2016 Firewall Management **Trends Report**

A survey of trends in firewall use and satisfaction with firewall management

JANUARY 2016

Prepared for Skybox® Security by Jon Friedman, CyberEdge

Executive Summary

Firewalls are a core component of cyber security for every enterprise, regardless of size and industry. They are the frontline defense for blocking attacks and malicious web traffic. They collect information that is critical for detecting advanced attacks and alerting security teams. With the expanding use of "next generation firewalls" (NGFWs), they also serve as platforms for an increasing range of security services, including intrusion prevention system (IPS) and web filtering capabilities and application monitoring.

Yet very little hard data is available on how firewalls are used and managed today.

This report seeks to provide that data so managers can make informed decisions about how to improve their security programs. Information on industry practices and trends can also help enterprises make intelligent investment choices that strengthen security and protect their business in the most cost-effective way.

The report is based on a survey conducted by Skybox Security in late 2015. The survey questioned IT personnel at 334 enterprises and government agencies with 500 or more employees in a cross-section of industries. The survey was designed to elicit three types of information:

- **Data on current practices**, so readers can compare themselves with industry norms.
- **Data on plans and intentions**, so readers can see what their peers are thinking and planning.
- **Data on satisfaction with current firewall management capabilities**, so readers can assess where current practices are succeeding and where they have the most room for improvement.

In a number of cases we drill down to look at data from segments of the respondents and answer questions about which factors are most likely to be linked with high or low satisfaction.

Some of the key findings from this survey include:

- Two-thirds of the enterprises in this survey have firewalls from two or more vendors.
- Most organizations are either not satisfied or only "mildly satisfied" with their ability to perform analytic tasks such as auditing firewalls, analyzing proposed firewall rule changes, cleaning up firewall rules, performing periodic rule reviews, mapping networks, analyzing proposed routing changes, and analyzing network paths.
- Enterprises that use third-party firewall management tools and in-house developed firewall management tools are significantly more satisfied than enterprises using management tools supplied by firewall vendors and enterprises with no firewall management tools at all.
- The most important tasks related to NGFW were optimizing and managing IPS capabilities, followed by utilizing application-related rules.
- Updating IPS signatures frequently is seen as either "very important" or "mildly important" by a whopping 97% of the respondents. However, only 37% of the enterprises currently update IPS signatures frequently, indicating that this will probably be a high priority goal in 2016.

About the Survey Population

This report incorporates data collected from IT professionals around the world at 334 enterprises and government agencies with 500 or more employees. The largest clusters of enterprises were in financial services and IT services, but significant numbers were included from telecommunications, healthcare, retail, manufacturing, education, utilities, and state, local and federal government agencies.

Respondents were drawn from a variety of roles, including security operations, network operations, security architecture, and firewall administration. But the sample also includes significant numbers of IT security executives and managers and also staff from compliance management and risk management groups.

Data about the enterprises and respondents is included in the appendix.

Importance Scores and Satisfaction Scores

Several of the questions in the report asked the respondents to rate the importance of various firewall management tasks as "very important," "mildly important," or "not important." In order to compare the importance of these tasks to each other, we calculated an "Importance Score" for each question using the formula:

$$\frac{(\#\text{ of "very importants"} \times 9) + (\#\text{ of "mildly importants"} \times 5) + (\#\text{ of "not importants"} \times 1)}{\#\text{ of responses}}$$

Other questions in the report asked respondents to assess their satisfaction with various firewall management capabilities as "very satisfied," "mildly satisfied," or "not satisfied." We used the responses to calculate a "Satisfaction Score" for each question, using the formula:

$$\frac{(\#\text{ of "very satisfieds"} \times 9) + (\#\text{ of "mildly satisfieds"} \times 5) + (\#\text{ of "not satisfieds"} \times 1)}{\#\text{ of responses}}$$

For both scales, lots of "very important" or "very satisfied" responses produce a score greater than 5.0, while lots of "not importants" or "not satisfieds" produce a score less than 5.0.

Current Practices

NUMBER OF FIREWALLS

We asked respondents about the number of firewalls in their organization. Exactly 50% have between one and 49, another 30% have between 50 and 499, and 20% have 500 or more.

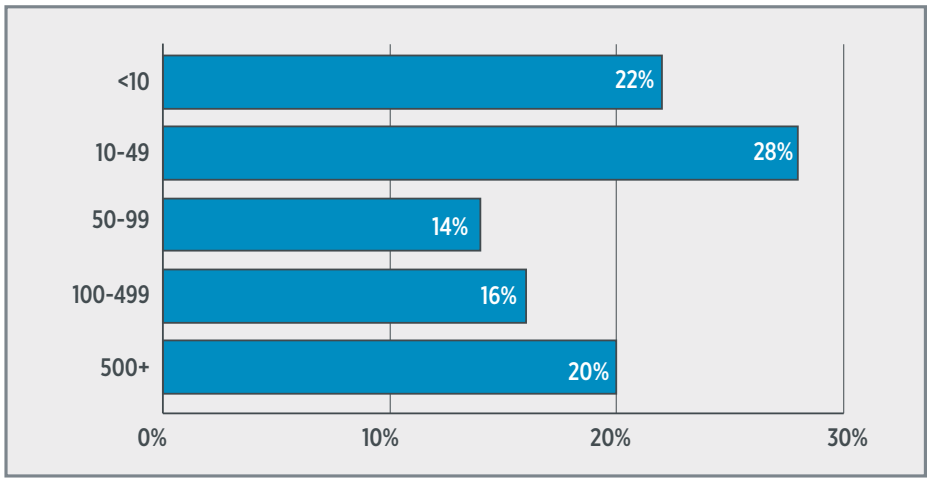

FIGURE 1: NUMBER OF FIREWALLS IN ORGANIZATION (319 RESPONDENTS)

Not surprisingly, in most cases the number of firewalls is related to the number of employees. For example, of enterprises with 500-999 employees, 93% have 49 or fewer firewalls. Of organizations with 10,000 or more employees, 75% have at least 50 firewalls and almost half of those have 500 or more.

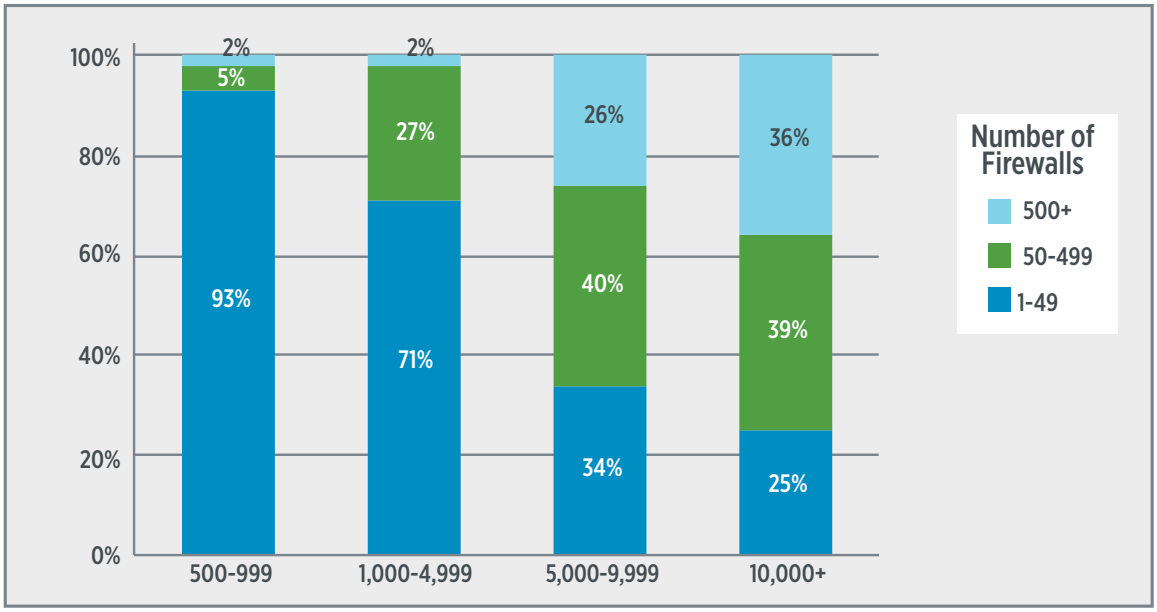

FIGURE 2: NUMBER OF FIREWALLS IN ORGANIZATION 319 EMPLOYEES

FIREWALL VENDORS

In terms of firewall vendors in use in the enterprise, Cisco and Check Point lead the pack, followed by Juniper Networks and Palo Alto Networks. Fortinet, McAfee, SonicWALL, Barracuda Networks, WatchGuard, and HP round out the field.

Looking at just these 10 suppliers, 32% of the organizations have just one vendor, 28% have two, and the remaining 40% are definitely multivendor shops with between three and six suppliers represented. The two-thirds that are multi-vendor shops have an average of 3.1 firewall suppliers.

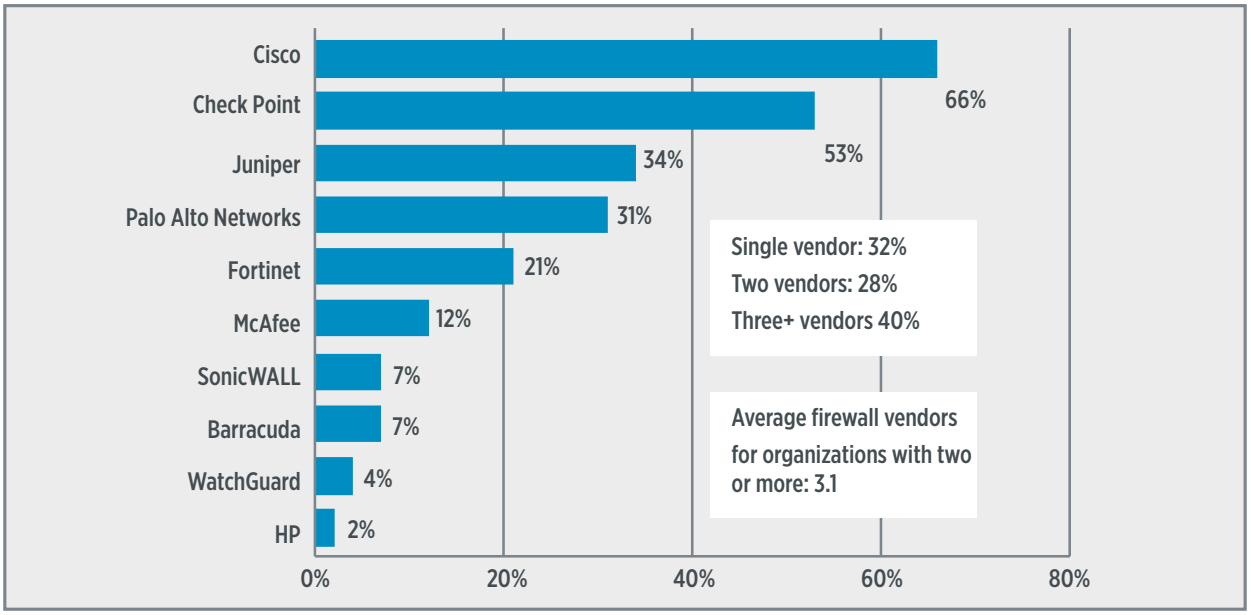

FIGURE 3: FIREWALL VENDORS IN ORGANIZATION
319 RESPONDENTS (MULTIPLE ANSWERS ACCEPTED)

STANDARDS COMPLIANCE

When asked about standards, 77% of respondents cited the need to enforce internal policies. The pervasiveness of this response implies that there are many industry- and business-specific security and compliance needs not reflected in broad industry standards. Another contributing factor is that many regulations such as Sarbanes-Oxley and HIPAA don't specify requirements at a level that can be reflected in regulation-specific firewall or IPS rules. Instead, enterprises are designing internal policies that reflect the intent of multiple standards and regulations.

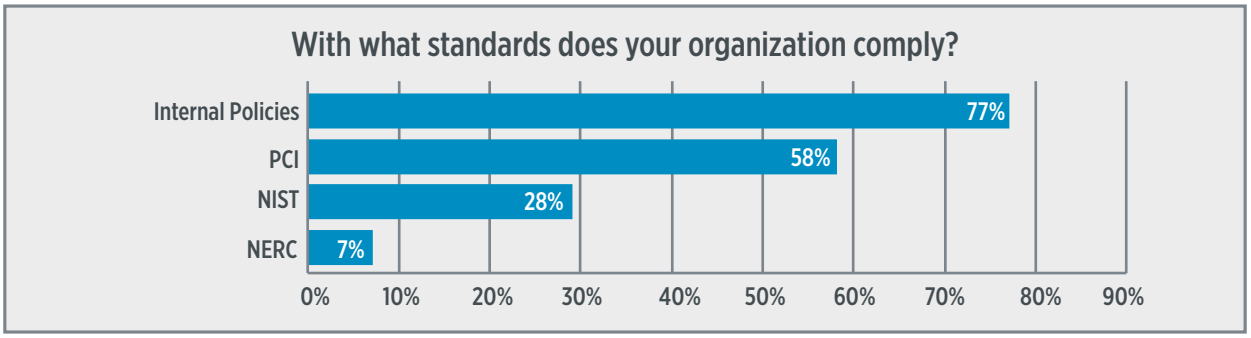

FIGURE 4: 299 RESPONDENTS (MULTIPLE ANSWERS ACCEPTED)

FIREWALL MANAGEMENT TOOLS

Respondents were asked what tools their organization uses to manage firewalls. The largest group (39%) mentioned only "tools supplied by the firewall vendor." Almost as many (37%) mentioned more than one type of tool. Smaller groups mentioned third-party management tools only (10%) or in-house developed tools only (5%).

The quantity of firewalls in the enterprise made a big difference on some of the answers. More than half (57%) of organizations with nine of fewer firewalls rely entirely on tools from a firewall vendor, but that number drops rapidly as the number of firewalls managed grows. Only 16% of enterprises with 500+ firewalls use firewall vendor-supplied tools exclusively. Conversely, the use of multiple tools rises from only 17% when there are few firewalls to manage, to 63% when there are more than 500. The percentage that rely exclusively on third-party and in-house developed tools is fairly constant across all sizes of enterprise.

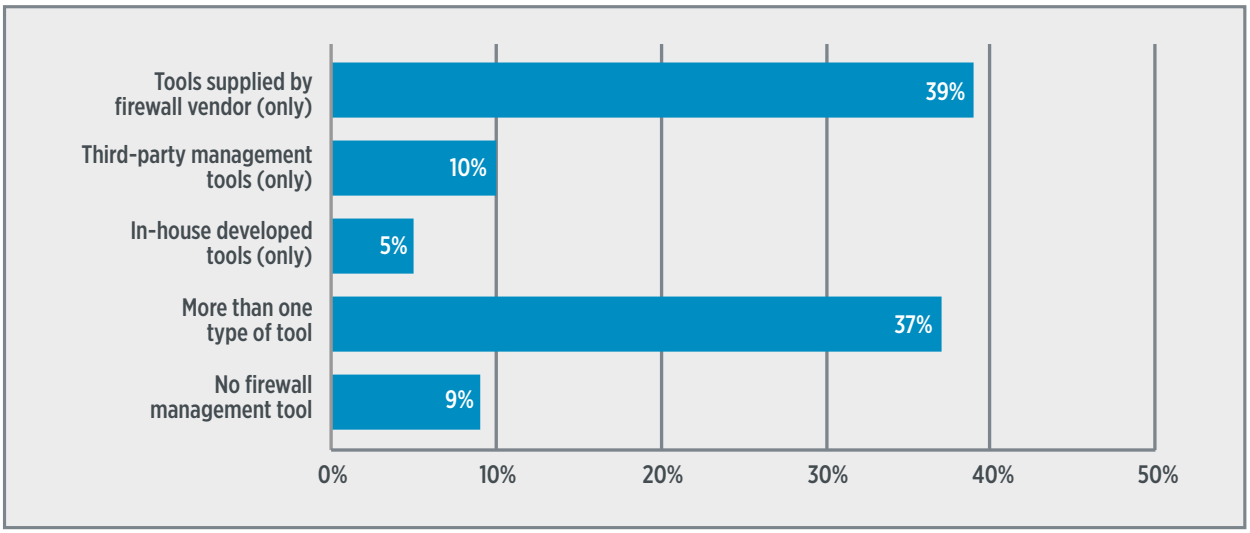

FIGURE 5: TOOLS USED TO HELP MANAGE FIREWALLS
322 RESPONDENTS

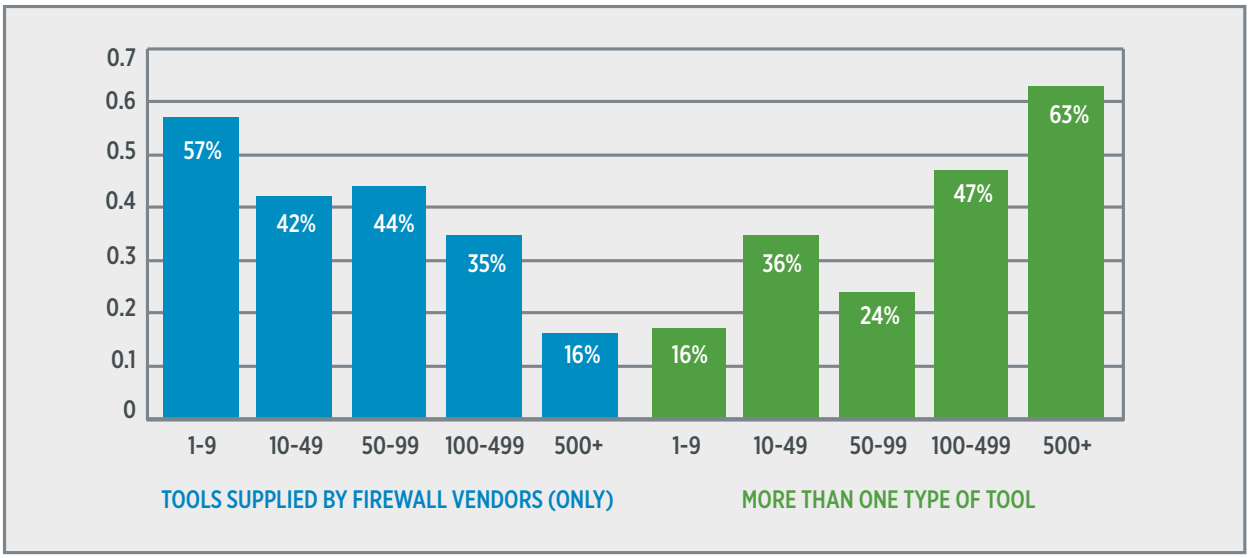

FIGURE 6: TOOLS USED TO HELP MANAGE FIREWALLS
322 RESPONDENTS

Plans and Intentions

Outsourcing Firewall Management

The idea of outsourcing firewall management has its fans, but they are still a small group. Only 20% of the respondents said their organizations are currently outsourcing any aspect of firewall management or plan to do so within one year. Almost three out of four (72%) said their enterprises have no plans in that direction.

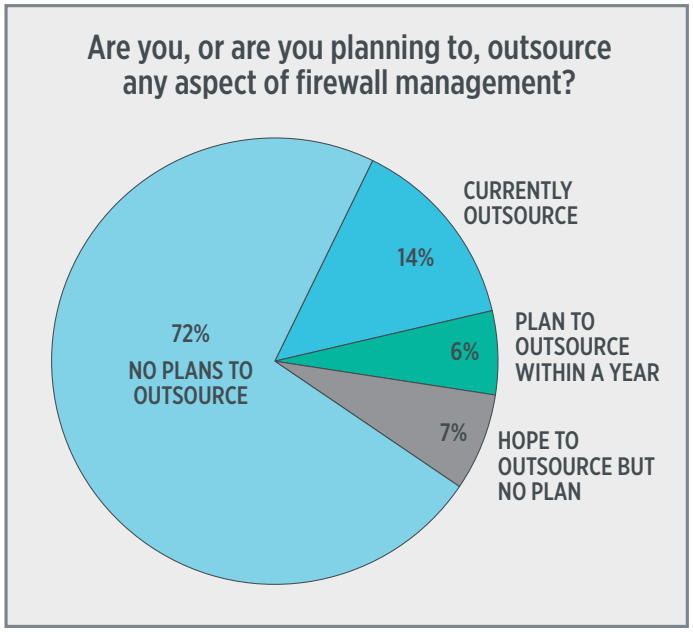

FIGURE 7

Automated Provisioning of Firewall Rules

Views are mixed on the practice of using third-party tools to automate the provisioning of firewall rulesets (that is, changing rulesets programmatically, without human intervention). Almost a quarter of the enterprises in our survey currently use third party tools, slightly more than a quarter wish to, and exactly one quarter each plan to use third-party tools only for certain situations and say they will never use them.

The reluctance shown by many respondents can be attributed to reservations about the reliability of automated provisioning, and the concern that mistakes could disrupt important business processes.

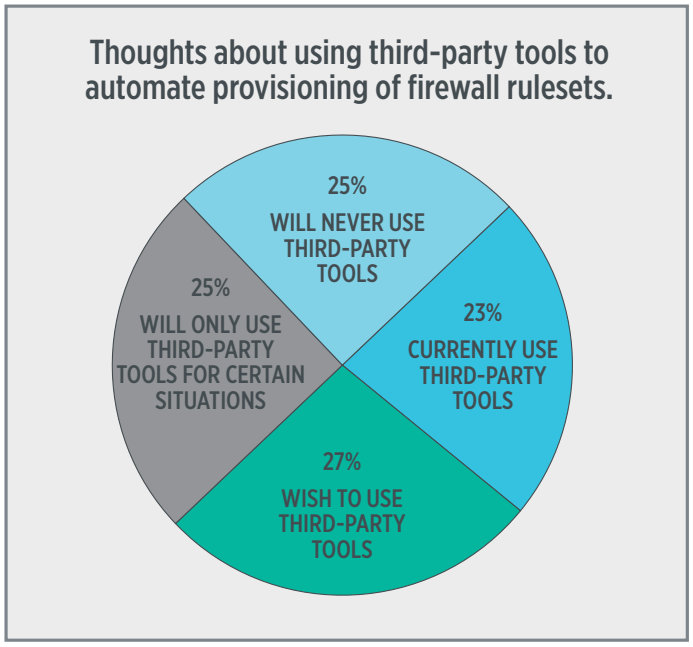

FIGURE 8

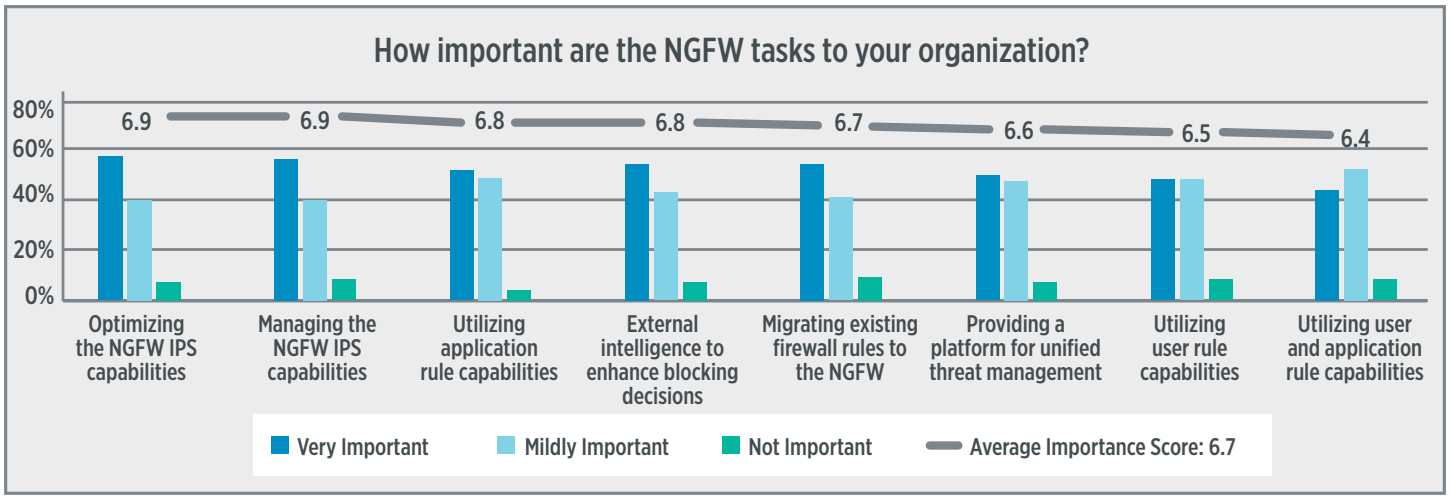

FIGURE 9: 293-300 RESPONDENTS

Next Generation Firewalls (NGFWs)

The adoption of NGFWs is certainly a hot topic in firewall circles right now. We wanted to get a sense of why enterprises were moving toward NGFWs, and how important various capabilities are for them. Respondents were asked to describe whether each of eight capabilities is "very important," "mildly important," or "not important" to their enterprise. We then calculated an "importance score" for each capability. (The formula is described in the introduction section of this report.)

The goals of optimizing and managing NGFW IPS capabilities earned the highest importance scores (6.9 each). Such a strong response highlights the very high value enterprises are placing on the IPS component of NGFWs.

The next-highest importance scores went to utilizing application rule capabilities and using external intelligence to enhance blocking decisions (6.8 each). The former most likely reflects the fact that application-related rules are relatively easy to develop and apply. The latter is an indication of the increasing reliance enterprises are putting on up-to-date threat intelligence to block advanced and targeted attacks.

At the other end of the spectrum, utilizing user rule capabilities and utilizing user and application rule capabilities were given the lowest importance scores (6.5 and 6.4). This probably reflects the challenge involved in pinning down user identities and roles and applying them without error.

Updating IPS Signatures

Updating IPS signatures is another critical (albeit challenging) task. This was confirmed by answers to the question: "How important is it to update your IPS signatures frequently?" An overwhelming two-thirds of the respondents answered "very important." Only 3% answered "not important."

It appears, however, that importance does not always translate to action. Only 37% of the enterprises with NGFWs are updating signatures frequently and using them to block suspicious network traffic. Another 16% use IPS signatures to block traffic, but only updated and customized those signatures once, when their NGFWs were first deployed. An additional 19% have never updated or customized the signatures; they use only the default signatures that came with their NGFWs. A full 30% use their IPS capabilities in detect mode only, to generate alarms but not to block traffic.

If everyone agrees that updating IPS signatures frequently is important, why are so few enterprises doing it? One factor may be difficulty finding reliable signature feeds. The amount of work required to test and deploy new signatures probably also plays a role. However, the obvious gap between importance and current implementation suggests that many enterprises will place a high priority in 2016 on moving toward frequent signature updates.

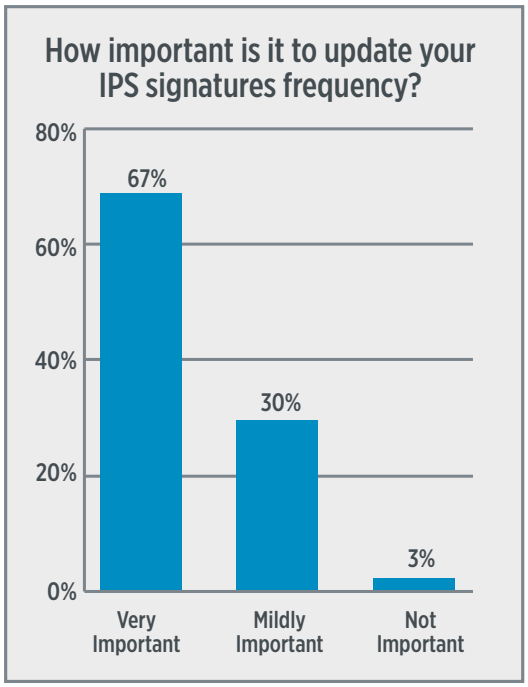

FIGURE 10:
305 RESPONDENTS

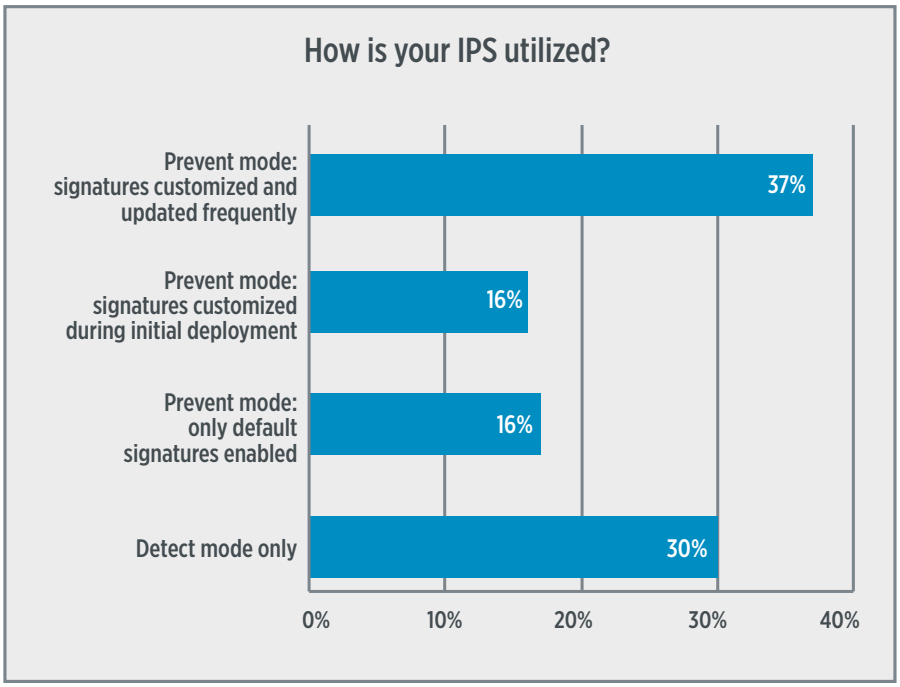

FIGURE 11:
263 RESPONDENTS

IPv6

The move toward IPv6 is widely discussed in the press and by certain vendors. Our survey shows, however, that most enterprises are still taking a wait-and-see approach. Only 20% are using IPv6 on their network currently or are planning to do so within one year. A full 59% have no concrete plans to deploy IPv6.

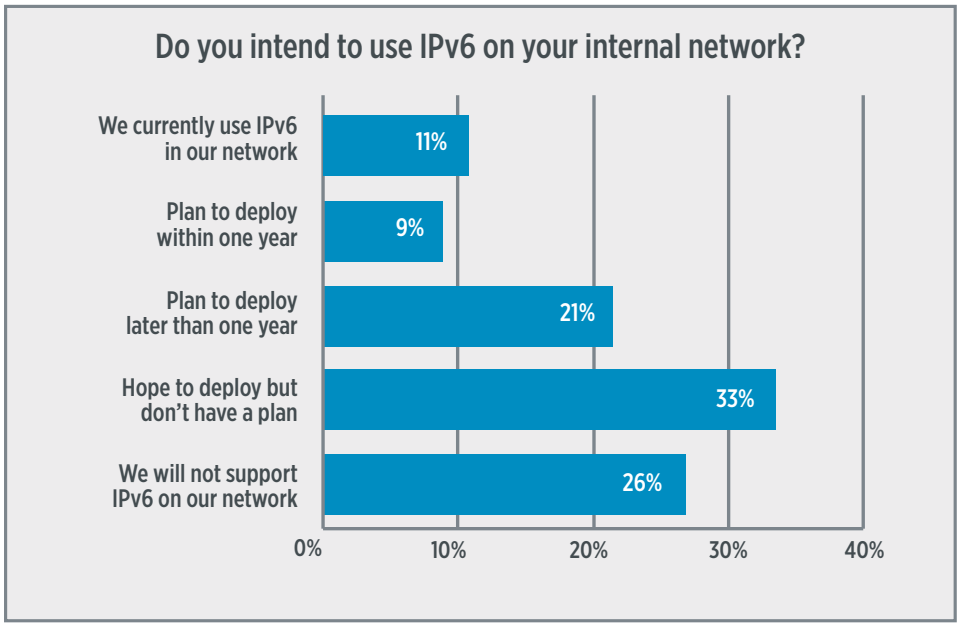

FIGURE 12: 321 RESPONDENTS

Satisfaction

Satisfaction with Firewall Management Capabilities

It is useful to know in what areas current technology and management practices are succeeding and where they have the most room for improvement. The former indicates how organizations are receiving value today, and the latter where it makes sense to look for better tools and processes.

We asked respondents to rate their organization's satisfaction with its ability to perform a variety of firewall management tasks as "very satisfied," "mildly satisfied," or "not satisfied." We then calculated a "Satisfaction Score" for each capability.

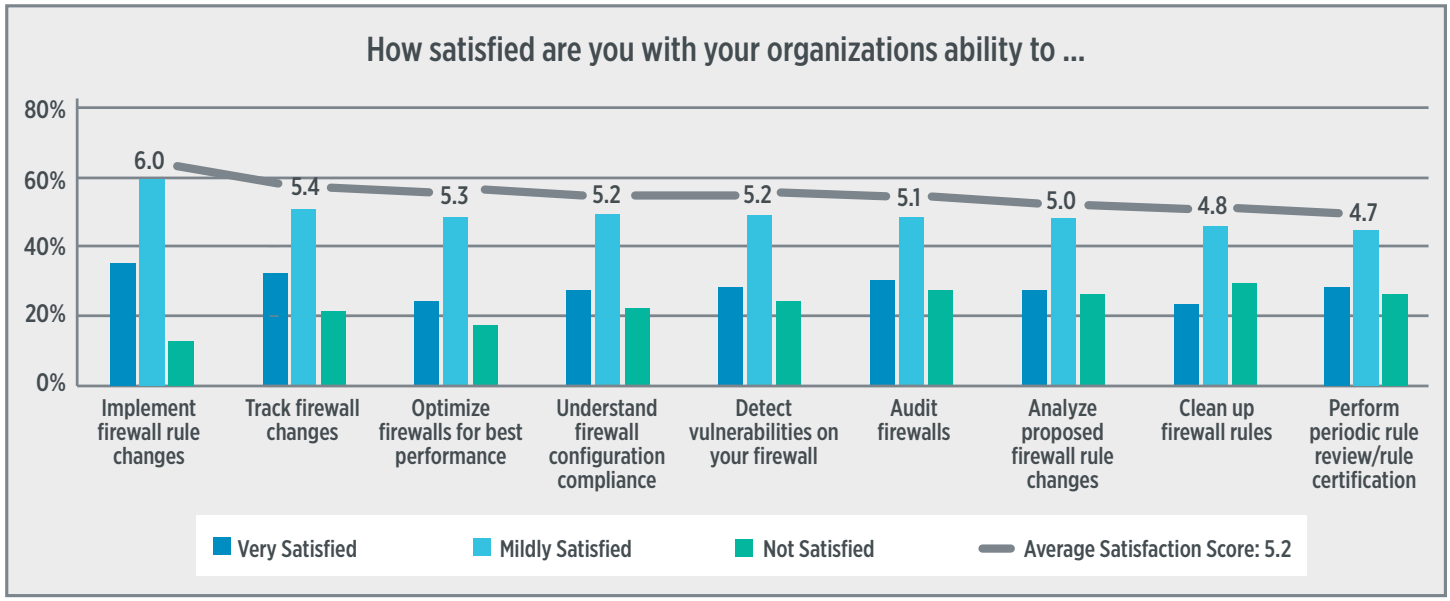

FIGURE 13: 303-319 RESPONDENTS

Satisfaction was highest for implementing firewall rule changes (Satisfaction Score of 6.0). Next on the list were tracking firewall changes and optimizing firewalls for best performance. These are operational tasks where tools and processes have been established for some time.

The lowest levels of satisfaction were reported for auditing firewalls (5.1), analyzing proposed firewall rule changes (5.0), cleaning up firewall rules (4.8), and performing periodic rule reviews and rule certifications (4.7).

These are complex analytical tasks that require comparing existing firewall rules with policies. Some also involve assessing the impact of rules in one set of firewalls on business processes that span multiple systems. The potential value of these tasks is great, but they are difficult to perform with the tools and processes most enterprises have in place today.

Drilling down on this data provides some interesting insights. For example, larger enterprises are generally less satisfied with their firewall management capabilities than smaller enterprises. This likely reflects the fact that larger enterprises have more complex environments, with more firewalls to manage, and more complex business processes.

FIGURE 14

©Skybox Security
www.skyboxsecurity.com

One of the most striking findings from the survey is the fact that satisfaction is dramatically affected by the type of firewall management tools being used. Enterprises that use only third-party firewall management tools or in-house developed tools have much higher satisfaction scores than enterprises using tools supplied by firewall vendors or multiple tools. Enterprises with no firewall management tools have extremely low satisfaction scores.

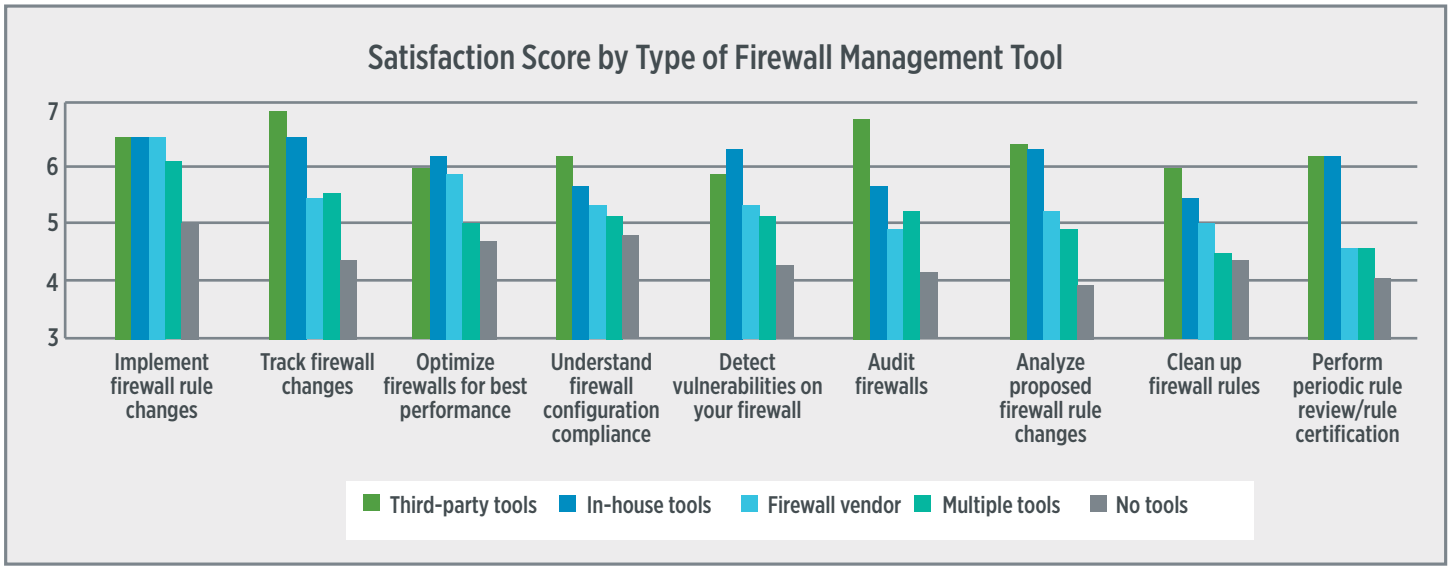

FIGURE 15

©Skybox Security
www.skyboxsecurity.com

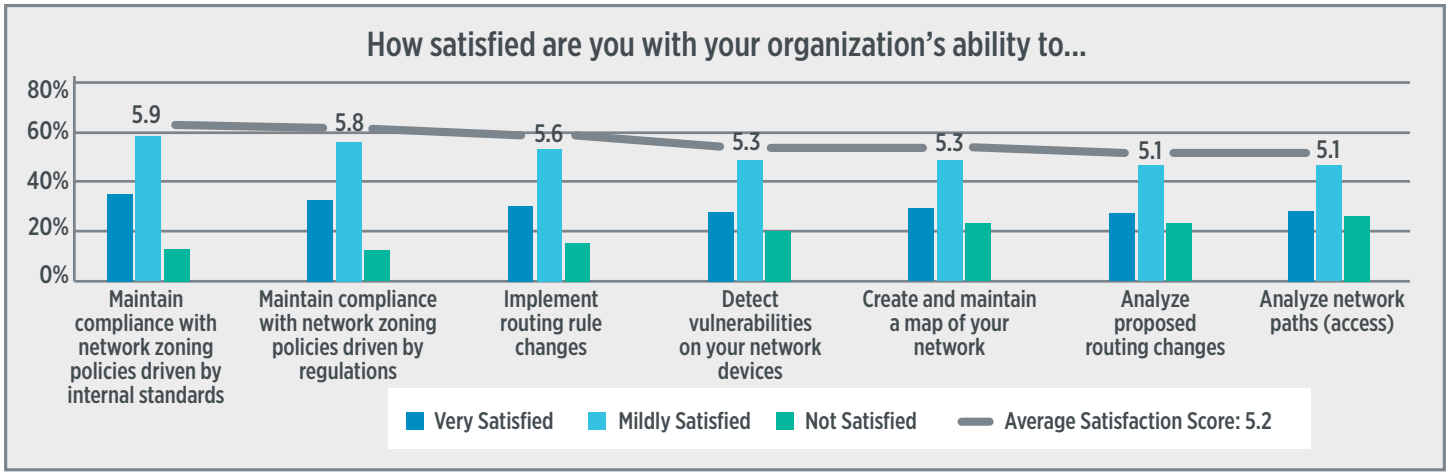

FIGURE 16: 295-304 RESPONDENTS

Satisfaction with Compliance and Analysis Capabilities

The survey also included a series of questions about compliance and analysis capabilities.

Satisfaction was highest for maintaining compliance with network zoning policies driven by both internal standards and external regulations (satisfaction scores of 5.9 and 5.8). Satisfaction was also high for implementing routing rule changes (5.6).

In comparison, satisfaction was much lower for their ability to analyze network access paths (5.1), analyze proposed routing changes (5.1), and create and maintain a map of the network (5.3). These activities can pay very large dividends in terms of improved security and prevention of mistakes that can disrupt business processes. In the near future we expect enterprises to put a lot of emphasis on improving their capabilities in theses areas.

Satisfaction does not vary significantly based on enterprise size or number of firewalls. However, organizations with three or more firewall vendors are much more likely to be dissatisfied than organizations with only one.

As with the firewall management tasks, satisfaction levels are decisively affected by the type of firewall management tools being used. Enterprises that use only third-party firewall management tools and in-house developed tools have the highest satisfaction scores, followed by enterprises using tools supplied by firewall vendors or multiple tools. Enterprises with no firewall management tools trail far behind.

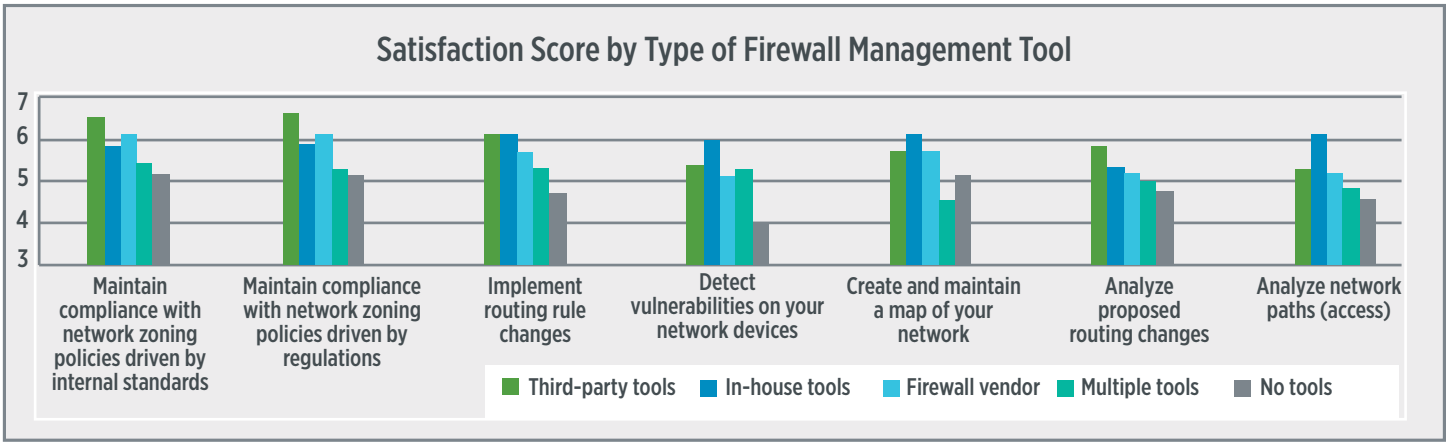

FIGURE 17: SATISFACTION SCORE BY TYPE OF MANAGEMENT TOOL

Conclusions

Firewalls are expanding their role in cyber security, not only blocking malicious web traffic, but playing a critical role in enforcing corporate policies, detecting advanced attacks, and serving as a platform for a wide range of security services.

But with increasing power comes increasing management complexity. To get the most out of firewalls and next-generation firewalls, security teams need to be able to implement, analyze, track, and audit firewall rules; detect vulnerabilities; update IPS signatures; maintain compliance with internal and external standards; utilize user and application-based rules; maintain maps of the network; analyze proposed routing changes; and perform many other challenging tasks. These activities are complicated by the fact that most medium and large enterprises have firewalls from multiple vendors.

This survey provided a number of insights into current practices and satisfaction levels for firewall use and management. Among them:

- Some topics covered widely in the press are, in reality, not high priorities for most enterprises. Few respondents have any immediate plans for outsourcing firewall management, automating the provisioning of firewall rules, using IPv6 on internal networks, or using private cloud-based firewalls.
- Close to 100% of enterprises recognize the high value of updating IPS signatures frequently, but only 37% are doing so. This is likely to be a high priority goal for 2016.
- Most organizations with NGFWs are comfortable using application-based rules, but less so enforcing rules that involve user identities and roles.
- Relatively few enterprises are very satisfied with their firewall management capabilities today. Satisfaction is higher in smaller organizations and lower in organizations with more firewalls and more firewall vendors.
- Satisfaction is relatively higher for established operational tasks like implementing rule changes and optimizing firewalls for performance.
- Satisfaction is relatively low for more analytic tasks such as auditing firewalls, analyzing proposed firewall rule changes, cleaning up firewall rules, performing periodic rule reviews, mapping networks, analyzing proposed routing changes, and analyzing network paths.
- In companies reporting usage of no firewall management tools, or only those supplied by the firewall vendor, satisfaction was lower than the satisfaction of those enterprises using third-party firewall management tools and in-house developed firewall management tools.

Appendix: The Survey Population

This report incorporates data collected from IT professionals at 334 enterprises and government agencies with 500 or more employees. Respondents were only surveyed if they answered "yes" to the question: "Are you knowledgeable about your organization's use of firewalls?"

Of the companies surveyed, 16% had 500 - 999 employees, 28% had 1,000 - 4,999, 14% had 5,000 - 9,999, and 42% had 10,000 or more employees.

The organizations surveyed belong to a wide range of industries, led by financial services and IT services.

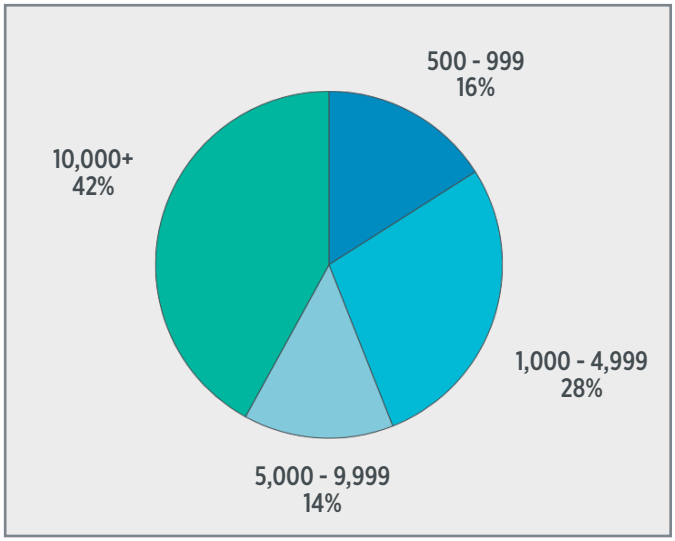

FIGURE 18: RESPONDENT ORGANIZATION SIZE BY EMPLOYEES

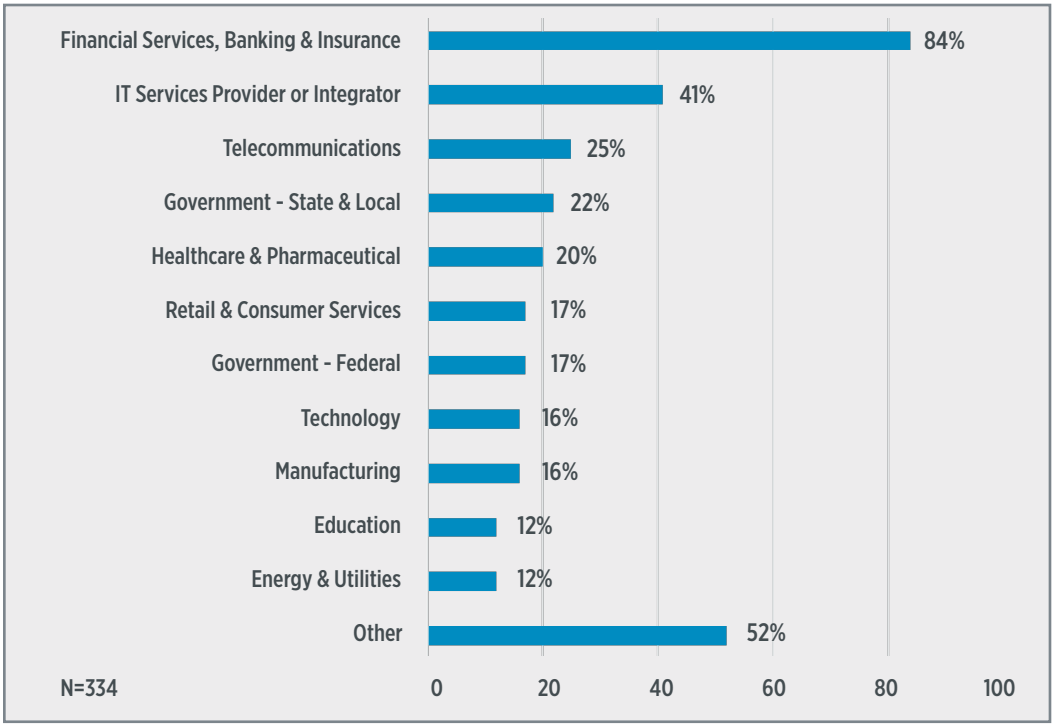

FIGURE 19: RESPONDENT PRIMARY INDUSTRIES

Respondents were drawn from a variety of security, management and specialist roles. They are typically involved in a variety of processes, including vulnerability assessment, incident response, firewall management and risk management. Most respondents have multiple responsibilities. On average they are involved in four of these processes on a daily basis.

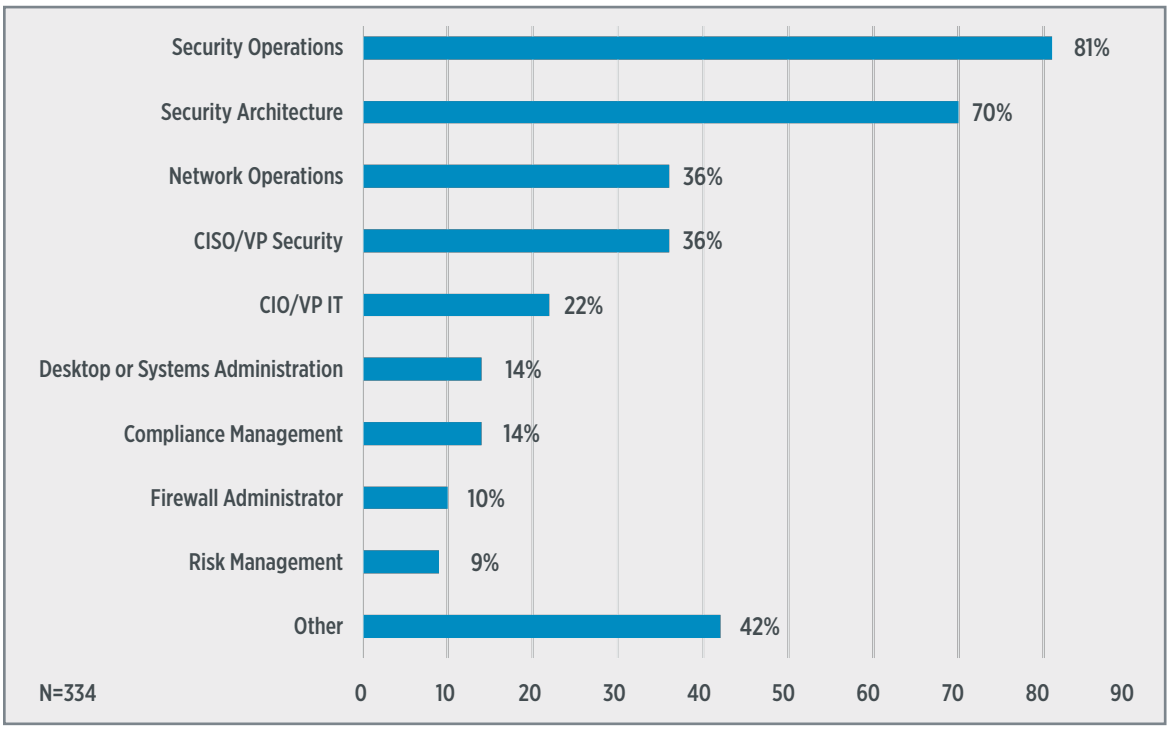

FIGURE 20: RESPONDENT PRIMARY ROLE

©Skybox Security
www.skyboxsecurity.com

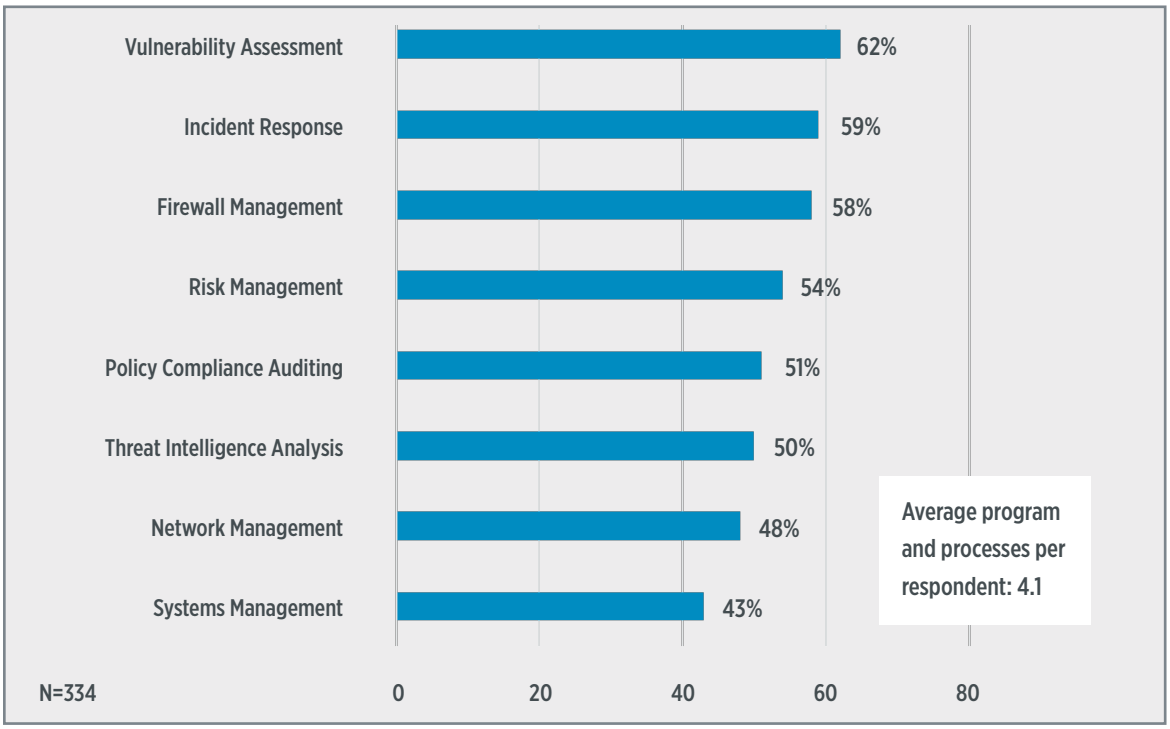

FIGURE 21: RESPONDENT PROGRAMS & PROCESSES INVOLVED WITH DAILY

©Skybox Security
www.skyboxsecurity.com

About Skybox Security

Skybox arms security teams with a powerful set of security management solutions that extract insight from security data silos to give unprecedented visibility of the attack surface, including all Indicators of Exposure (IOEs). With Skybox, security leaders can quickly and accurately prioritize and address vulnerabilities and threat exposures.