# Research Summary: Network Security Policy Management Tools –Tying Policies to Process, Visibility, Connectivity, and Migration

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report

Written by David Monahan

Updated Q1 2018

**Sponsored by:** tufin

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

# Report Summary: The Value of Network Security Policy Management Tools for Improving Change Management, Application Continuity, Security, Cloud Migration and Disaster Recovery

## Table of Contents

# Executive Summary

This report queried companies that use Network Security Policy Management (NSPM) tools and companies that do not in order to compare and contrast their security change management process, timeliness and efficacy. The evaluation considered whether there were any differences in their inherent risk profiles and if or how NSPM created improvements in security performance.

In fact, organizations leveraging NSPM demonstrated significant advantages in both IT operations (ITOps) and security operations (SecOps). Advantages included more consistent security policies, which led to fewer attack surfaces, shorter change approval and implementation processes, fewer change-related outages, more successful business continuity and disaster recovery testing, and more.

Participants coming from environments where NSPM was not used felt they had strong IT and security visibility, but had more significant issues with poorly implemented security policies, non-standardized policies, and failed cloud migrations for critical business applications. The NSPM group had a more realistic outlook.

# Demographics Overview

The data-driven security research team contacted 100 companies that used NSPM solutions and 102 that did not. Participants were from North America. Within the respondent pool, the roles identified represented a good selection of executives down through individual contributors from IT- and security-related disciplines. The security-related disciplines included cyber security, fraud, risk, and compliance, and will be collectively referred to as "security" throughout the report.

For the purposes of this report, company size by number of employees and distinct geographical locations having their own gateway security controls were recorded and, as expected, were germane to multiple aspects of the report.

Small businesses generally have fewer locations and were found to have simpler gateway control policies, which essentially negates the need for a policy management and orchestration solution. A significant catalyst for deciding when to purchase an NSPM solution also related to the number of different firewall vendors the organization used for defense. Having at least two different firewall vendors in operation increased the need for an NSPM solution. It was interesting to see that 66 percent of the organizations surveyed used between two and three different firewall vendors' solutions.

# The Driving Need for NSPM

## Key Problem Driver: Security Should not Restrict Business—it Should Facilitate it.

In the race to continue forward, many organizations seem to forget that security policies are not tied, but must be driven by business processes. To this end, network security policies should be considered, created, and tested in the context of how they will impact the business process they are meant to protect. In today's ecommerce-driven and Internet-connected world, a policy should be invoked to protect communications and transactions. If they do not, then they should not be considered. However, one of the common problems is the inability to have true visibility into the end-to-end effectiveness or impacts of changes. The lack of visibility came out as an interesting issue. Organizations that have never used an NSPM really believe they have visibility into how changes will affect business processes and application operation. However, their responses (compared to organizations using an NSPM solution) are significantly different when it comes to changes negatively impacting business process, application operation, migrating applications into the cloud, and in business continuity and disaster recovery planning.

## Breaking Through the Security Façade

Despite the high rate of failed changes, 98 percent of the organizations doing manual inspection think they have moderate to high visibility in how applications communicate within their infrastructure. Ninety-seven percent said they have high to moderate visibility into how requested changes may negatively impact running applications. Yet, 58 percent of organizations using manual policy inspection said the inability to maintain standardized policies was a significant to very significant factor in security or operations incidents, including accidental blocking of applications, and 34 percent said that security device misconfigurations were the primary cause of outages.

How can that be? Much of it comes down to the fact that companies don't know what they don't know, and never had greater enlightenment. Their perspective on how much greater visibility they could have is skewed. This would be comparable to having always walked everywhere without knowing cars existed and, thinking you are a fast walker, stated you get everywhere quickly.

In another correlation, of the organizations that said they do not have the ability to thoroughly test applications, 71 percent are confident that their business continuity/disaster recovery (BC/DR) plan will operate the first time it is activated. Without full visibility of application connectivity flows, the probability of being successful in the first run of a BC/DR rollover is very low. Having been through multiple tests in several companies, a lack of visibility into business-critical applications was a serious impediment to success, requiring hours of additional investigation and testing after the failure. Being open-minded and realistic about ITOps and SecOps capabilities is essential to maintaining success in BC/DR planning and testing.

## Ad Hoc Firewall Policies

Participants were asked if they had established baselines for their firewall policies. Surprisingly, for a technology that has been well established for years, 71 percent of respondents had problems establishing and maintaining security policy baselines and standardized policies. Only 29 percent of participants indicated their organizations had strong consistent firewall security policy baselines and 40 percent had done almost nothing to establish policy standards!

## Manual Policy Analysis vs. Using the Right Tool for the Job

Forty-three percent of organizations using manual inspection indicate they spend 5-10 hours per firewall per quarter reviewing policies. Only 28 percent of organizations using a firewall vendor's tool are in the same bracket. That number drops to only nine percent for those using a third-party tool like NSPM, because they generally spend significantly less time on change management.

Eighty-one percent of those using a third-party tool like NSPM said they experienced a problem in less than ten percent of their change windows while 86 percent of those using manual policy inspection experienced a problem in greater than ten percent of their change windows. Organizations using an NSPM solution have far fewer changes that negatively impact operations.

## Cloud Migration of Business Applications Fraught with Problems

Seventy-one percent of participants said they currently have or had a project in the last 12 months to migrate a business-critical application into the cloud. Of those organizations, forty-nine percent indicated the migration was negatively affected by their lack of understanding about how the application communication flows operated. Of the organizations that were negatively affected, only 14 percent were using a third-party tool like NSPM.

## Strategies for Managing Security Workloads and Complex Policies

The research identified three strategies for dealing with security policy complexity and workload. One was to outsource the function to an MSSP. Another was to purchase an NSPM solution. The last was to just muscle through with whatever resources and vendor-supplied or home-grown tools the companies had. The latter was fraught with the most problems which are identified throughout the report. The first two seemed to be the better choice, with the decision being based on business operations, compliance, and financial requirements.

The primary reason for outsourcing seemed to be a lack of trained security resources and a generally overburdened program. On the other hand, choosing to retain firewall management and use an NSPM solution was more based on having the staff, but needing to be able to do more with them and reduce errors, which in turn freed more cycles because there is less rework.

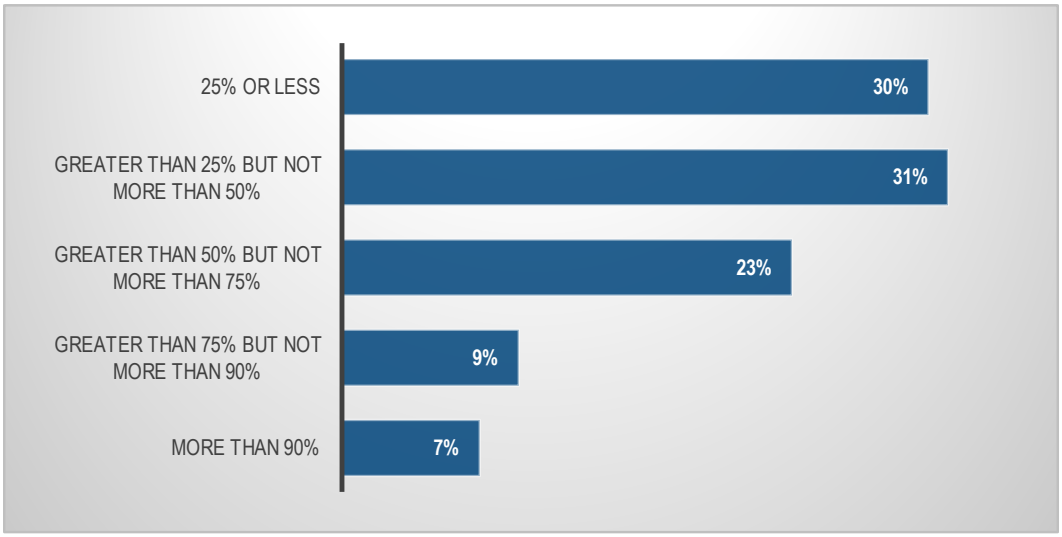


*Figure 1: Firewall Management Outsourcing*

Short turnaround times for changes, combined with high volumes of change, is a growing issue. In organizations with at least two firewall vendors or over ten firewalls in place from a single vendor, the problems with errors impacting production and additional load and delivery delays due to rework increase. Sixty-two percent of respondents with two or more firewall brands in-house indicated their greatest benefit of utilizing an NSPM solution was reducing improperly implemented changes. Organizations with greater than 25 firewalls from the same vendor indicated their NSPM solution had most improved the prevention of change-related outages.

### The Intersection of Heterogeneity and Policy Misalignment

It takes a coordinated effort to standardize security policies. In general, 69 percent of respondents indicated it was moderately difficult to virtually impossible to maintain standardized firewall policies.

For organizations that have trouble maintaining the synchronized policies, over 90 percent indicated that the inability to maintain the standardized policies was a significant to very significant factor in security operations incidents. The root cause of such issues was inappropriate access (leading to denial of service or data leak), or in causing unintended blocking of authorized applications, which creates a business impact.

# Improving Security with an NSPM Solution

## Benefits of Use

Listed are the top ten benefits that NSPM users indicated they get out of their chosen solution.

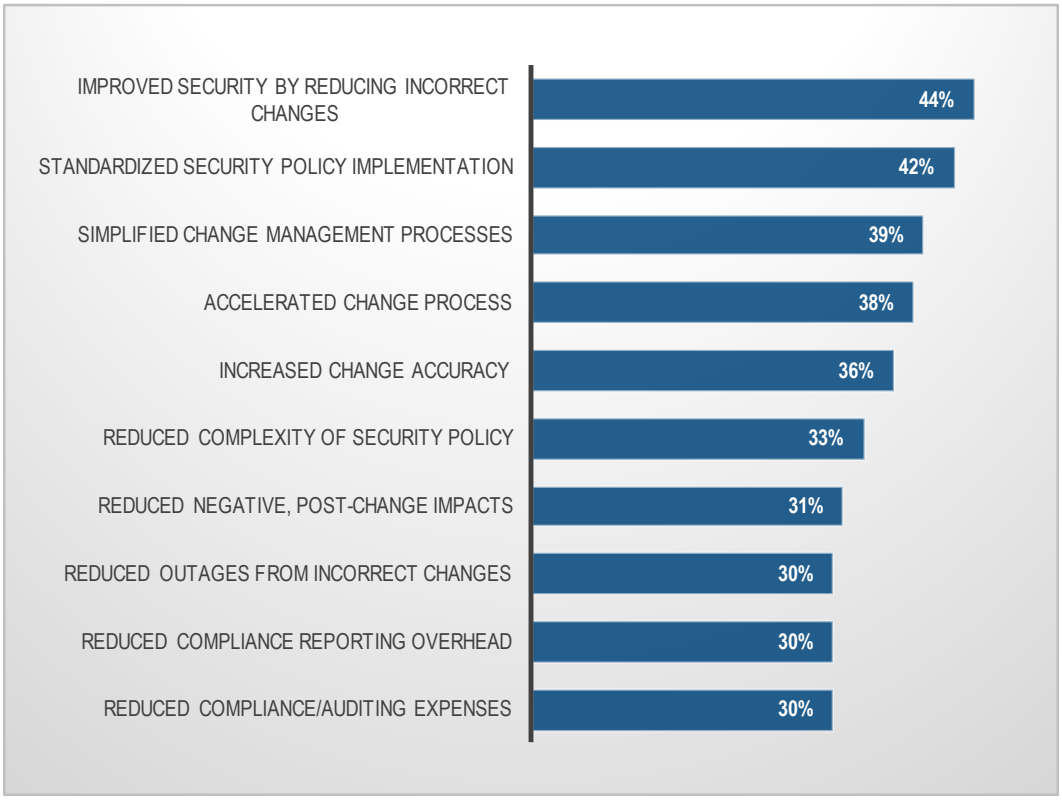


*Figure 2: Top 10 Benefits of Using an NSPM Solution for Firewall Change Management*

Each of the listed items is a significant improvement area when applied to SecOps and many apply to ITOps as well. If a change causes an outage, it directly affects ITOps.

## Improved Work Outcomes

In addition to the benefits already listed, respondents identified a set of improved outcomes from having an NSPM solution. The highest response was reducing security incident frequency. By standardizing policies and becoming more readily able to do pre-change testing, SecOps was able to preemptively reduce their incidents. This created more time for the analysts to do value-add work. Thirty-eight percent of respondents identified reduction of pre-implementation change testing as a key part of NSPM improving change management. Other reductions are listed in Figures 3a and 3b.

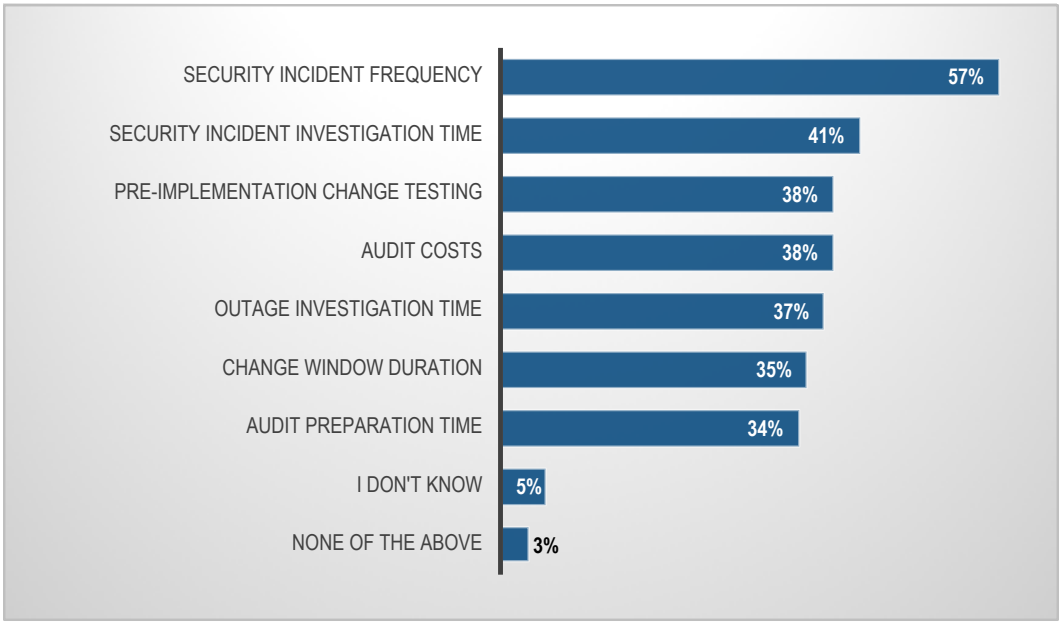


*Figure 3a: Work Reductions Created by Utilizing NSPM*

Though security is a top concern and improved security is a core outcome, more respondents felt that they had greater improvement in change management outcomes. In fact, respondents using an NSPM solution reduced their change approval and implementation process from an average of 12 work days to 1 per change.

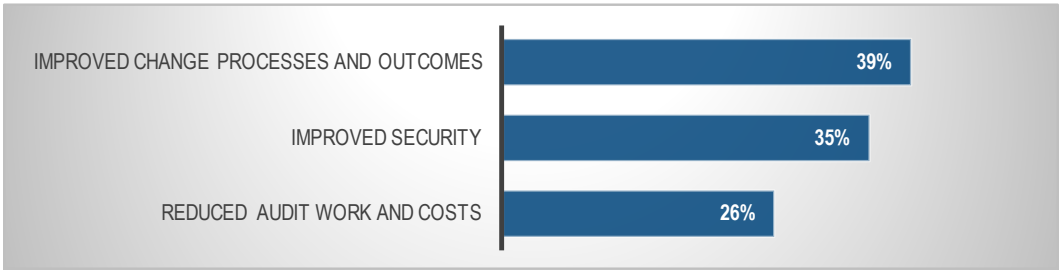


*Figure 3b: Most Improved Outcomes of Utilizing NSPM*

## Detection and Prevention of Undesirable Outcomes

Pre-change, NSPM solutions can validate proposed changes to ensure they meet the desired security posture and do not break existing applications, while detection after the changes has numerous other benefits.

- Thirty-four percent of respondents use it for identifying incorrect or unsynchronized firewall policies.
- Sixty-four percent of respondents said their NSPM solution prevented improperly implemented changes and the related outages. Twenty-six percent of respondents indicated their NSPM solution prevented the spread of ransomware.

- Twenty-three percent of respondents stated that using the NSPM solution post changes for verification allowed them to identify improperly executed or unauthorized changes.
- Respondents who are not using an NSPM solution had a higher rate of occurrence of incidents stemming from incorrectly implemented changes, between forty-six percent and fifty-nine percent higher, than those using an NSPM solution, depending on the volume of changes in the organization.[1]

The data clearly shows how imperative it is to have a reliable tool to perform configuration checks both prior to and after change implementation to reduce errors and related incidents and outages.

# Choosing the Right NSPM Solution

## Primary Use Cases for NSPM

Evaluating the comments from respondents revealed that there is more value in separating the use cases customers and prospects are trying to address with their solutions. This breakout is not only helpful to vendors to understand the differences, but also perspective buyers. Since the participants were split almost equally, each group is well represented. Each group can see how their peers are using or intending to use the solution.

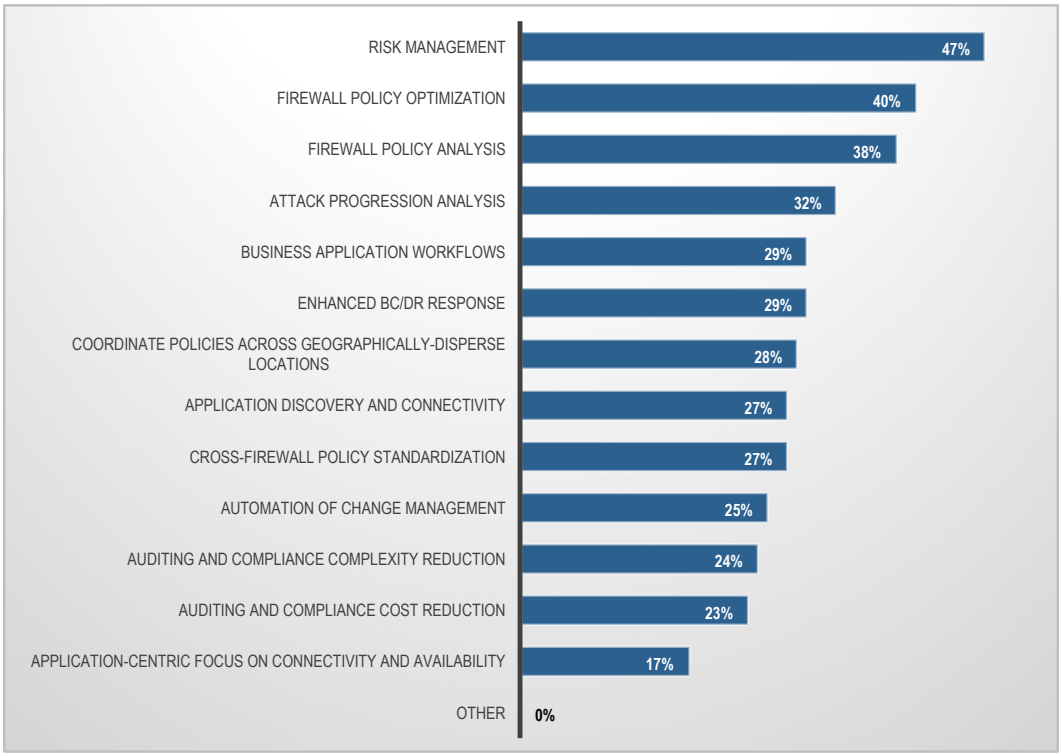


*Figure 4: Primary Use Cases for NSPM (From Customers)*

[1] Figures based on at least a weekly change frequency.

### Why Customers Feel They Received Greater Than Expected Value

Of the respondents who are using NSPM, 23 percent said they had received greater than expected value. When looking at the cumulative responses (the question offered the opportunity to choose up to three responses), 60 percent of organizations improved security by reducing incorrect changes. Many of the answers can be attributed to better visibility into policies and how changes affect their environment (29 percent), reducing the time and dollar expenses of required compliance activities (22 percent), and others. These are often outcomes of identifying additional use cases after purchase, greater than expected ability to automate change processes, higher visibility into the change process and security policies, and better understanding of how business applications communicate and are accessed.

### Why Customers Feel They Received Less Than Expected Value

The nine percent of respondents who indicated they received less than expected value are driven by several issues. However, most of these can be boiled down into two areas. The first is a lack of understanding the problem they are trying to solve, and therefore purchasing the wrong solution for the wrong problem(s). Most of the time, this occurs when organizations fail to properly understand the root cause of their problems and fail to document their requirements. The second is a failure or inability to sufficiently test the solution to understand how it works and how it will disrupt their current processes. Though there is extensive common ground among solutions, each solution provider has its own strengths, which should be mapped to requirements and to both the current and desired business state.

## Conclusion

No tool is a perfect answer, and not all solutions do everything flawlessly. However, each tool category has its place and can provide value. In the case of Network Security Policy Management, each vendor has an approach to solving the issues surrounding poorly implemented firewall policies, impacts from an inability to manually scale policy management and audit firewall policies, the effect of firewall policy changes prior to implementation, and the overall network security change process.

Though useful for any company with a firewall in place, NSPM tools provide the greatest value as the company grows, providing more value with large-scale coordination and policy review, and broad policy pushes across multiple firewalls in homogeneous and heterogeneous architectures.

Leveraging these tools will absolutely increase security, decrease attack surface and risk, and accelerate the ability to process changes more quickly and accurately. They allow staff to give more focus to high-value tasks in areas such as architecture, application, policy design, and other areas technology is not ready to address.

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

---



**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3635-SUMMARY_Tufin.062718