audit (900)
🟩 policy_quality (222)
🟥 access_control,inbound (124)
🟧 access_control,outbound (68)
⬜ access_control,insecure_services (37)
🟦 access_control,Inbound (34)
🟩 access_control,msservices,outbound (17)
🟥 access_control (1)

Failed Controls by % (Top 15)

Severity	Control Code	Control Name	No. of Failing Rules	% Devices Failing
4	RA-00001	Unused Rules - 30 Days (Rule Usage)	50	88.89%
8	RA-00004	Unused Rules - 365 Days	50	88.89%
6	RA-00002	Unused Rules - 90 Days (Rule Usage)	50	88.89%
3	RA-00068	Unused Rules - 90 Days (Rule Searc...	0	88.89%
7	RA-00003	Unused Rules - 180 Days	50	88.89%
5	RA-00013	Unused Rules - 30 Days (Rule Searc...	0	88.89%
4	RA-00067	Unused Rules - 60 Days (Rule Searc...	0	88.89%

FireMon

Security Intelligence Platform

As its name suggests, FireMon Security Intelligence Platform is focused on monitoring and managing firewalls. That puts it squarely on the technology-driven side of GRC. It runs on a purpose-built platform and it mixes GRC and enterprise security, an excellent mix in our view. The architecture is such that it can be distributed easily and can be deployed from one or multiple platforms.

The premise behind the tool is that by managing communications devices and predominantly firewalls, security and good GRC can be maintained. Sprinkle in some really good reporting and searching and you've got a pretty good mix. We really liked the contextual approach that FireMon takes. It watches the flows in the network and, using vulnerabilities reported from scanners, such as Qualys and such things as vulnerability reachability, it figures the relative risk for any device under any set of conditions. This gets played against policies and standards to get a contextual picture of the IT risks in the enterprise.

The agents that sit on the monitored devices are very lightweight and FireMon supports more than forty different devices. We dropped into the system through the security manager dashboard. This is a bare-bones dashboard with just the picture that the administrator or analyst needs to get started. There is a series of key performance indicators and several good starting points for analysis, such as a look at the top 10 devices recently revised – they monitor for change in real-time. From here you can drill down and get to anywhere you need to be within the tool.

One unique capability that we particularly liked is the traffic flow analysis report. This lets us see how traffic is flowing on the network. Configurations dictate data flows, so watching data flows provides an indicator of network security health. Playing all of this against FireMon's reporting and analysis tools gets you to a good view of risk and compliance. This is enabled by the database architecture of the system. The database uses FireMon's SiQL. Searching is via omni search and it is very simple and Boolean-based.

Firewalls can have hundreds of thousands of rules and many of those rules are not often needed. So what do you do if you have a hundred firewalls throughout your widely distributed enterprise? How do you keep all of them running at top efficiency without doing something that breaks security? FireMon addresses that with its Removable Rules report. This tells what rules on what devices can or should be removed

Pricing on the system is reasonable and there is a good customer portal. Support is free for the first 30 days and can purchased in two levels.

DETAILS

Vendor FireMon

Price One-time startup cost of $10,000 plus cost per device.

Contact info@firemon.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths One of the best examples of a technology-driven GRC program we've seen. It has all the functionality needed to combine solid security management with GRC.

Weaknesses None that we found.

Verdict With a large number of devices, this can get a little pricey, but it still is a good value considering everything it does.

Reprinted from the November 2015 issue of SC Magazine • www.scmagazine.com