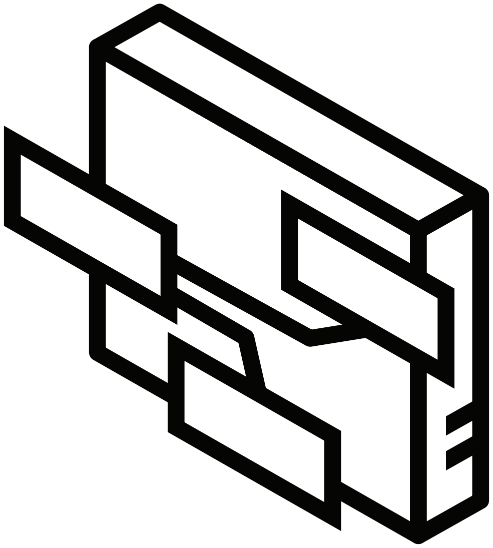
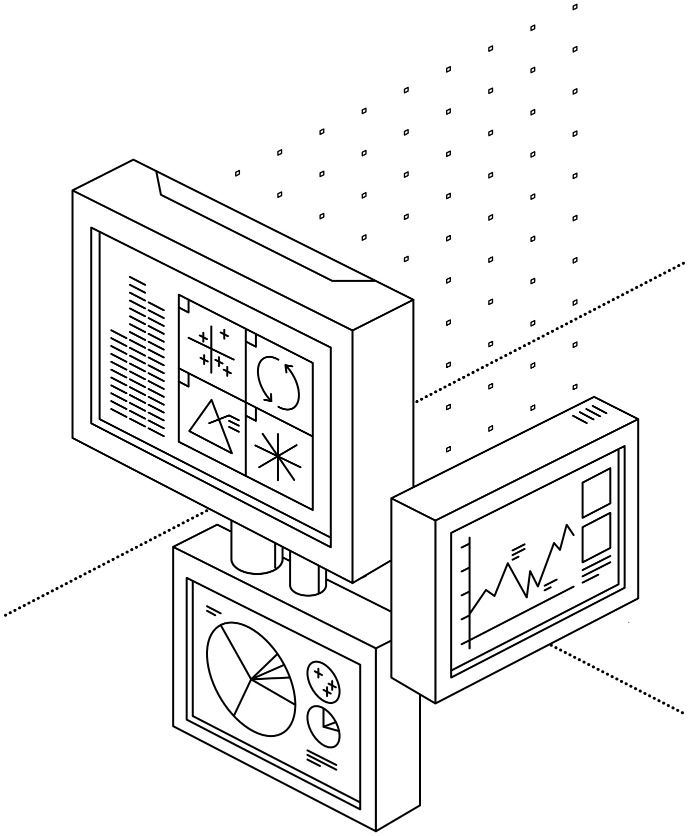


THE TOP 5 REQUIREMENTS TO LOOK FOR IN YOUR NETWORK SECURITY POLICY MANAGEMENT SOLUTION

FIREMON

INTELLIGENT SECURITY MANAGEMENT



EXECUTIVE SUMMARY

Network Security Policy Management (NSPM) continues to be a difficult practice for organizations the world over. In the last 20 years, network security policies (e.g. firewall rules) have grown by more than 3,500%. Yes, you read that number correctly. Why is that?

If you expand a network's functions and capabilities, you will invariably see complexity in network security policies. With changing tides in network security, it still remains that policy governs what can happen within the environment.

Consider this a call to arms. Network security teams are swamped with overly complex, often outdated and vulnerable network policies. These brave souls serve as the garrisons to our most valuable information resources. And our intrepid heroes need solutions that take aim at this complex and changing world.

Let's take a look at the requirements for a world-class NSPM solution.

COMPREHENSIVE SUPPORT & COVERAGE

Any solution that will help security teams manage amoeba-like policies starts with connecting and extracting data from a wide-range of network security devices. Most of the security device manufacturers have a large enough footprint for any solution to have native integrations to these devices, including: Check Point, Palo Alto Networks, F5, Cisco, Juniper, Fortinet, Barracuda, among others.

But having native integration is only the first ingredient. Our heroes need an NSPM solution with an open API to quickly evolve as new devices and configurations change. Traditionally, security teams have been "Dr. No," but with increasing pressure from continuous delivery and agile models, security teams need to operate at the speed of the business. Any NSPM must have forward flexibility. We do not know which devices or assets we will have tomorrow, but we can presume they will vary from what we have today.

An open API can adapt to whatever the business needs. This is a non-negotiable for our heroes looking for an NSPM solution.

FireMon's solution offering delivers on all key components of an NSPM solution as identified by Gartner.*

- Security Policy Management
- Change Management System
- Risk & Vulnerability Analysis
- Application Connectivity Management

* *Network Security Policy Management Solutions Have Evolved, Analysts: Adam Hils & Rajpreet Kaur, Published: 30 October 2015*

PERFORMANCE AT SCALE

How many buzzwords can we fit into one paper? All joking aside, what does it really mean to have performance that scales?

Scale is ultimately a relational model: many-to-one. Now comes the performance piece. Any NSPM solution should function just as well with 1,000 firewalls as it does with 10. Essentially, we are talking about data ingestion and normalization, but having the ability to ingest millions of events from a network of security devices can be a challenge – for some.

The many-to-one scalable requirement is for purposing all that rich data. Any NSPM solution must have the option to use global search and reporting from a single console. Far too many solutions require separate appliances dedicated to sections of the network or data centers. This means, our heroes run reports at each terminal, which limits the enterprise-wide reporting they need. How are you going to make a decision about policies if you can't see them all?

Worst of all, NSPMs that do not perform at scale because of limited reporting from archaic models for data management, devoid of open-ended search.

Imagine you are a security engineer looking for answers to how many unused rules you have. Fairly simple, no? Well, systems that do not perform at scale would require logging into 5-10 separate terminals, running a standard report (almost always missing key data) and then 'stitching' together the details into a single, offline report – usually Excel.

What happened while you were fiddling with Excel? Well, as you were going from console-to-console and doing your best to quilt the data together, additional rules changed or search results have updated – but they are not in your spiffy stitched together report. You were busy piecing together different reports while things in the network were changing.

Without a truly scalable architecture, we will only see marginal improvements to Network Security Policy Management. To be sure, the separate console model is far better than running reports one firewall at a time, but if you follow the logic...doesn't eliminating all the manual stitching get you where you want to be?

Test your potential NSPM vendors, talk to peers, get demonstrated proof of the solution's scalability. Also, don't fall for the trap of confusing heterogeneous support or ingest rates with scale. Performance at scale is all about operations that can be done in one place across multiple systems. To conclude this section with another buzzword, does your NSPM have a true 'single-pane-of-glass'?

FIREMON: PERFORMANCE AT SCALE

Maintain a single installation to enable enterprise-wide search

Elasticsearch for sub-second, ad-hoc querying and reporting across organizational and geographic boundaries

Distributed architecture allows the system to scale widely while minimizing network load

Enterprise-class solution that keeps pace with business growth

Full data retention, no limits

COMPREHENSIVE AUTOMATION

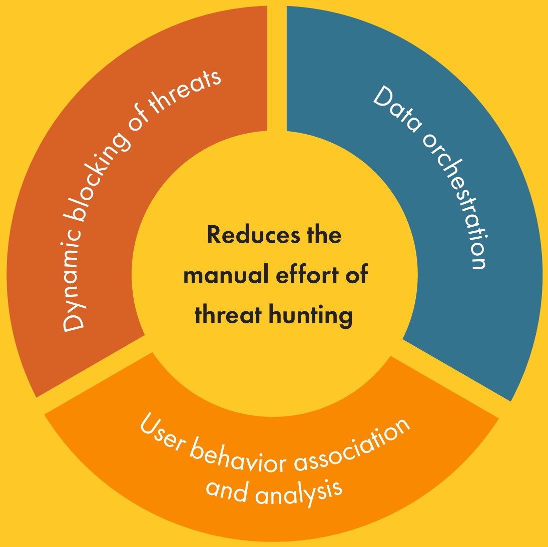
Since world-class security personnel are growing on trees, this isn't really all that important... gotcha! There is a 10% negative unemployment rate in security. That means, for every 10 job openings, there are only 9 people with the requisite skills to fill them. What the world needs now is automation, sweet automation.

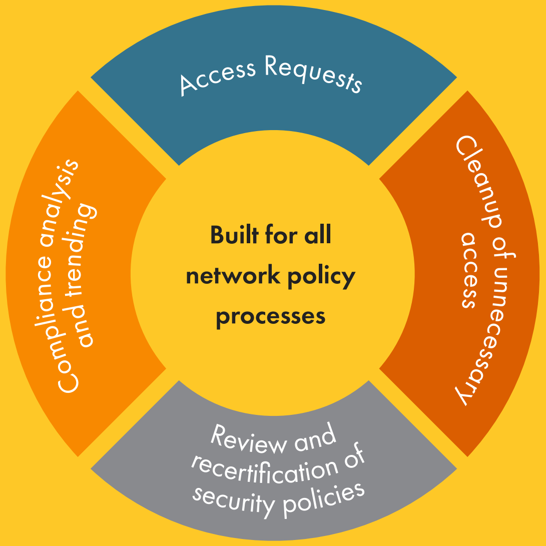
But what do you automate? Many vendors make claims for all kinds of automated functions. But if tossing automation at the NSPM challenge was the silver bullet, why the continuing complexity gap? Because making the claim to automate a single function is not equivalent with comprehensive automation – from rule recommendation to design to implementation. Any NSPM vendor must maximize agility for managing network security policy with Comprehensive Automation. There are four (4) principle areas for NSPM, each of which lends itself to automation.

1. Access Requests
2. Access Cleanup
3. Policy Review & Recertification
4. Compliance Analysis & Attestation

With the skills shortage we mentioned earlier, automating these pillars of NSPM saves valuable time and resources. We hear our customers say it every day. FireMon has automated what matters: "In just a few minutes, we can generate an audit or compliance report that takes months for a professional services engagement to duplicate," said Daniel James of Southwest Airlines.

In the wake of the skills shortage, organizations are spending truck-loads on professional services, but we can use automation instead; saving time and money on our way to improved security.


Dynamic blocking of threats
Data orchestration
Reduces the manual effort of threat hunting
User behavior association and analysis


Access Requests
Cleanup of unnecessary access
Built for all network policy processes
Review and recertification of security policies
Compliance analysis and trending

CUSTOMIZABLE WORKFLOW

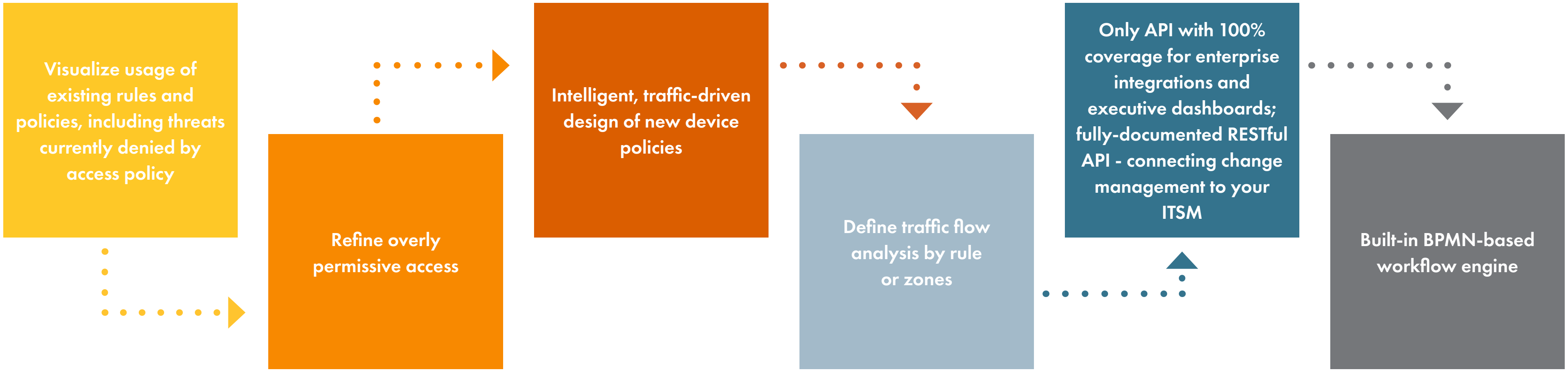
The idea behind workflow in the context of NSPM is a natural extension from the change management process. Any solution should have a complete and integrated workflow application, and optimally, ties into the ITSM (e.g. ServiceNow, BMC Remedy). The power of a customizable workflow tool is clear: Manage the change process to ensure only the correct rules are designed and implemented. Firewalls are unique from hosts and the inputs for a firewall change are unique as well. This is often the driver to implement a policy-centric workflow application.

Unfortunately, many organization stop here. But any workflow functionality for policy management should provide more value than just fields to travel through the workflow. Any true customized workflow will know about the environment, outside regulation, and the interconnectedness of the network – that's how you unlock the real value.

By bringing it all together, we get a framework for rule recommendation. Rule recommendation prevents security policy mistakes by identifying if a change is even necessary, what change should be made, and just as critical, where in the policy the change should be made. This not only prevents mistakes, but reduces security risk and time to modify policy.

There you have it, the Holy Grail: Customized workflow and automation with intelligent policy recommendations. Take that skills shortage!

FireMon's Automated, Intelligent Workflow



Visualize usage of existing rules and policies, including threats currently denied by access policy

Refine overly permissive access

Intelligent, traffic-driven design of new device policies

Define traffic flow analysis by rule or zones

Only API with 100% coverage for enterprise integrations and executive dashboards; fully-documented RESTful API - connecting change management to your ITSM

Built-in BPMN-based workflow engine

RISK ANALYSIS & ASSESSMENT

Now that we have cleaned up rules and automated our discovery for improving our policies, we can move to looking at how NSPM can help with risk mitigation.

Quantifying and assessing risks has become a critical part of security policy. Primarily, because with an adequate view of risks, our heroes can make informed decisions around policies that will improve their security posture.

Any NSPM solution should have an enterprise-wide architecture to handle large, complex networks. Using vulnerability scans paired with network security policies, your NSPM solution can automate attack paths, run simulations and probe for weaknesses within the context of your policies. Furthermore, using quantitative metrics, you can rank risks based on real-world scenarios. We no longer have to use the time-honored tradition of best guesses, but can optimize the network's security policies with evidence.

Risk analysis has become table stakes for NSPM. Any solution without risk analysis can be confined to the dust bin of good tries.

FIREMON RISK ANALYZER

- View risk posture in real time
- Simulate how attackers might gain access to assets through network vulnerabilities
- Assess the impact of a potential attack
- Determine where multiple exploits can be used in combination to reach an asset
- Adapt device rules to reroute access to address the risk immediately
- Prioritize patching based on impact

COMPLIANCE

As you have probably recognized by now automation, enterprise-wide visibility, scale and risk analysis all serve to keep our networks secure and compliant. Network Security Policy Management came out of the demand for quickly assessing rules and compliance attestation in a messy world.

When evaluating NSPM solutions for compliance, it would be short-sighted to stop with reports. Instead, security teams should look for ways to actually improve the compliance posture. That begins with stringent documentation.

Nearly all compliance regulations require justifying access permitted through the firewall. Whether you are considering PCI DSS, NERC, NIST or your own internal standards, compliance requires documentation for why a firewall is configured in a given way.

Implementing change management is a great step, but only part of the answer. Any NSPM solution should extend beyond simply informing you of the current compliance position and make recommendations to regain compliance.

There is an agile compliance mandate that is only achievable from a solution that distills all aspects we've mentioned:

1. Comprehensive Support & Coverage – You can't confirm compliance if you can't see data from unsupported devices.
2. Performance at Scale – If it takes days to stitch together a report, you can't have confidence that your compliant in real-time.
3. Automation – If compliance audits are a manual effort, by the time the audit is done, another compliance standard has failed.
4. Customizable Workflow – Everyone has their own standards and methods to achieve compliance, workflows must be flexible.
5. Risk Analysis & Assessment – Without quantifiable risks, it becomes difficult to determine where to begin.

FIREMON'S CUSTOMIZABLE COMPLIANCE REPORTING

- ✓ Validate policies against regulatory standards
- ✓ Verify real network traffic conforms to policy
- ✓ Easily report compliance for audit and attestation

CONCLUSION

We need a hero. Each day we work with network and security teams who are asked to do Herculean feats to keep their networks safe, while keeping pace with business requirements in an on-demand world. These heroes need a helping hand to deliver the protection and security needed for our evolving world. It starts with policy.

Several options are out there, and plenty of claims have been made. But as the market leader, we serve our customers by providing solutions that truly address their greatest challenges. They are true heroes of the enterprise. They slay the dragons, we provide the sword.

ABOUT FIREMON

FireMon is the No.1 provider of Intelligent Security Management solutions worldwide, combining advanced benchmarking, simulation and analysis to deliver next generation security intelligence. Since creating the first-ever network security management solution 15 years ago, FireMon solutions have continued to deliver visibility into and control over complex network security infrastructure, policies and risk to over 1,500 customers around the world.

Using the FireMon Intelligent Security Management platform, today's leading enterprise organizations, government agencies and managed security providers have the automation and intelligence required their network security teams require to streamline security operations, reduce the attack surface and respond to threats faster.

Learn more about our solutions: www.firemon.com

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA

REV 110917RGB