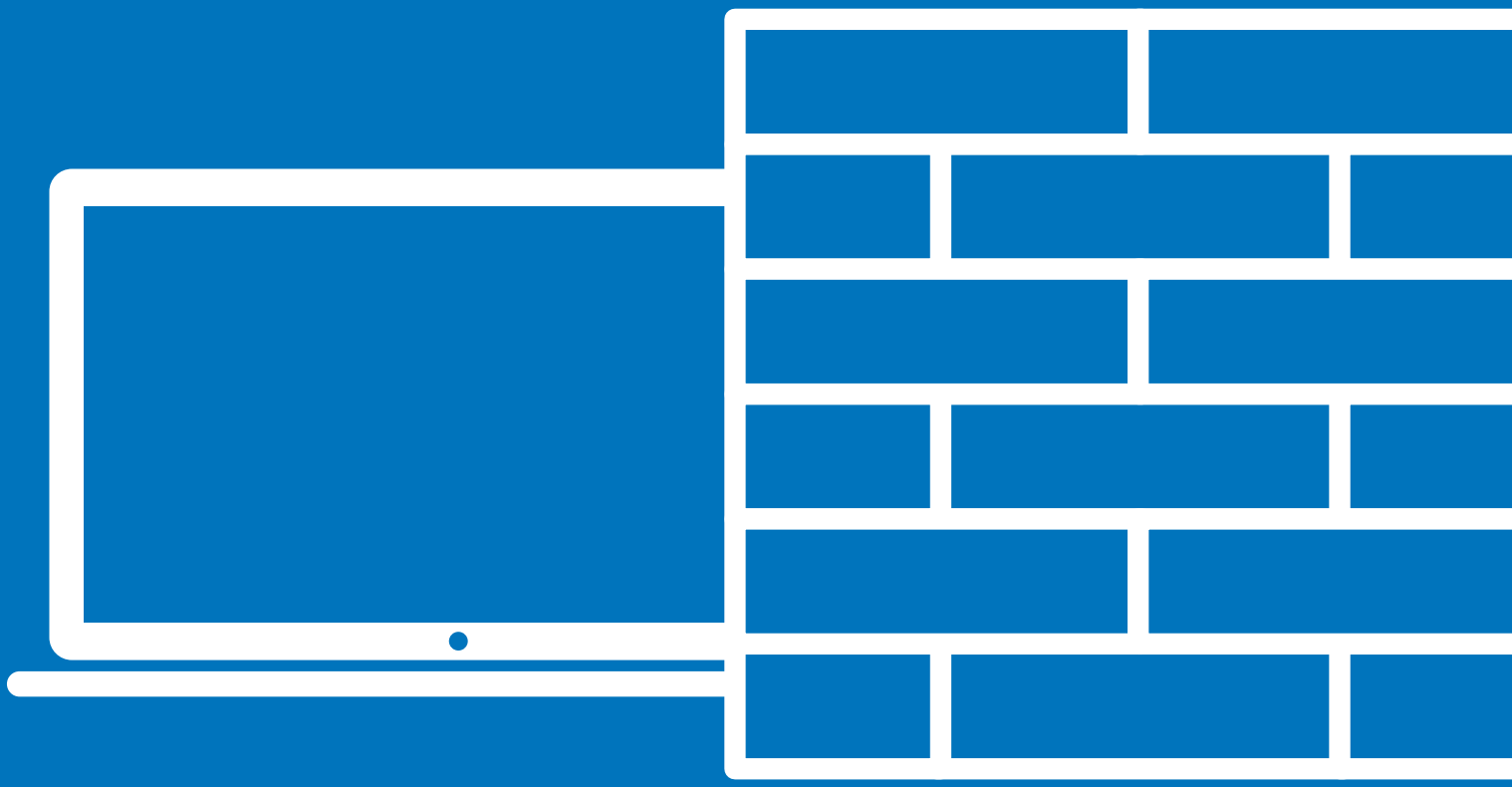
PeerPaper Report

Business Factors Driving Selection of Network Security Policy Management (NSPM) Solutions

Network security professionals weigh in

2020



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Network Security Policy Management (NSPM) solution selection factors need to align with business needs. Security shouldn't be a barrier to the business, but frequently, security needs are shortchanged to ensure business agility. Ideally, this tradeoff should not exist. Network and security managers thus look for NSPM solutions that can make the business run better by efficiently automating network security policy management, improving visibility in network traffic and rules, and facilitating compliance. This paper offers insights and feedback from real users, who discuss what went into their NSPM selection process.

CONTENTS

INTRODUCTION

What constitutes a good Network Security Policy Management (NSPM) solution? Selection criteria relate to Information Technology (IT) and security, but both tie into the business. The technical qualities of an NSPM solution should support existing business processes and help the business move forward. Security should not get in the way of business agility. Indeed, business and IT stakeholders are increasingly recognizing that security risks have a clear financial impact on your business – from reputational damage, lost business, and lower corporate valuations. Breaches are costly and time-consuming to remediate. The loss from a data breach or outage is real.

The right NSPM solution enables the business to achieve its strategic and operational goals while cost-effectively mitigating risk. In this paper, enterprise IT professionals discuss how the right NSPM solution will address such challenges through greater visibility into the network, policy automation and compliance. Their insights come from reviews of the AlgoSec NSPM solution, published on IT Central Station.

The Continuing Evolution of NSPM

Network security managers face pressure on multiple fronts. They're dealing with increased network complexity. There are growing global compliance requirements and rules to track. The network itself now spans on-premises, public clouds, private clouds and everything in between. At the same time, the business wants to accelerate time-to-market, increase agility, produce more innovative applications and on and on—all without suffering a data breach or outage.

Aligning security with businesses requirements in NSPM takes automation. Old, manual processes that rely on Visio and Excel are unable to keep up with the pace of business changes. The new generation of NSPM solutions gives network security managers and network administrators the tools they need to deliver what the business wants—without overspending or stretching network operations teams beyond reason. They do this by unifying visibility, policy automation, and compliance.

All of this is happening in a complex environment. To stay secure and agile, the business needs its NSPM solution to automate the policy change process, conduct continuous network analysis, and monitor the network across the cloud and on-premises data center. Figure 1 depicts some of the elements the NSPM solution must interact with to realize such functions.

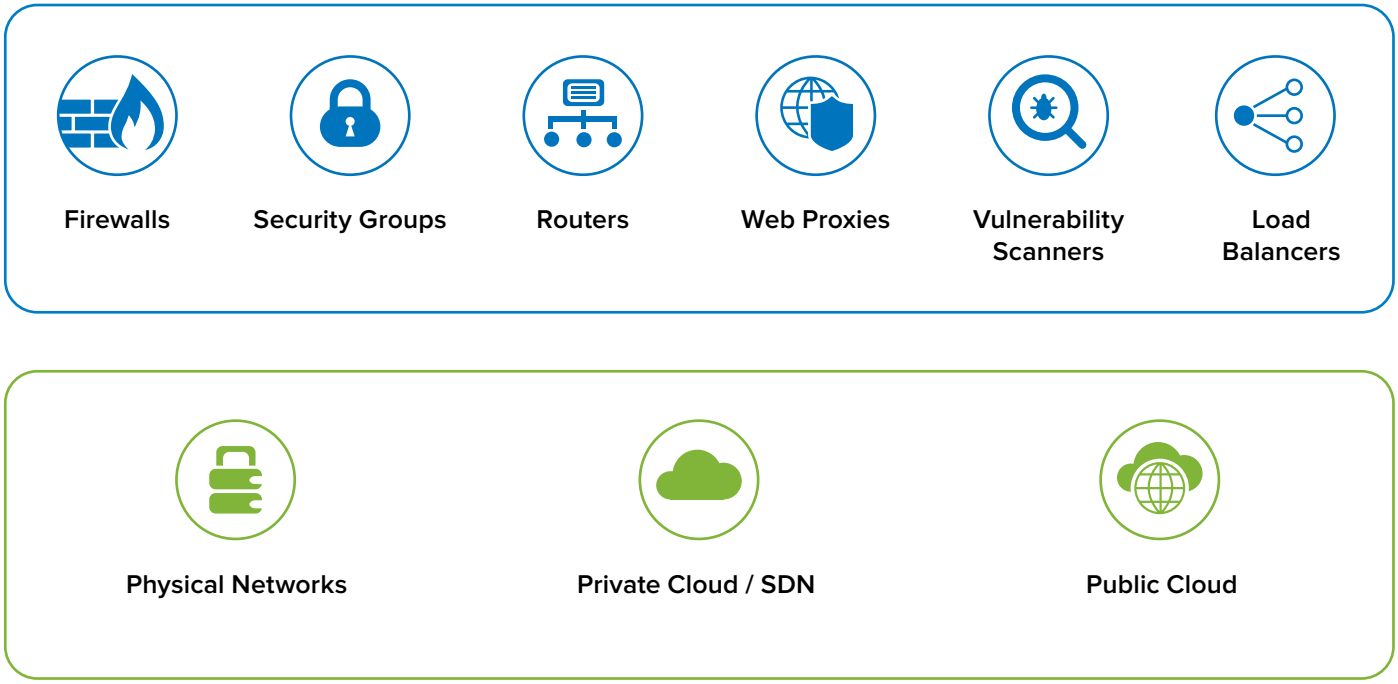


Figure 1 – NSPM solutions must provide visibility and automation for a wide range of network hardware, software and functional areas—on top of physical networks, private clouds frequently running software-defined networks (SDNs), and public cloud infrastructure.

Challenges Inherent in Selecting an NSPM Solution

There is no NSPM solution that satisfies all needs. Every organization has different technical and business requirements and security cultures. Solutions have to fit the network, business strategies, and existing business processes. However, when evaluating an NSPM solution, there are four critical issues:

- Dealing with misconfigurations - Manual processes frequently lead to misconfigurations. According to industry data, nearly all firewall breaches are caused by misconfigurations, not flaws. Automating previously manual processes results in fewer mistakes and misconfigurations.

- Automation as a strategy - Network policy automation is not an end unto itself. Rather, it supports the business strategy like maintaining security, ensuring SLAs, increasing cooperation and reducing friction between departments. It improves competitive differentiation through better customer engagement, e.g. by moving applications to the cloud, network policy automaton helps with regulatory compliance and frees IT time from housekeeping so it can be applied to digital transformation and supporting strategic initiatives.

- Understanding visibility requirements - Powerful NSPM tools give network admins and security managers a new depth of visibility into both network devices and business applications. By understanding their traffic flows across multi-vendor and hybrid devices, they can plug security holes, troubleshoot more easily, and discover applications and services.

- Compliance requirements - Meeting an audit requirement frequently takes your IT department out of commission as they focus on auditing. Organizations need to determine their regulatory compliance requirements, decide how much time they want to spend preparing for audits, and figure out how important continuous compliance is to them. They need to be sure that new changes do not violate internal or regulatory compliance requirements.

NSPM Solution Selection Factors

Members of IT Central Station, an industry site that features candid discussions and peer-to-peer user reviews from enterprise technology professionals, weighed numerous factors in their processes of selecting an NSPM solution. As they described in reviews of AlgoSec, a key consideration was the alignment of network security with business objectives. Their assessments touched on a wide variety of issues. These included the solution's ability to reduce misconfigurations during the process of digital transformation as assets move some of their data to the cloud and organizations embrace hybrid networks. NSPM user reviews also discussed the efficiency of network management operations and team performance.

Visibility and automation were significant factors affecting selection of an NSPM solution. Users want visibility into the network, traffic, and applications. They want to see what is happening with rules and applications while also monitoring policy changes. Regarding automation, what mattered to users was the ability to automate rules management, as well as configuration and change management. "Zero-touch" automation was considered useful, as was the ability to automate a multi-vendor environment.

Compliance is the other main driver of NSPM selection. Users rely on their solutions to facilitate compliance, including reporting. These needs include ensuring a state of continuous compliance as well as ensuring and demonstrating audit-ready regulatory compliance for major regulations such as PCI DSS, GDPR, and SOX. Users also have to ensure and demonstrate audit readiness for internal compliance requirements.

Network Security Policy as a Business Issue

Policies governing the network are inherently business-facing. Even when they concern entirely technical matters, a business objective is ultimately driving the policy process. For example, an IP network expert at a comms service provider with more than 200 employees described the value of AlgoSec by commenting, “It provides faster go to market with fewer resources. In one system, users can request access through the firewall for business services, which can be approved by the appropriate team and can be implemented automatically by the system itself.”

IT Central Station members spoke to the need to align network security with business objectives. An AlgoSec user at an energy/utilities company with over 10,000 employees remarked, “With AlgoSec, we can show a view of firewall compliance that is clean and easy to read and present. This also helps our business units ensure their policies are clean. With that data, we can show management that the firewalls connected to our network, but owned by other business units, meet our standards.” A Network Engineer at a tech services company with over 10,000 employees, shared that AlgoSec “helps us deploy new business applications quickly and securely. It ties cyber threats directly to critical business processes.”

> **...helps us deploy new business applications quickly and securely. It ties cyber threats directly to critical business processes**

Enabling Digital Transformation and Cloud Migrations

As network managers and security teams grapple with digital transformation and cloud initiatives, they want an NSPM solution that will facilitate the process. As an AlgoSec user put it, “We see

the value... for organizations involved in digital transformation projects migrating to public/private/hybrid cloud models." A Director of Information Security Operations at a consumer products company with over 1,000 employees, similarly shared that AlgoSec helped him with cloud support, spanning both native and hybrid environments.

Optimizing Team Performance

Network operations and security managers are keenly aware of team performance and its impact on the broader business. Budget-cutting pressure is relentless, while skills shortages potentially hamper effective operations. SLAs are a constant pressure. At the same time, the faster the team, the more agile the business. For these reasons, users view team performance optimization as a selection factor for an NSPM solution. For instance, an IT Technical Consultant at a manufacturing company with over 10,000 employees said that AlgoSec FireFlow "increases business efficiency and helps avoid bottlenecks in our NOC [Network Operations Center] team."

A Security Engineer at a financial services firm with more than 500 employees had a similar experience. He said, "Since we deployed AlgoSec, we have been able to assign more of our time to what really matters. It now takes less than half of the time it took before we had this tool to deploy the flows requested by the business." Previously, this had been a "very painful job," as he put it. "Now," he added, "We just put the source and destination into the AlgoSec Firewall Analyzer and most of the job for the flows is done." Another AlgoSec user found that the solution let him "increase the effectiveness of the team, allowing them to prioritize more complex and business-critical tasks in a faster manner."

> **"Since we deployed AlgoSec, we have been able to assign more of our time to what really matters.**

Visibility

Being able to align network security with business priorities depends on seeing what's happening across the network as well as within its policies and rules. A Manager of Network Service Delivery at a financial services firm with over 10,000 employees summed up the issue when he said, "It is worth spending the cost for visibility on security." A Security Engineer at a manufacturing company with over 1,000 employees, echoed this sentiment, commenting, "I think we have a great ROI due to the improved visibility and management that the solution now provides us."

Visibility into Network and Traffic

The network itself is the starting point of business-oriented NSPM. Network managers must see how traffic and network policies affect the network and their applications. Without the right tooling, however, much of the network can remain hidden. To this point, an AlgoSec user at a company with over 10,000 employees said, "I use this solution to have full visibility of the network, to simulate traffic queries, and to generate security reports according to the security policies of my company. The most valuable features are the network map, which provides the full visibility of the network, and the security reports."

Another AlgoSec user spoke about the benefits of the network map, saying, it was "a very good thing to get a clear view of every single region

> **... we have a great ROI due to the improved visibility and management that the solution now provides us.**

in your network." A Lead Security Infrastructure Consultant at a financial services firm with over 10,000 employees, added: "We also use AlgoSec to get better visibility into our traffic flows, to optimize our firewalls rules, and to analyze risks."

An AlgoSec user at a company with over 10,000 employees noted, “This solution provides visibility and comprehension of the network in our organization. It assists us in network security reviews and audits. In the end, a lot of time, we add context and build a security matrix matching our own standards.” A Senior Technical and Integration Designer at a retailer with over 10,000 employees further remarked that “AlgoSec provided a much easier way to process FCRs [Firewall Change Requests] and get visibility into traffic.” He contrasted this capability with his experience with previous vendors, a situation where, as he said, “we had to guess what was going on with our traffic and we were not able to act accordingly.”

Visibility into Applications

Network managers need to understand the impact of policy changes on business-critical network applications. Security policies affect application migrations as well as initiatives to establish network segmentation. In this sense, visibility into applications on the network is essential for aligning network security policy with business objectives. The Network Engineer addressed the issue by stating, “It [AlgoSec] automatically discovers applications and their connectivity flows, then associates connectivity

> “It automatically discovers applications and their connectivity flows...

with their underlying firewall rules.” For a System Architect at a school with more than 500 employees, the benefit came from the solution’s traffic simulation query. In his case, this “helps to understand which rules match or don’t match for a specific traffic pattern, helping troubleshoot application issues.”

“I have found the firewall optimization feature to be very valuable because most developers don’t know the ports or services their applications are running,” said an AlgoSec User. He then added, “After running the rules on any services for a short while, AlgoSec helps get the right service ports and IP addresses.” A Network Manager at a financial services firm with over 1,000 employees felt that AlgoSec has enabled his team to analyze rules to check access for an application or user. He related, “Breaking down a rule to specify used objects within groups and protocols used has proved invaluable for us to narrow exposure to potential threats.”

Visibility into Rules

NSPM users want visibility into rules. According to an AlgoSec user, the solution “provides great visibility into your firewall rules, thereby allowing

> “AlgoSec helps get the right service ports and IP addresses.

you to eliminate redundant or overlapping rules.” In particular, visibility into rules saved time by allowing his administrators to test network traffic and pinpoint which rules were being triggered for a particular traffic flow. A Technical Presales Engineer at a tech services company with more than 500 employees, described the value of AlgoSec’s policy tightening feature, which gave him visibility into ‘any to any’ rules. The tool could tell him which sources and destinations were used as well as the actual traffic from overly permissive rules. From this, he said, “We are able to tighten the policy of the firewall.”

Visibility into Changes

Policy changes are a potential source of risk exposure, especially in a large organization where team members may not be aware of others' actions. IT Central Station members highlighted this capability in their assessments of NSPM solutions. "Now, we can easily track the changes in policies," said a Network Security Engineer at a financial services firm with over 10,000 employees. "With every change, AlgoSec automatically sends an email to the IT audit team. It increases our visibility of changes in every policy."

"The compliance module provides full visibility of the risk required in firewall change requests," said the Manager of Network Service Delivery.

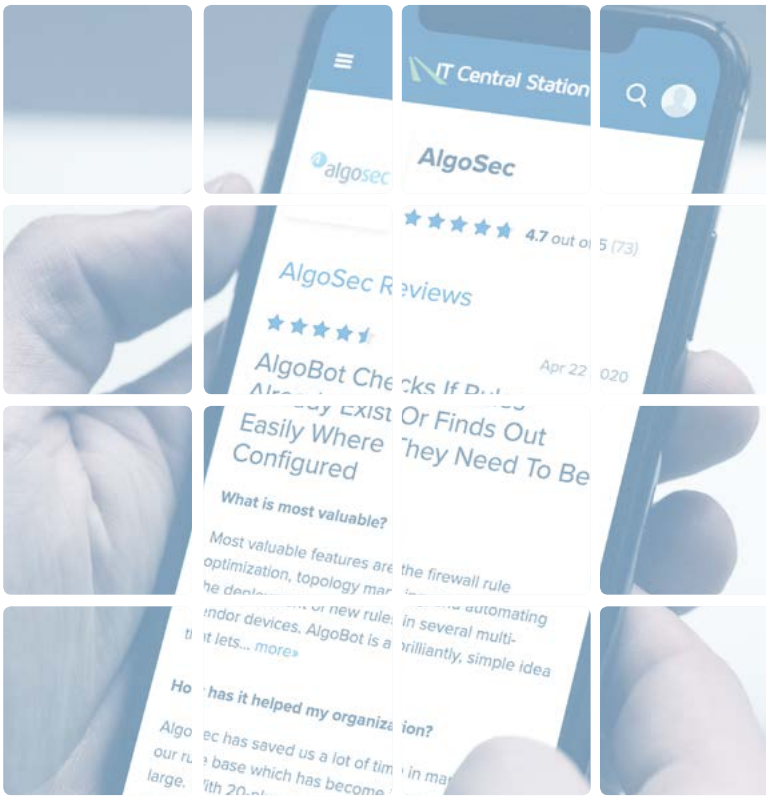
An AlgoSec user at a company with over 10,000 employees felt that "AlgoSec also allows us to have a history of changes." He believed the history was especially useful in the event of an outage or an unwanted change. For another AlgoSec user, "Policy optimization, visibility,

> **"With every change, AlgoSec automatically sends an email to the IT audit team.**

and a faster change management process has reduced unnecessary times required for manually changing processes. The resources are now utilized more effectively for other areas."

Automation

IT Central Station members stressed the importance of automation capabilities in selecting an NSPM solution. Reliance on manual processes is unsustainable. Experience shows that manual policy management leads to mistakes, misconfigurations, and missed SLAs. As the IT Technical Consultant pointed out, with AlgoSec, "we have eliminated any human mistakes that we have dealt with in the past and now we want to avoid as we are moving toward a completely automated network." Manual processes negatively affect agility as well. The issue is particularly salient today, as companies expect network operations to be as lean as possible.



Automated Rules Management

AlgoSec users are putting the solution to work in automating rules management. A Network and Security Engineer said, "We are also using AlgoSec to automate machine provisioning (creation of new rules associated with that machine) and machine decommissioning (removal of rules associated with that machine)." This capability is viewed as a positive attribute in an NSPM solution. According to an AlgoSec user, "We are currently in a rule base performance improvement process and AlgoSec is an invaluable tool to accomplish this. Furthermore, we are starting rule creation automation, which will also provide some relief on our workload."

> **"... we have eliminated any human mistakes that we have dealt with in the past and now we want to avoid as we are moving toward a completely automated network**

Other notable comments about rule management automation include:

- "My organization has used Firewall Analyzer for many years to simplify and automate rule set management across an estate of hundreds of Check Point firewalls. Key functionality provided covers compliance reporting and identification of duplicate and unused, as well as risky rules." - Security Consultant at a financial services firm with over 1,000 employees

- "We recently moved our data center to a new location, and we migrated our firewalls from one vendor to a different vendor. AlgoSec helped us tremendously to clean up shadow rules, unused objects even before moving to a new vendor." - AlgoSec User at a healthcare company with over 1,000 employees

- "Our primary use case is to clean up firewall rules of migration from Cisco ASA to another firewall vendor. We try to get rid of old rules and get these converted into new rules which apply better to our environment." - AlgoSec User

> **"The best feature for us is the ability to automate the change requests that come through our service desk..."**

Automated Configuration and Change Management

Being able to automate configuration and change management saves time. As a result, it's a driver of preference for NSPM solutions. "Automated change notification is a must and is critical in maintaining a safe environment and compliance," said an AlgoSec user. An Information Security Specialist at a company with over 10,000 employees also spoke to this benefit of AlgoSec when he said, "The best feature for us is the ability to automate the change requests that come through our service desk, which is done via the tool's intelligence to analyze the conditional rules." In his case, as he put it, "This used to be a big time sink for the guys which is now less of an issue. This means that the company can claim back valuable man-hours for other means (also showing a labor cost saving to the board)."

Zero-Touch Automation

To achieve the productivity gains desired by network security and operations managers, an NSPM solution should enable automation with as few hours as possible. The Network Engineer acknowledged AlgoSec in this regard,

> **"We use this solution for the management of firewalls on a client with a multi-vendor landscape.**

saying, "AlgoSec delivers a rich set of change management workflows and enables zero-touch change processes if no risks are identified." A Global Network Security Engineer similarly noted, "Initial deployment was straightforward. The FireFlow workflow can be configured to match the existing flow - customizing this to match any workflow permutations takes the most time."

Automating the Multi-Vendor Environment

Network security and operations environments are often multi-vendor in nature. They invariably have to support firewalls from Check Point, Fortinet, and Palo Alto as well as a host of other technologies, as shown in Figure 2. For this

reason, users prefer NSPM solutions that work well with more than one vendor platform. An IT Security Engineer III at a software company with over 10,000 employees, shared how he had previously spent time manually looking through rule bases trying to find risk rules. “Now we see it via AlgoSec,” he said, adding, “It also helps because we see those risks across multiple vendors.” This reduced the potential for error, in his view. A Senior Consultant at a consultancy said, “We use this solution for the management of firewalls on a client with a multi-vendor landscape.”

An AlgoSec user at an energy/utilities company with over 1,000 employees valued AlgoSec’s “ability to manage multiple vendor firewall policies and traditional firewalls with an intelligent way to prevent cyberattacks and reduce outages.” The AlgoSec user at the energy/utilities company further noted, “We are moving towards an automated environment so the ability to work

> **“... ability to manage multiple vendor firewall policies and traditional firewalls with an intelligent way to prevent cyberattacks and reduce outages.”**

with Ansible, ServiceNow, and Palo Alto gives us the ability to automate our firewall policy creation. And it does so in a manner where we do not have to worry about a policy being created that may put our organization at risk.”

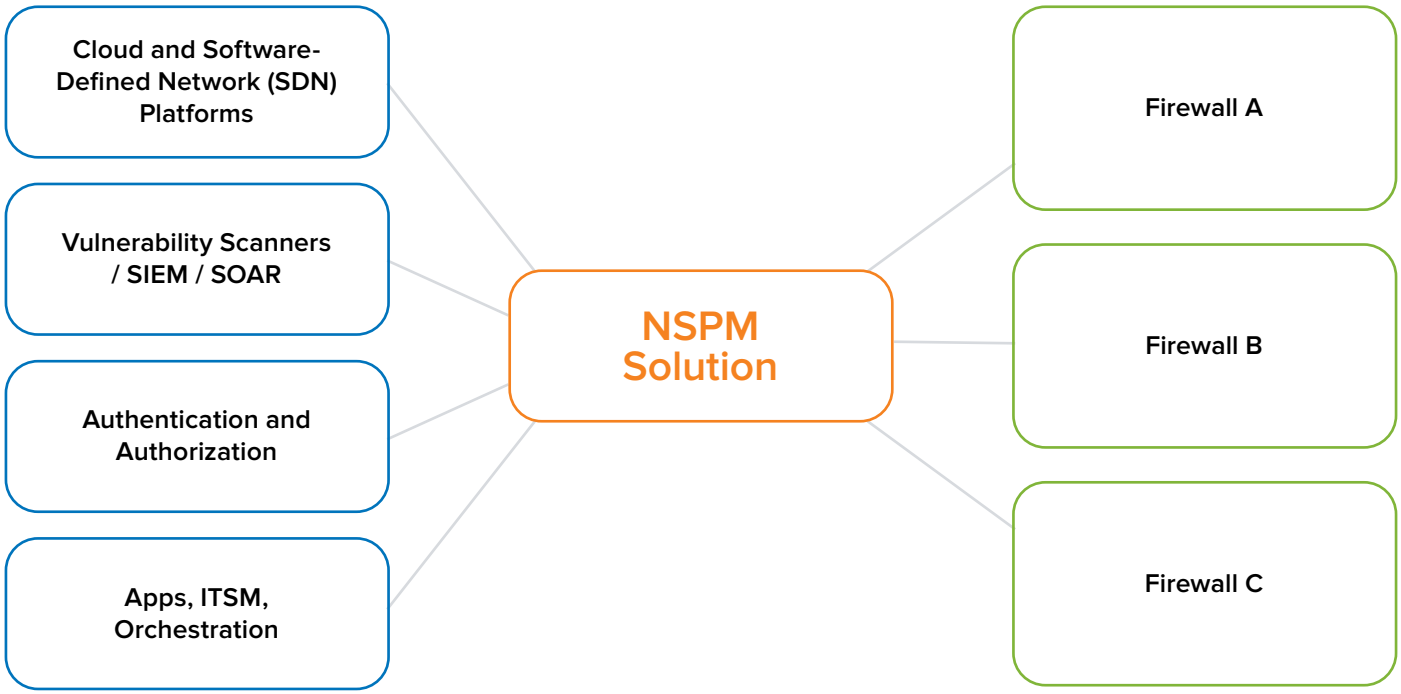
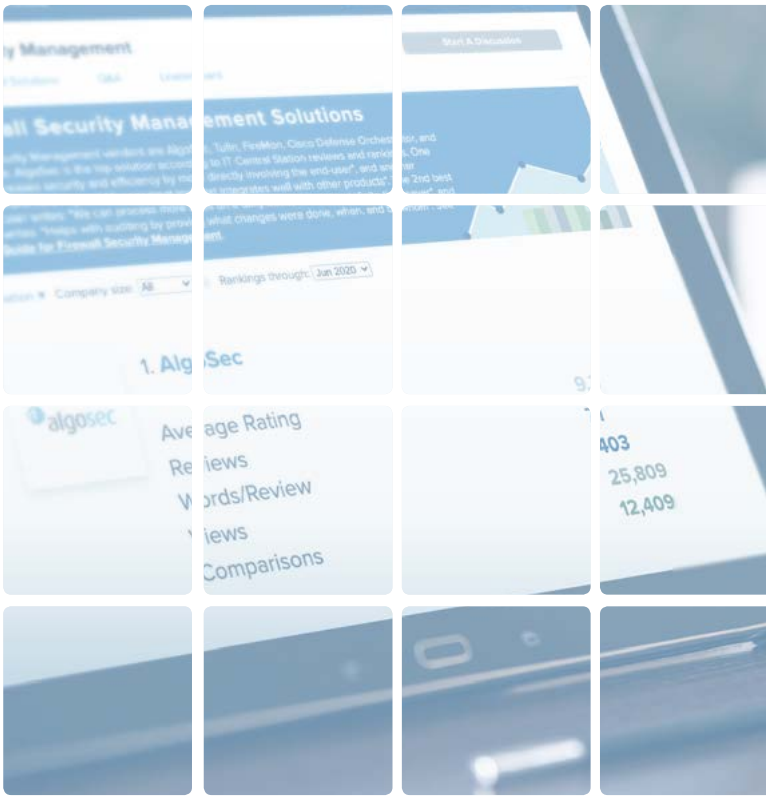


Figure 2 – Some of the platforms and technologies with which an NSPM solution should integrate.

Compliance

An NSPM solution must make it easier to enforce the network-level policies required for compliance with government regulations, such as Sarbanes-Oxley (SOX) and PCI DSS, than is possible without the solution. NSPM should also make it simpler to bring the network into compliance with internal-facing security policies and rules, e.g., “Routers may not be set to factory defaults.” These expectations are increasingly relevant as organizations adopt continuous compliance—no longer treating audits as a point-in-time exercise but rather working to adhere to policies and controls and continually maintain compliance, even with frequent and extensive network changes.



For example, a Security Consultant in a financial services firm with over 1,000 employees said, “Compliance and risk reporting are the most valuable features of the product.” A Global Network Solution Architect at AXA, an insurance company with over 10,000 employees, used AlgoSec for firewall rules compliance with global security policies. He relied on the solution “to ensure global policies are applied to all regional firewalls, provide auditing and compliance.”

Firewall Compliance

Network managers need to demonstrate that their firewalls comply with policies established to meet the audit requirements of regulations like SOX and HIPAA. This is a familiar aspect of network management and security, but one that gets revisited regularly as users try to make the process more efficient. In this context, the Prudential Manager of Network Service Delivery

stated, “The compliance module is one of the best features which can help anyone to perform security review with predefined security matrix configurations. The compliance module can save a lot of time for security reviews and provide full visibility of the risk required in firewall change requests.” The Security Engineer said, “It’s a great tool when preparing for audits and ensuring your firewalls are in compliance.”

Regulatory Compliance

Companies that are obligated to comply with government regulations benefit from automated policy management. The Network Engineer, for example, found that using an NSPM solution reduced his audit preparation efforts and costs drastically while enabling his team to maintain continuous compliance. An AlgoSec user also felt the solution helped in maintaining and providing regulatory compliance metrics and optimizing the overall security of the organization.

The PCI DSS compliance standard, required for companies that process credit card transactions, emerged as a frequent use case for NSPM:

- “The baseline of in-built policies such as PCI DSS helps us maintain good security ratings in compliance with regulatory standards.” - Security Operations Manager at a financial services firm with more than 200 employees
- “I work at a multi-vendor firewall environment. AlgoSec is primarily used to see what firewall policies are in place, as well as PCI compliance levels.” - Sr Firewall Engineer at a tech consulting company with over 1,000 employees
- “It is very useful for PCI DSS compliance.” - Presales Manager at a small company

Internal Compliance

IT Central Station members discussed their internal compliance needs as well. The Network Manager placed this issue into context by saying, “The risk and compliance area is key to ensuring we conform to company regulations. Having a number of compliance options to baseline ensures that we get the basics right before looking at advanced risks and remediation.” To this point, the Security Engineer said, “We also need the audit report and risk assessment features to send to our InfoSec team so that they can use it in our audit documentation. This is also very important because it significantly reduces our workload and makes it very easy to have the documentation ready to show to our auditors.”

> **“The compliance module is one of the best features which can help anyone to perform security review with predefined security matrix configurations**

The Network and Security Engineer was pleased that AlgoSec enabled his team to provide reports to auditors “without losing a single day from the network support department.” He said, “We simply provide AlgoSec reports and analysis.” Another AlgoSec user acknowledged AlgoSec’s ability to help him prepare for the audit in a short time and assist with continuous compliance. The Network Manager added, “The risk and compliance area is key to ensuring we conform to company regulations.” A Network Administrator at a government agency with over 10,000 employees, simply stated, “For us, it is a great management and audit tool.”

CONCLUSION

Many factors come into play in the selection of a network security policy management solution. In a business environment, where companies want to be agile, users want solutions that offer visibility into traffic and applications. For IT Central Station members, a good solution automates rules management along with configuration and change management. The best solution will also facilitate compliance, both internal and regulatory. With these qualities, an NSPM will be able to align security with business and make sure that your network adheres to your stated security policies.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT ALGOSEC

AlgoSec enables the world's largest organizations to align business and security strategies, and manage their network security based on what matters most — the applications that power their businesses.

Through a single pane of glass, the AlgoSec Security Management Solution provides holistic, business-level visibility across the entire network security infrastructure, including business applications and their connectivity flows — in the cloud and across SDN and on-premise networks. With AlgoSec users can auto-discover and migrate application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate time-consuming security changes— all with zero-touch, and seamlessly orchestrated across any heterogeneous environment.

Over 1,800 leading organizations, including 20 of the Fortune 50, have relied on AlgoSec to drive business agility, security and compliance. AlgoSec has provided the industry's only money-back guarantee since 2005. For more information, visit www.AlgoSec.com.