SURVEY REPORT

Understanding Security Processes and the Need to Automate

An Osterman Research Survey Report

Published August 2018

Sponsored by

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

Overview

This report presents the results of an in-depth Osterman Research primary research effort focused on understanding current security processes and how organizations are working to improve and automate them. The research was conducted in the United States, EMEA (the United Kingdom, France and Germany), and APAC (China, Japan and Singapore).

KEY TAKEAWAYS FROM THE RESEARCH

- There are some important deficiencies that organizations must address in the context of their firewall and security management, most notably in the areas of understanding existing vulnerabilities of the devices on corporate networks and the business impacts of security changes.

- The incident response process is a major consumer of security staff members' time and energy, but other issues are also time-consuming, including compliance management and making changes to the security infrastructure.

- Most organizations admit that they need to make major improvements in how they manage security and policy. The biggest improvements are needed in how organizations decommission applications, and how they can prune firewall rules so that rule sets do not become bloated.

- US-based staff members that are responsible for firewall and security policy management can support the largest number of employees, while those in APAC support the smallest number.'

- Automation for workflows and processes involved in the management of rules and security policy are most common in APAC, least common in EMEA. Many of these processes are already automated, but there is a long way to go before most have been fully automated.

- The key driver for automation is the desire to cut costs, although other drivers are also important, such as dealing with the challenges of large and complex networks.

- The migration to cloud applications and workflows is having a significant impact on the automation of security policy changes, most notably in APAC. The vast majority of organizations are working on initiatives focused on security automation to support cloud environments.

ABOUT THE SURVEY

The research for this report was conducted in June 2018 with a total of 465 respondents (162 in the United States, 153 in EMEA and 150 in APAC). A combination of online surveys and computer-assisted telephone interviewing were used. In order to qualify for participation in the survey, respondents had to meet the following qualifications:

- They had to be knowledgeable about security policy management and related issues in their organization.
- Their organization had to have a minimum of 1,000 employees.

The organizations surveyed had the following average number of employees:

- United States: 19,290
- EMEA: 4,314
- APAC: 10,102

Survey Findings

UNDERSTANDING OF KEY ISSUES IS LACKING

One of the more important takeaways from the research is that there are some important deficiencies that organizations must address in the context of their firewall and security management. For example, as shown in Figure Q3, we found that a large proportion of organizations do not have a solid understanding of why each firewall rule exists, a problem most acutely seen among the EMEA-based organizations we surveyed. There are also significant deficiencies in understanding how security policy impacts both inbound and outbound network traffic, as well as in understanding the business impacts of security changes.

Interestingly, one of the most glaring deficiencies that we discovered – and a problem that most seriously impacts organizations in the United States and EMEA – is the relative lack of understanding about vulnerabilities on network devices. We found that most organizations in the United States and EMEA, and fewer than three in five organizations in APAC, have

what they feel is a good understanding of these vulnerabilities.

Figure Q3
Extent to Which Organizations Understand Key Firewall and Security Policy Issues

		USA	EMEA	APAC
Why each firewall rule exists	Minimal understanding	9%	3%	3%
	Some understanding	28%	58%	43%
	Good understanding	62%	39%	54%
How security policy impacts inbound and outbound network traffic	Minimal understanding	7%	8%	5%
	Some understanding	36%	50%	43%
	Good understanding	57%	42%	53%
Understanding the business impacts of security changes	Minimal understanding	10%	5%	3%
	Some understanding	39%	58%	36%
	Good understanding	51%	37%	61%
Vulnerabilities on network devices	Minimal understanding	9%	6%	3%
	Some understanding	44%	57%	39%
	Good understanding	47%	37%	58%

Source: Osterman Research, Inc.

INCIDENT RESPONSE IS A MAJOR TIME SINK

Respondents were asked to rate on a scale of 1 (minimal amount of time) to 7 (a great deal of time) where they are spending time and energy in security policy management. As shown in Figure Q14, there are a number of areas in which security professionals are spending time and this varies substantially by the region in question. For example:

- Security professionals in the United States are particularly focused on incident response activities focused on triage and prioritization, as well as compliance management.
- EMEA-based security professionals are focused heavily on dealing with firewall configurations, with nearly one-half of respondents indicating that they are spending a "substantial" or "a great deal" of time and energy on this activity.
- Respondents in APAC are focused most heavily on compliance management and security changes.

Figure Q14
Areas in Which Organizations are Spending the Most Time and Energy in Security Policy Management
Percentage responding "a substantial amount" or "a great deal" of time

	USA	EMEA	APAC
Incident response - triage/prioritization	31%	31%	39%
Compliance management	30%	29%	49%
Security changes	28%	28%	43%
Firewall configurations	27%	47%	38%
Business application connectivity requirements	27%	30%	39%
Firewall audits	26%	31%	37%
Analysis for decision support	23%	23%	43%
The process of decommissioning applications	21%	24%	34%
Rule optimization and cleanup	20%	29%	41%
Access troubleshooting	20%	26%	44%
Out-of-process changes	18%	35%	40%

Source: Osterman Research, Inc.

Overall, when evaluating the 11 activities shown in Figure Q14, we found that respondents in the United States reported investing the least amount of time – the average response of "substantial" or "a great deal" of time and energy was 24.6 percent. This is in significant contrast to respondents in EMEA, which reported an average across the 11 activities of 30.4 percent, and in APAC that averaged 40.7 percent. This indicates that the infrastructure in place within US-based organizations may be somewhat more efficient than the corresponding infrastructure in EMEA or APAC. It also tracks with the fact that US-based security staff members focused on firewall and security policy management can support a much higher number of employees, a shown later in this report in Figure Q16.

SIGNIFICANT IMPROVEMENTS ARE NEEDED IN SECURITY AND POLICY MANAGEMENT

As shown in Figure Q4, organizational decision makers believe there is significant room for improvement in the way that they manage things like security changes, out-of-process changes, firewall configurations, and pruning of firewall rules. Organization are particularly poor at the process of decommissioning applications with only 28 percent of US-based organizations reporting that they do this "well", and fewer than one-half of EMEA- and APAC-based organizations reporting that they perform these activities well.

Figure Q4
How Well Do Organizations Manage Various Security and Policy Requirements

		USA	EMEA	APAC
Security changes	Poorly	7%	5%	3%
	Moderately	46%	65%	40%
	Well	47%	30%	57%
Firewall configurations	Poorly	9%	5%	3%
	Moderately	34%	52%	35%
	Well	57%	44%	63%
Out-of-process changes	Poorly	7%	7%	5%
	Moderately	56%	64%	51%
	Well	36%	29%	44%
Compliance management	Poorly	10%	5%	2%
	Moderately	48%	69%	41%
	Well	42%	26%	57%
Business application connectivity requirements	Poorly	6%	3%	1%
	Moderately	58%	66%	45%
	Well	36%	31%	53%
The process of decommissioning applications	Poorly	12%	9%	3%
	Moderately	60%	58%	51%
	Well	28%	33%	45%
Firewall audits	Poorly	12%	7%	2%
	Moderately	48%	66%	47%
	Well	40%	27%	51%
Pruning firewall rules so that rule sets do not become bloated	Poorly	10%	5%	4%
	Moderately	57%	73%	44%
	Well	33%	22%	52%

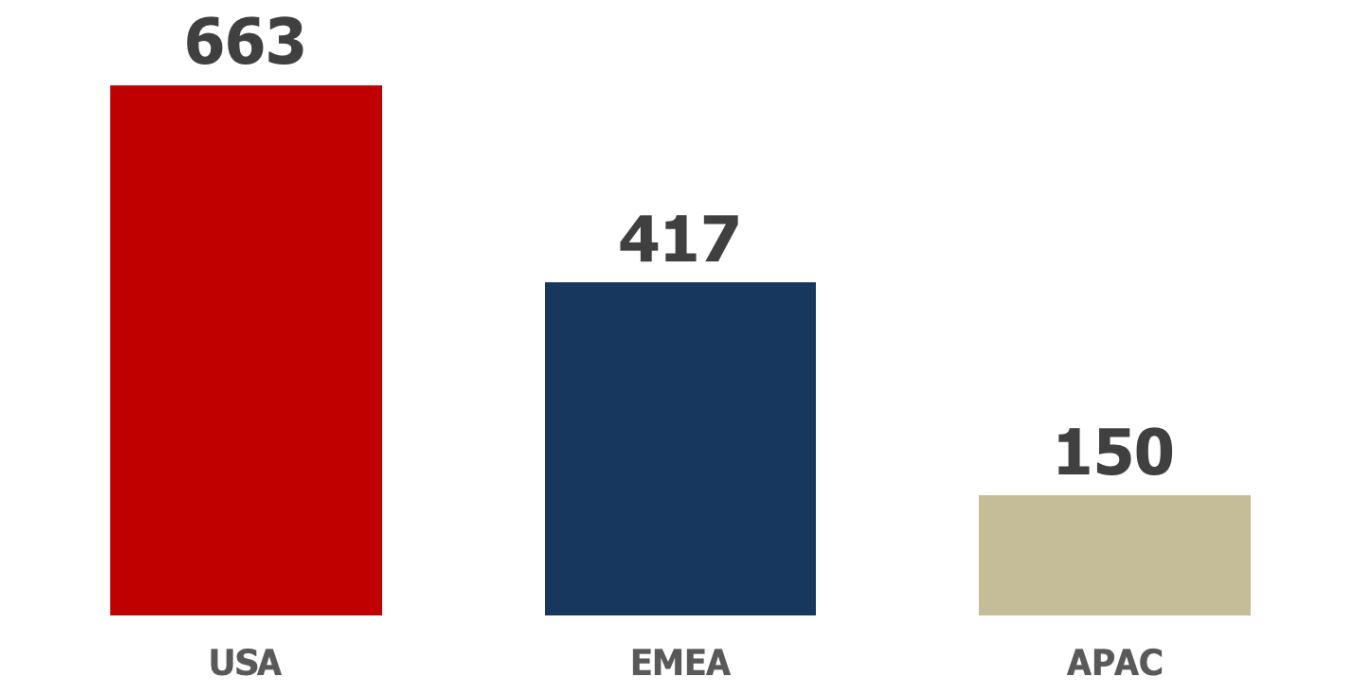
Source: Osterman Research, Inc.

An examination of the data in Figure Q4 reveals that the average of the "managing well" responses is the lowest among EMEA-based organizations, with only 30 percent reporting they are managing these activities in a satisfactory manner. Organizations in the United States come in next at 40 percent managing these activities well, with 53 percent of organizations in APAC reporting this level of satisfaction with their efforts. The better than average response for APAC-based organizations tracks with the number of security-focused staff members that are available to manage these activities, but is likely not explained completely by staffing availability issues.

THERE ARE SIGNIFICANT DIFFERENCES IN STAFFING LEVELS FOR FIREWALL AND SECURITY POLICY MANAGEMENT

One of the more significant differences we found in the research is the difference in the number of employees that are supported per full-time equivalent (FTE) staff member focused on firewall and security policy management in each of the regions. As shown in Figure Q16, the number of employees per FTE staff member in US-based organizations is 663, but this drops to 417 for EMEA-based organizations and only 150 in APAC. In some cases, this might be explained by the size of the organizations surveyed, but the number of employees per FTE staff member does not track with the number of employees per organization: for example, the organizations we surveyed in APAC are, on average, larger than their EMEA-based counterparts, but their staff members support fewer employees.

Figure Q16
Number of Employees Supported per FTE Staff Member Focused on Firewall and Security Policy Management



Source: Osterman Research, Inc.

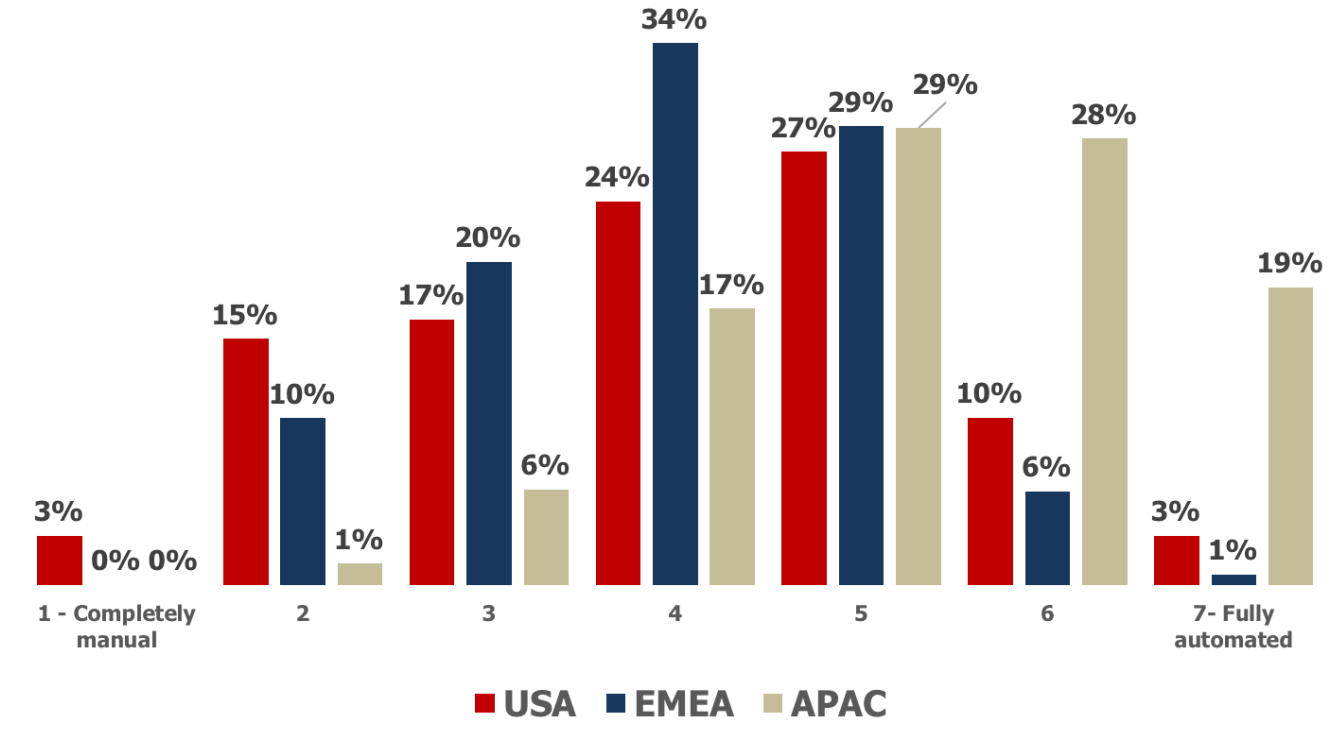
One explanation for the much smaller number of employees supported by organizations, at least in the APAC region, is that salaries for security professionals are much lower and so organizations can afford more staffing to make up for any deficiencies they might have in the technology stack they have deployed. For example, an application manager in Shanghai has an annual salary of roughly US$3,200 to US$5,400[1] compared to an equivalent position in St. Louis, Missouri that has an annual salary of more than US$103,000[2].

AUTOMATION IS MORE WIDELY DEPLOYED IN APAC

Interestingly, and somewhat in contrast to the data showing that APAC-based organizations employ more labor to address security and policy management, is the data in Figure Q5 that shows a greater degree of automation among APAC-based organizations. We found that 47 percent of the APAC-based organizations we surveyed are nearly or fully automated for their workflows and processes in managing rules and security policy compared to only 13 percent of US-based organizations and seven percent of organizations in EMEA.

[1] http://www.morganmckinley.com.cn/en/article/2018-it-information-technology-shanghai-salary-survey-guide
[2] https://www.glassdoor.com/Salaries/st-louis-application-manager-salary-SRCH_IL.0,8_IM823_KO9,28.htm

Figure Q5
Extent to Which Organizations Have Deployed Automation in the Workflows and Processes for Management of Rules and Security Policy



Source: Osterman Research, Inc.

MANY PROCESSES ARE ALREADY AUTOMATED

Further supporting the data shown in Figure Q5 is the more detailed data about the automation of various processes shown in Figure Q6. Among the most heavily automated processes in US-based organizations are data collection and traffic flow analysis/path analysis, while among organizations in EMEA the most automated processes are data collection and automating the collection/gathering of data to understand rules/configurations on the network. In APAC, the most automated processes are policy and compliance management to determine where there are rule violations, network change management/risk analysis and data collection. Overall, across all of the activities shown in the table below, US-based organizations report they are nearly or fully automated for 24 percent of the processes compared to only 17 percent in EMEA and 41 percent in APAC.

Figure Q6
Extent to Which Organizations Have Automated Various Processes

		USA	EMEA	APAC
Automating the collection/gathering of data to understand rules/configurations on the network	Manual	17%	10%	2%
	Hybrid	59%	62%	51%
	Automatic	23%	27%	47%
Building and validating the network model (i.e., the collection, normalization and centralization of data)	Manual	20%	19%	3%
	Hybrid	57%	65%	50%
	Automatic	23%	16%	47%
Rule optimization and cleanup	Manual	26%	17%	5%
	Hybrid	52%	68%	50%
	Automatic	22%	15%	45%
Policy and compliance management (to determine where there are rule violations)	Manual	23%	27%	5%
	Hybrid	54%	60%	41%
	Automatic	23%	13%	53%
Change management (e.g., path analysis, risk analysis, policy push, reconciliation, etc.)	Manual	20%	16%	5%
	Hybrid	54%	71%	53%
	Automatic	25%	13%	43%
Rule lifecycle management	Manual	25%	18%	4%
	Hybrid	54%	66%	54%
	Automatic	21%	16%	42%
Provisioning of firewall changes	Manual	21%	14%	5%
	Hybrid	54%	71%	51%
	Automatic	25%	16%	45%
Auditing and report	Manual	23%	25%	7%
	Hybrid	54%	61%	54%
	Automatic	24%	14%	39%
Policy automation	Manual	23%	24%	3%
	Hybrid	59%	63%	55%
	Automatic	18%	13%	41%
Data collection	Manual	17%	11%	2%
	Hybrid	44%	59%	47%
	Automatic	39%	30%	51%
Traffic flow analysis/path analysis	Manual	14%	11%	3%
	Hybrid	59%	67%	48%
	Automatic	28%	22%	49%
Network change management/risk analysis	Manual	22%	19%	3%
	Hybrid	56%	68%	46%
	Automatic	22%	13%	51%
Compliance (i.e., identifying and resolving policy violations, both internal and external regulations)	Manual	23%	25%	7%
	Hybrid	57%	64%	53%
	Automatic	20%	11%	41%

Source: Osterman Research, Inc.

AUTOMATING WORKFLOW IS PRIMARILY FOCUSED ON CUTTING COSTS

Our research found that the primary driver for automating workflows for security and policy management, at least in the United States and EMEA, is to cut the costs associated with these activities. As shown in Figure Q7, this is particularly true in EMEA, where more than three in five organizations reported that cost-cutting is a reason for deploying automation. By contrast, organizations in APAC reported that the key drivers for the deployment of automation are centered around dealing with the challenges of managing a large and complex network and to improve the speed of security provisioning. To be sure, cost-cutting is also an important driver among APAC-based organizations, but it was not the primary driver as in the other two regions. Here again, the cost of labor in APAC, being so much lower than in the other two regions, may explain at least part of

the lower importance assigned to cost-cutting as a driver for automating workflows.

Figure Q7
Reasons That Organizations are Automating Workflows

Text	USA	EMEA	APAC
We are trying to cut costs	43%	61%	35%
Because of the challenges in managing a network that has the size and complexity of ours	42%	38%	43%
We want to be able to move skilled staff off of routine/mundane security activities and on to higher value/skill security tasks	40%	22%	32%
To improve the speed of security provisioning	39%	22%	41%
We are trying to reduce our security exposure	35%	27%	29%
To improve the speed of auditing	34%	22%	23%
We lack the internal staff to adequately address our firewall and security policy management workload	32%	26%	15%
To keep up with the pace of changes in our environment	32%	24%	21%
To improve the accuracy of reporting	29%	30%	26%
To better align our security, application and operations activities	29%	16%	28%
Because of the challenges associated with unifying policy across complex environments	26%	18%	26%
To remove firewall rules that are no longer required	25%	17%	13%
To standardize reporting and improve delivery	23%	17%	14%
To produce quick, ad hoc queries	18%	28%	5%
To have a single pane of glass view into policy	17%	12%	17%
To better understand application connectivity requirements	16%	14%	18%
To reduce application outages arising from firewall misconfigurations	16%	18%	22%
We have had one or more major security incidents that prompted us to introduce automation into our processes	15%	20%	5%
To decommission applications in a more secure manner	13%	15%	17%

Source: Osterman Research, Inc.

ORGANIZATIONS ARE EAGER TO AUTOMATE THEIR PROCESSES

One of the questions we asked in the survey is the extent to which organizations are eager to automate various processes in the context of security and policy management, whether or not they have already done so. When asked to rate their desire for automation of various processes on a scale of 1 (we do not want to automate) to 7 (this is a high priority for automation), we found that the leading areas for automation in US-based organizations focused on automating the collection/gathering of data to understand rules/configurations on the network and rule optimization/cleanup, as shown in Figure Q8. Among organizations in EMEA, the primary area in which automation is desired is data collection (which is the least automated activity among the three regions, as shown in Figure Q6). In APAC, the areas in which organizations are most eager to automate are data collection and network change management/risk analysis. The average of the "priority" or "high priority" responses for automation in APAC were the highest at 51 percent, followed by the United States at 36 percent and EMEA at 24 percent.

Figure Q8
Eagerness With Which Organizations Desire to Automate Various Processes

	Degree of Automation Desired	USA	EMEA	APAC
Automating the collection/gathering of data to understand rules/configurations on the network	None/little	12%	8%	3%
	Some	44%	56%	45%
	Lots	44%	35%	52%
Rule optimization and cleanup	None/little	12%	9%	4%
	Some	48%	60%	49%
	Lots	40%	31%	47%
Policy and compliance management (to determine where there are rule violations)	None/little	12%	15%	4%
	Some	56%	67%	49%
	Lots	31%	18%	47%
Change management (e.g., path analysis, risk analysis, policy push, reconciliation, etc.)	None/little	14%	10%	3%
	Some	54%	69%	45%
	Lots	33%	20%	52%
Rule lifecycle management	None/little	11%	11%	1%
	Some	60%	71%	52%
	Lots	29%	18%	47%
Provisioning of firewall changes	None/little	13%	10%	3%
	Some	58%	65%	51%
	Lots	29%	25%	47%
Auditing and report	None/little	14%	16%	4%
	Some	51%	67%	47%
	Lots	35%	16%	49%
Policy automation	None/little	16%	17%	7%
	Some	54%	63%	45%
	Lots	30%	20%	49%
Data collection	None/little	10%	7%	1%
	Some	41%	52%	41%
	Lots	49%	42%	58%
Traffic flow analysis/path analysis	None/little	11%	10%	3%
	Some	43%	66%	43%
	Lots	46%	24%	53%
Network change management/risk analysis	None/little	14%	10%	3%
	Some	52%	66%	39%
	Lots	34%	24%	57%
Compliance (i.e., identifying and resolving policy violations, both internal and external regulations)	None/little	16%	12%	3%
	Some	54%	69%	45%
	Lots	30%	20%	52%

Source: Osterman Research, Inc.

HOW DO ORGANIZATIONS DETERMINE IF AUTOMATION IS SUCCESSFUL?

As shown in Figure Q9, the primary means of determining the benefits of automation and if automation efforts are successful among US-based organizations is the reduction in the number of issues that require human involvement, also the most important measurement for organizations in APAC. While this was very closely the second most important driver among organizations in EMEA, the key way that organizations in that region determine if their automation efforts are successful is by measuring the number of incidents that impact the network, endpoints, etc. It's important to note that the measurements in Figure Q9 are not mutually exclusive, since a reduced number of incidents, for example, will typically lead to less human involvement, either in initial evaluation/triage or escalation of more complex incidents.

Figure Q9
Means by Which Organizations Measure the Benefits of Automation and How They Determine if Automation Efforts are Successful

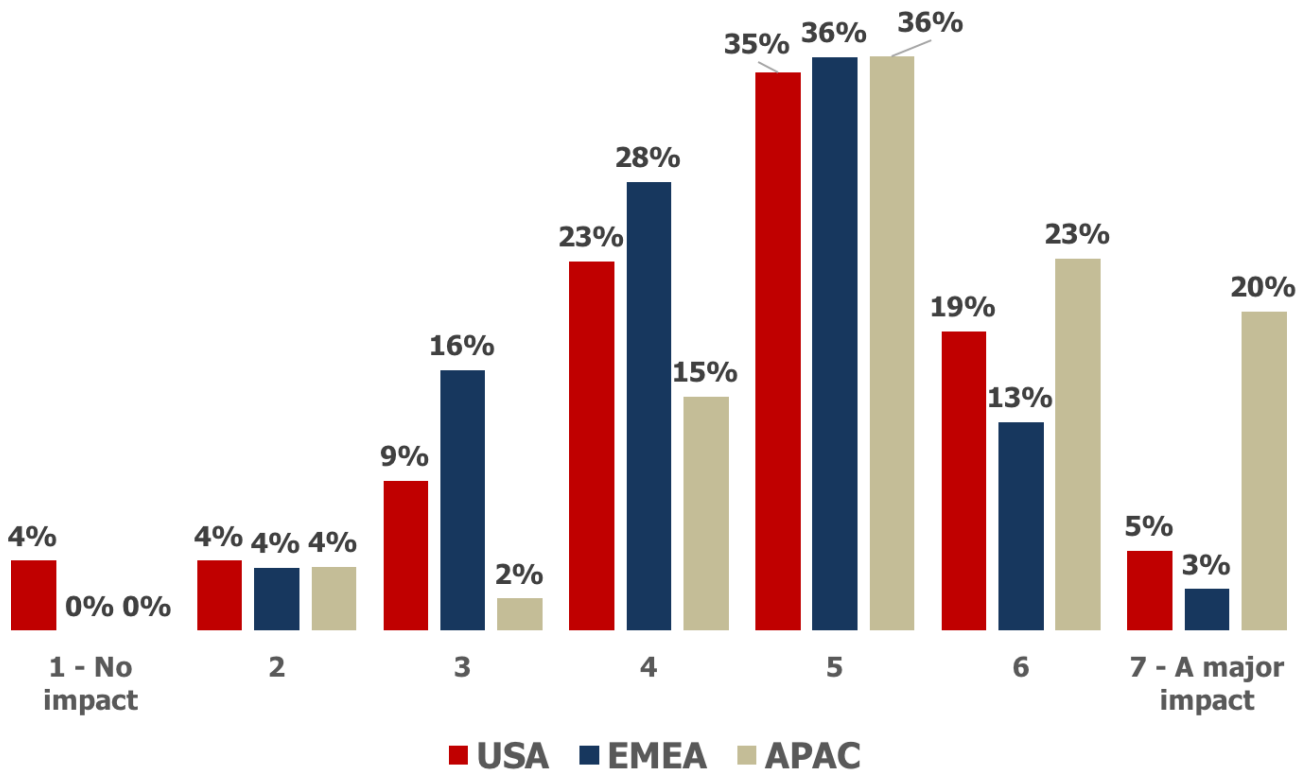
	USA	EMEA	APAC
Reduced number of issues that require human involvement	69%	55%	59%
Reduced number of security incidents impact the network, endpoints, etc.	67%	56%	49%
Reduced labor requirements for security management	57%	49%	67%

Source: Osterman Research, Inc.

THE CLOUD IS HAVING A SIGNIFICANT IMPACT

As shown in Figure Q12, the cloud is having a significant impact on the automation of security policy changes as more applications and workflows are migrated to the cloud. The impact of the migration of key applications and workflows to the cloud is most pronounced among the organizations we surveyed in APAC, where 43 percent of organizations reported it is having a significant or major impact on the automation of security policy changes. Cloud migration is having an important, but lesser, impact in the other two regions, as well: just under one-quarter of US-based organizations report a significant or major impact, while only one in six report this level of impact in EMEA.

Figure Q12
Extent to Which Migration to the Cloud is Having an Impact on Automation Security Policy Changes

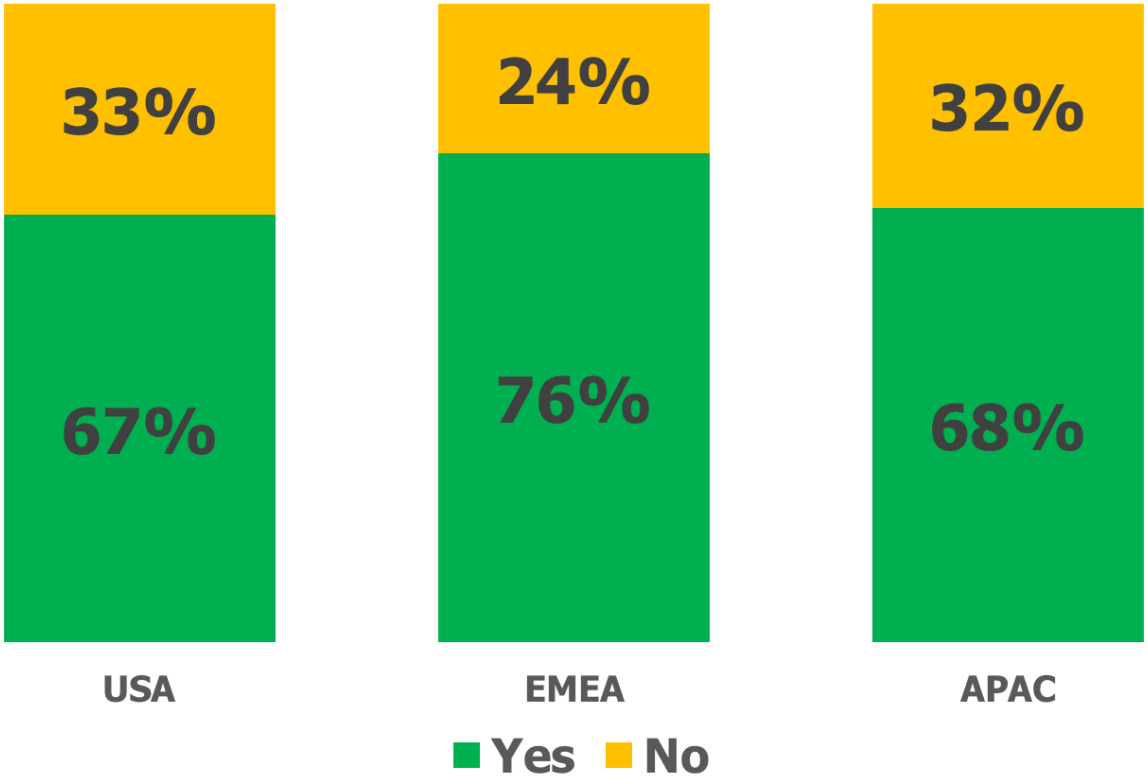


Source: Osterman Research, Inc.

MOST ARE WORKING TOWARD AUTOMATION IN CLOUD ENVIRONMENTS

Our research found that the vast majority of organizations in all three regions have already implemented security automation initiatives to support cloud environments, or they are working on these initiatives, as shown in Figure Q13. Security automation initiatives are being pursued the most aggressively among the organizations we surveyed in EMEA, and less so in both the United States and APAC.

Figure Q13
"Do you have, or are you working on, security automation initiatives supporting cloud environments?"

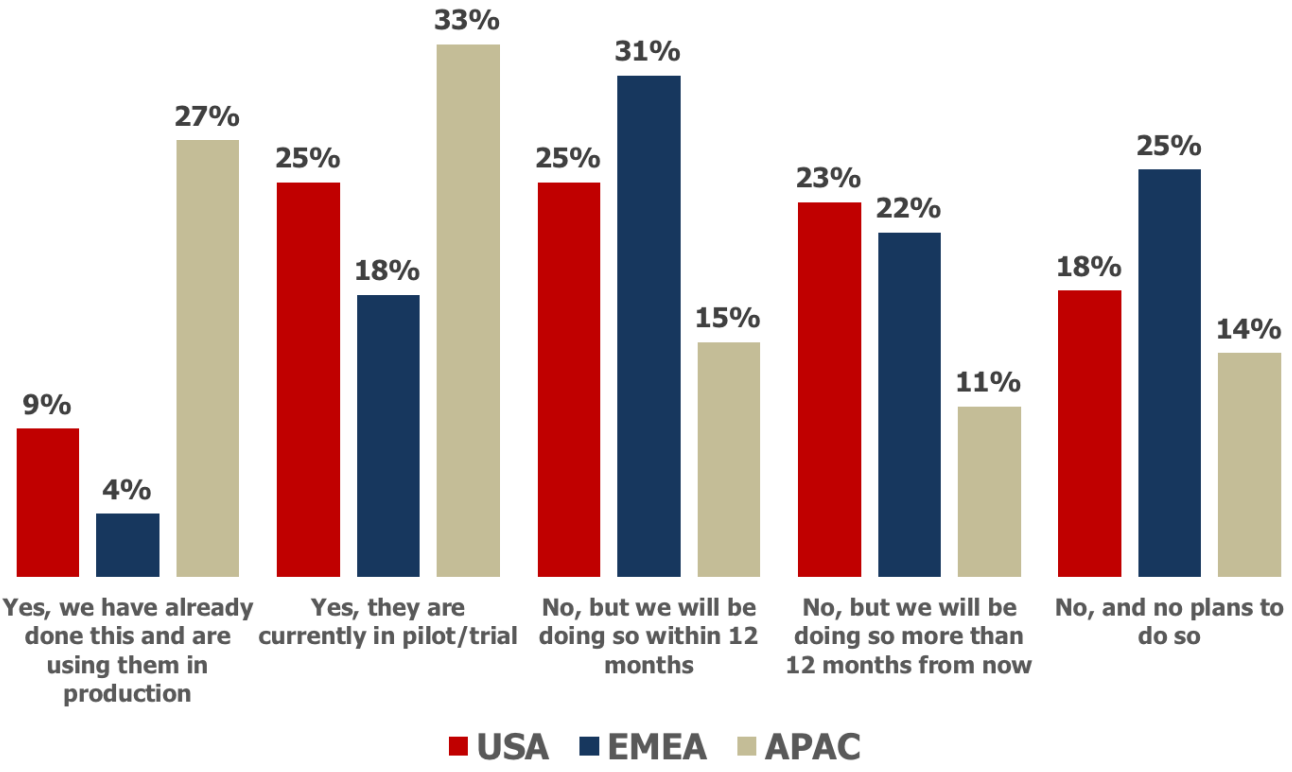


Source: Osterman Research, Inc.

AI/ML FIGURE PROMINENTLY IN SECURITY AUTOMATION PLANNING

The use of Artificial Intelligence/Machine Learning (AI/ML) is key for many organizations. As shown in Figure Q15, 27 percent of organizations in APAC have already implemented AI/ML in their production systems – nine percent of organizations in the United States and four percent of those in EMEA have done likewise. However, significantly more organizations are currently in pilot or trial of AI/ML solutions in all three regions and many are planning to do within the next 12 months.

Figure Q15
Extent to Which Organizations are Researching or Exploring Artificial Intelligence/Machine Learning Technologies to Include in Security Automation Plans



Source: Osterman Research, Inc.

Summary and Conclusions

Most organizations have room to grow in their understanding of key security and security automation processes, such as why firewall rules exist, where vulnerabilities exist among their various network devices, and how security policies impact network traffic. That said, despite the significant improvements that are needed, most organizations are working aggressively toward implementing automation into their firewall and security management processes and are pursuing the use of AI/ML technologies to improve understanding and cut the costs of managing their security infrastructure.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox®Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.