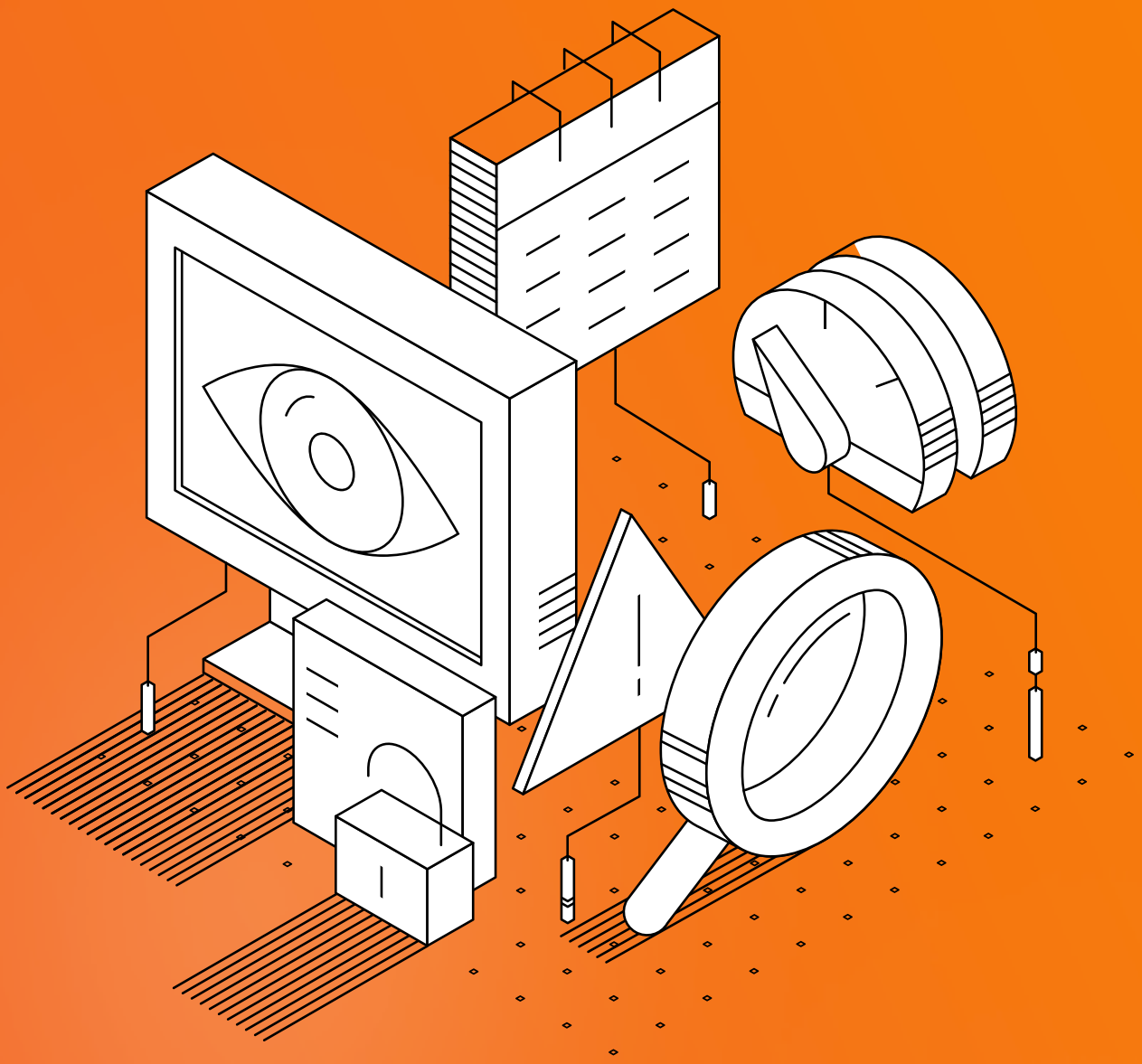
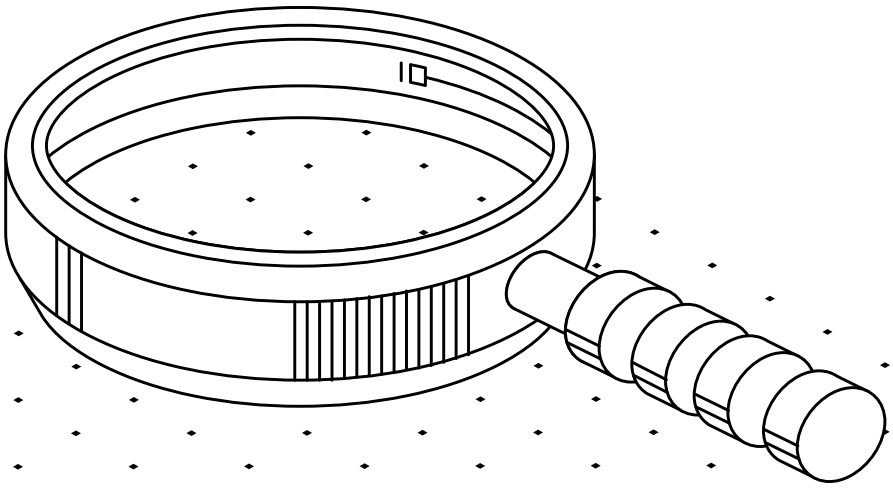


FIREMON

The 2017 State of the Firewall

TABLE OF CONTENTS



Executive Summary

FireMon is proud to present its 3rd Annual State of the Firewall Report based on 437 survey responses collected between November 16, 2016 and December 6, 2016. Respondents included IT security practitioners representing a range of professional roles, organization sizes and industry verticals. Survey participants were asked 26 questions about their current firewall infrastructure and management challenges as well as questions about adoption and impact of emerging technologies such as SDN, cloud, microsegmentation and Internet of Things (IoT).

This year's report demonstrates the significance of firewalls to organizations' security strategies, showing that nine out of ten practitioners believe that the firewall will remain critical over the next five years.

Nowadays, corporate network infrastructure likely consists of multiple vendor firewalls, and two-thirds of survey respondents reported they have ten or more firewalls. As such, firewall management is not without its challenges. Complexity reigns as a top concern when it comes to firewalls, with rule optimization, managing multiple types of firewalls and compliance and audit readiness as the next biggest concerns.

In addition, FireMon gauged opinions about the impact of cloud, Software Defined Networking (SDN) and the complications microsegmentation and IoT will add to the complexity of IT environments. It found that for more than one-third of respondents, responsibility for cloud security falls outside of security operations, which adds an extra layer of complexity to security management. Microsegmentation that breaks the data center in logical elements and manages them with high level IT security policies and IoT were concerns for 41% of the organizations surveyed.

Regardless of what the networking environment looks like, firewalls support it all. And for a majority of organizations, at least a quarter of their security budgets are dedicated to them, showing that the firewall is here to stay.

Three trends are explored in depth in this report: the complexity of firewall management, the impact of emerging technologies such as SDN, cloud, microsegmentation and Internet of Things (IoT); and the role of firewalls in supporting varied network environments.

REPORT HIGHLIGHTS

9 of 10

IT PRACTITIONERS BELIEVE THE FIREWALL WILL REMAIN CRITICAL OVER THE NEXT 5 YEARS

COMPLEXITY

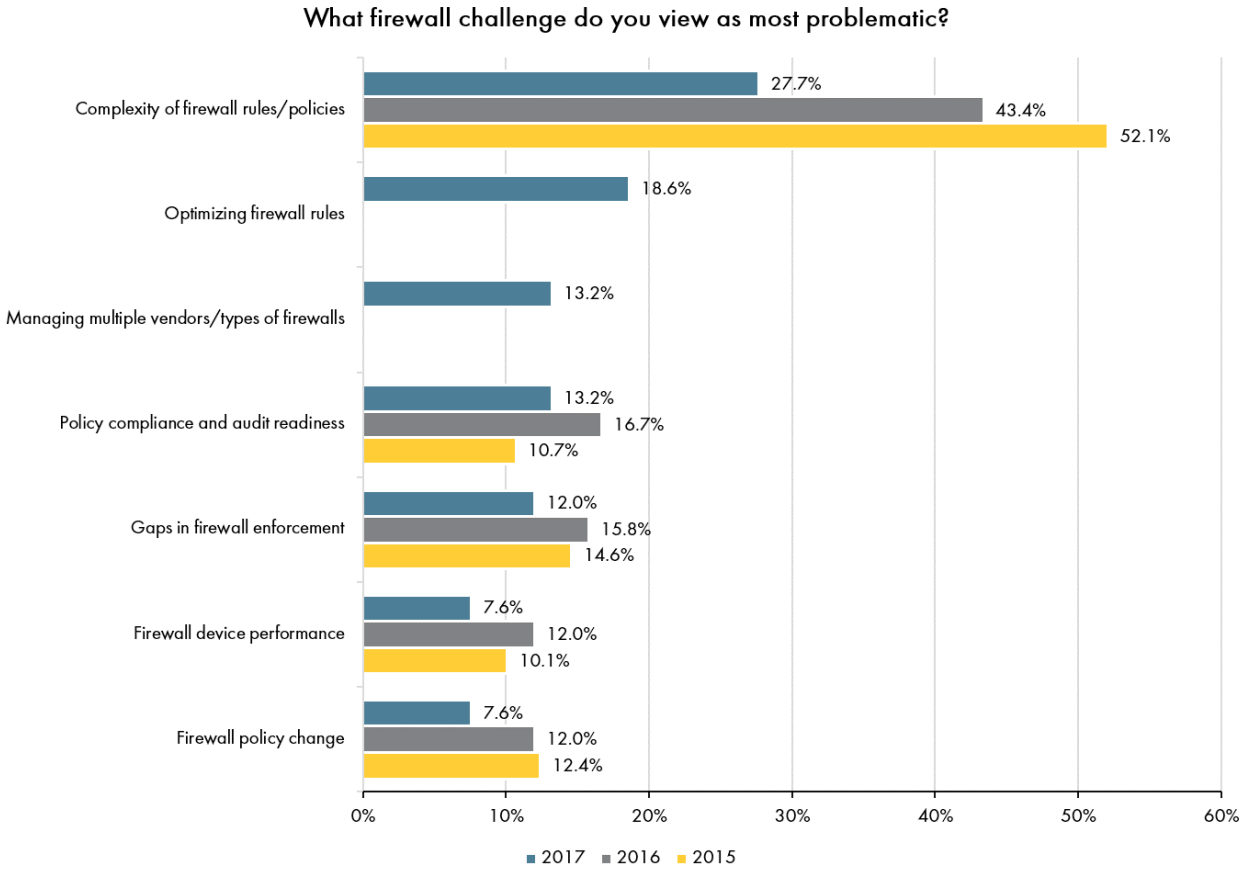
IS THE #1 RANKED CHALLENGE FOR FIREWALL MANAGEMENT

90%

HAVE ADOPTED A CLOUD SOLUTION

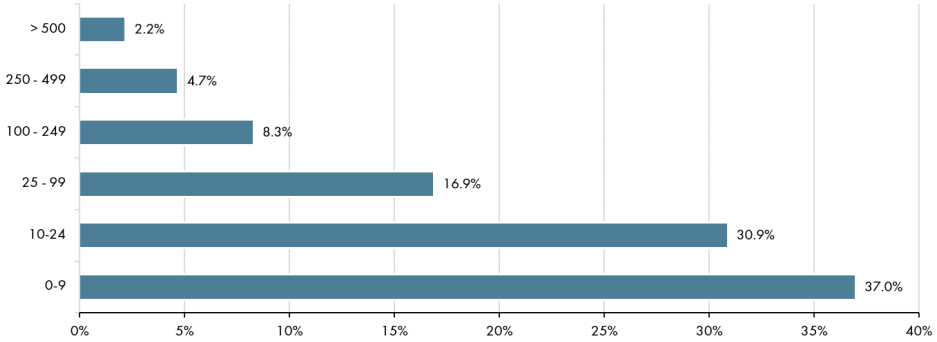
Complexity reigns as top challenge.

For the third year in a row, survey respondents indicated that complexity is the top challenge for managing firewalls. Rounding out the Top 3 are rule optimization and managing multiple types of firewalls, which could in their own way contribute to or result from network complexity.

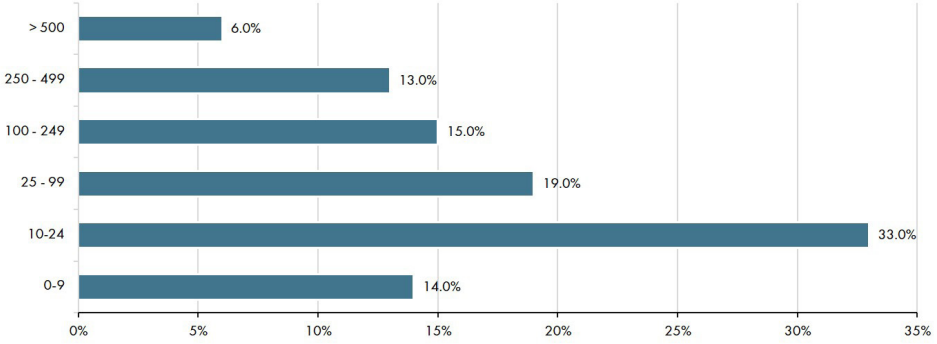


Moreover, large enterprises (15,000 employees and above) are processing 100 changes per week, and the majority do not leverage any automation to help ensure a swift, accurate process.

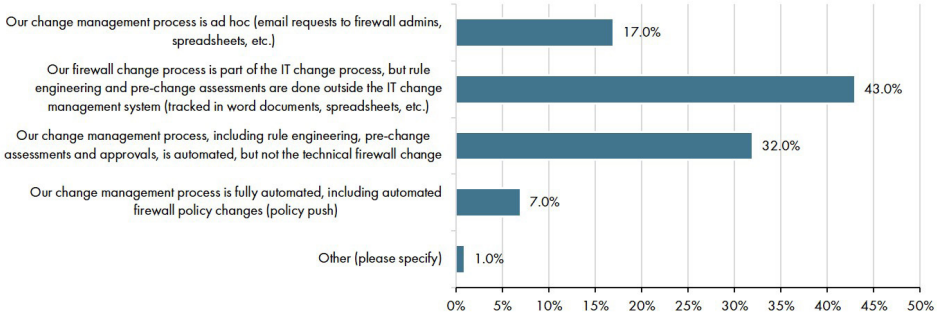
How many firewall change requests does your organization process each week? (all respondents)



How many firewall change requests does your organization process each week? (organizations >15,000 employees)



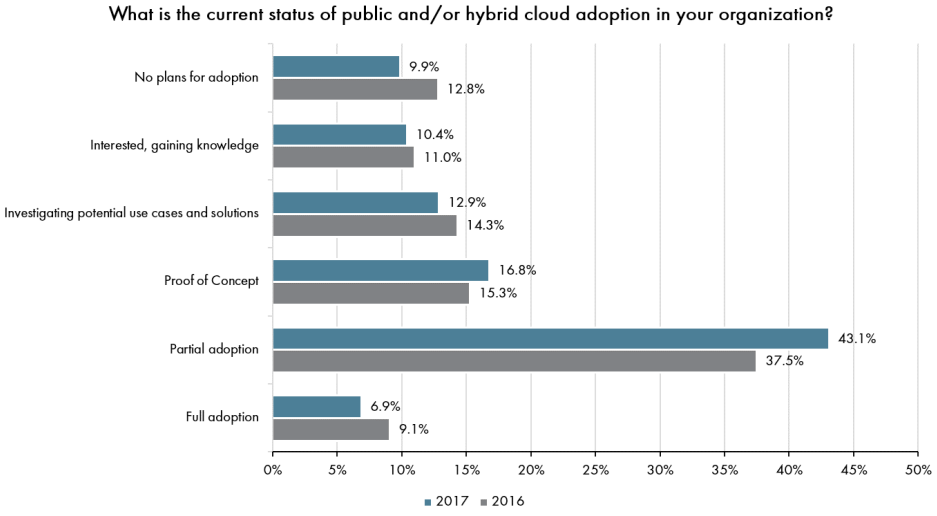
How do you currently utilize automation to manage the firewall change process? (organizations > 15,000 employees)

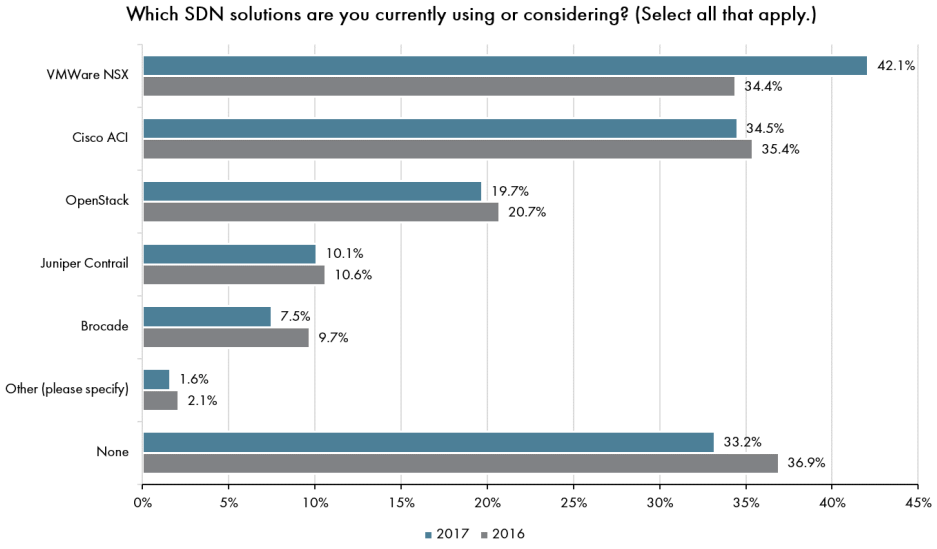


Cloud and SDN are gaining steam.

Increasingly, organizations are making investments in cloud and Software Defined Networking solutions to help them become more efficient and agile.

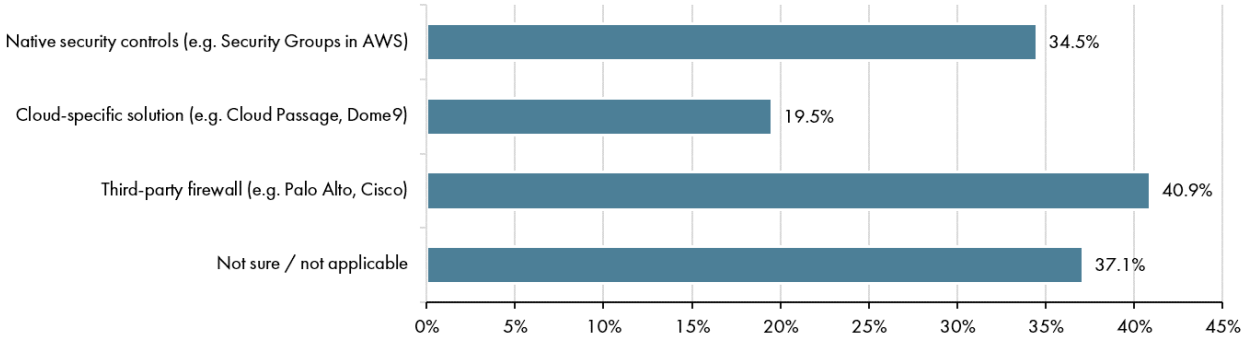
This study shows that 90% of organizations are adopting cloud technologies in some manner, and 67% are adopting an SDN solution.



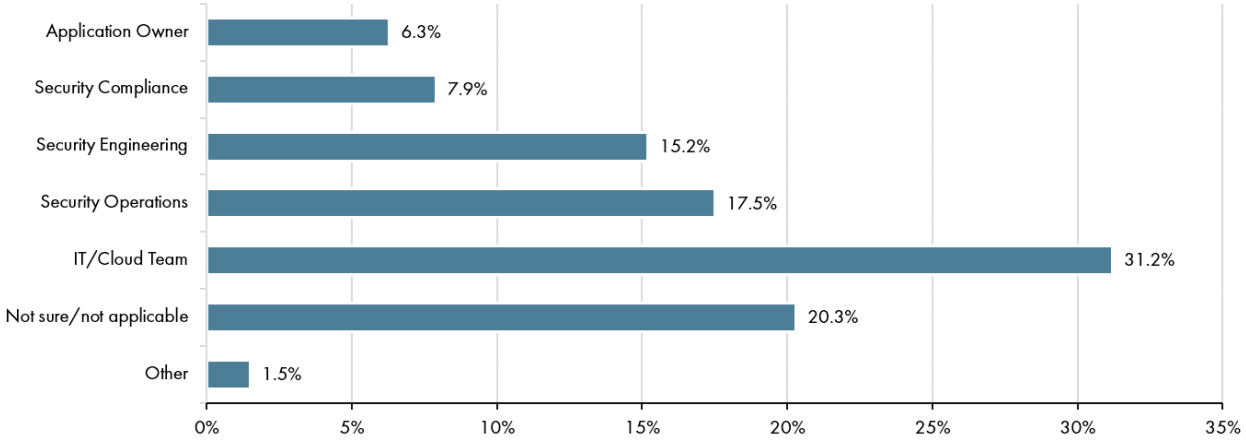


While businesses may rely more and more on the cloud, on-premises infrastructure is still very much relevant. This increases network security complexity two-fold. Methods for securing the cloud environment are split between traditional firewalls (41%) and non-traditional firewall solutions (54%). Ownership of security groups is split as well. 37% responded that responsibility for cloud security falls outside the security group, and 40% put responsibility on the security operations/engineering/compliance teams.

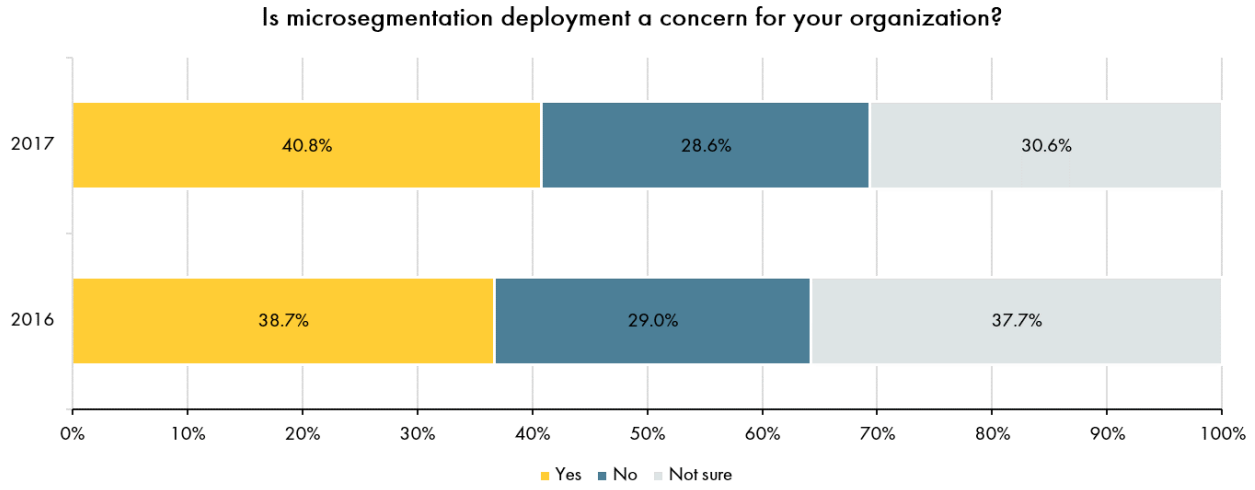
What types of network security control are you using in your cloud environment? (Select all that apply.)

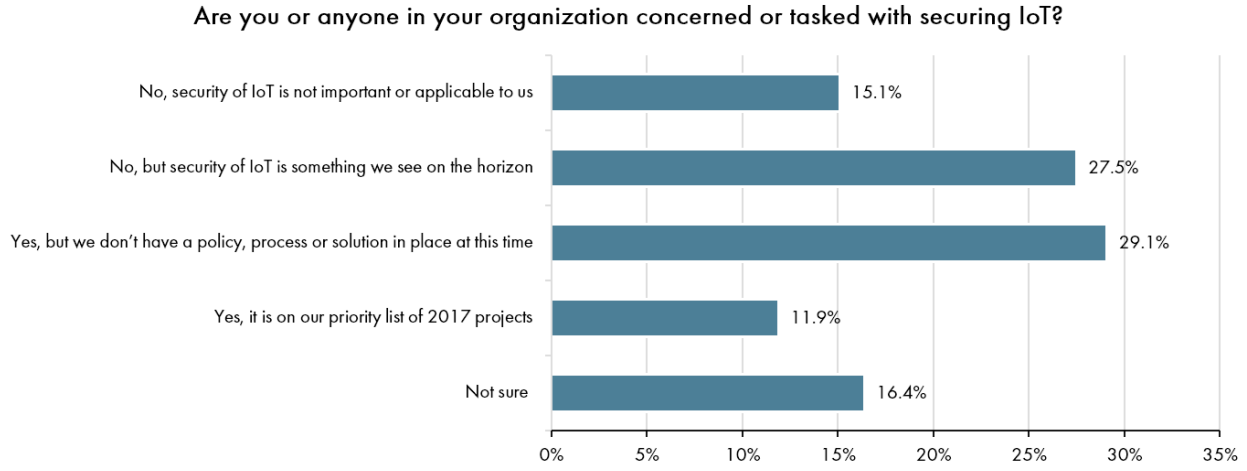


Who is primarily responsible for your network security in the cloud?



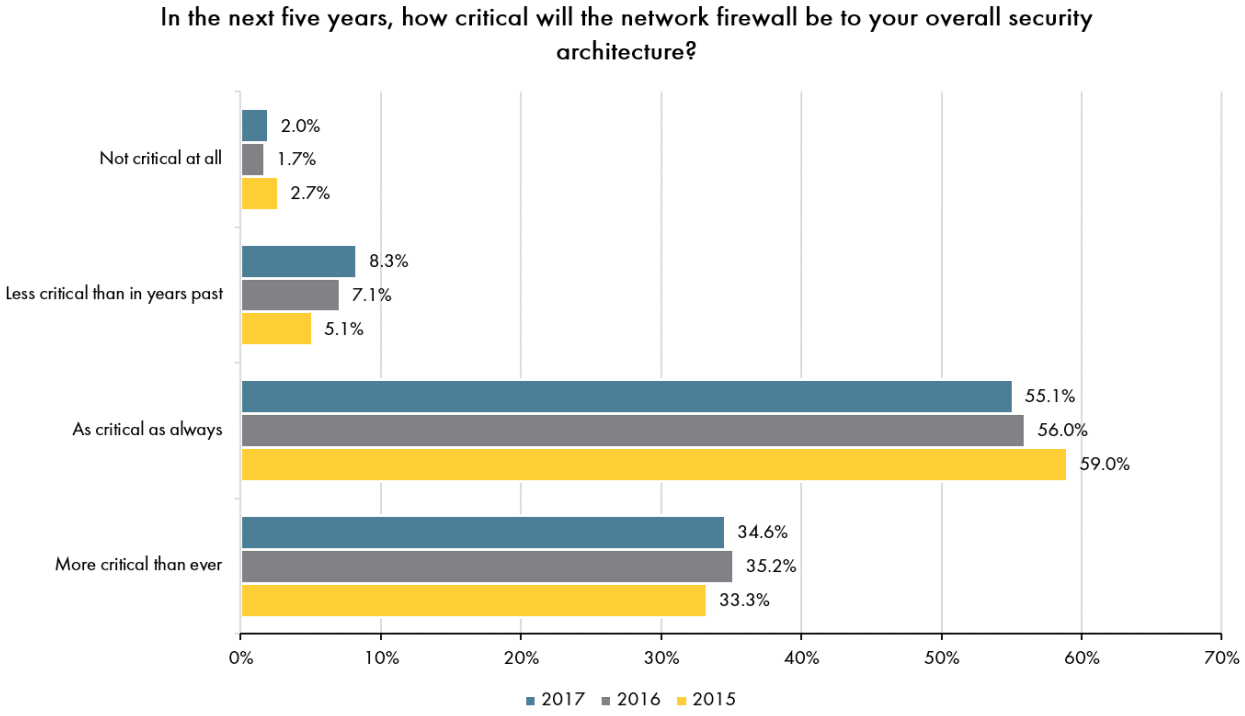
Furthermore, microsegmentation is a concern amongst 41% of organizations, slightly higher than 2016's 39%. One reason more organizations might be more focused on microsegmentation is the rise in IoT - 41% view securing IoT as a concern. With IoT malware becoming more prevalent with the likes of Mirai creating bots from millions of devices, microsegmentation is one option for attempting to cut IoT devices off from the rest of the network and control the problem.



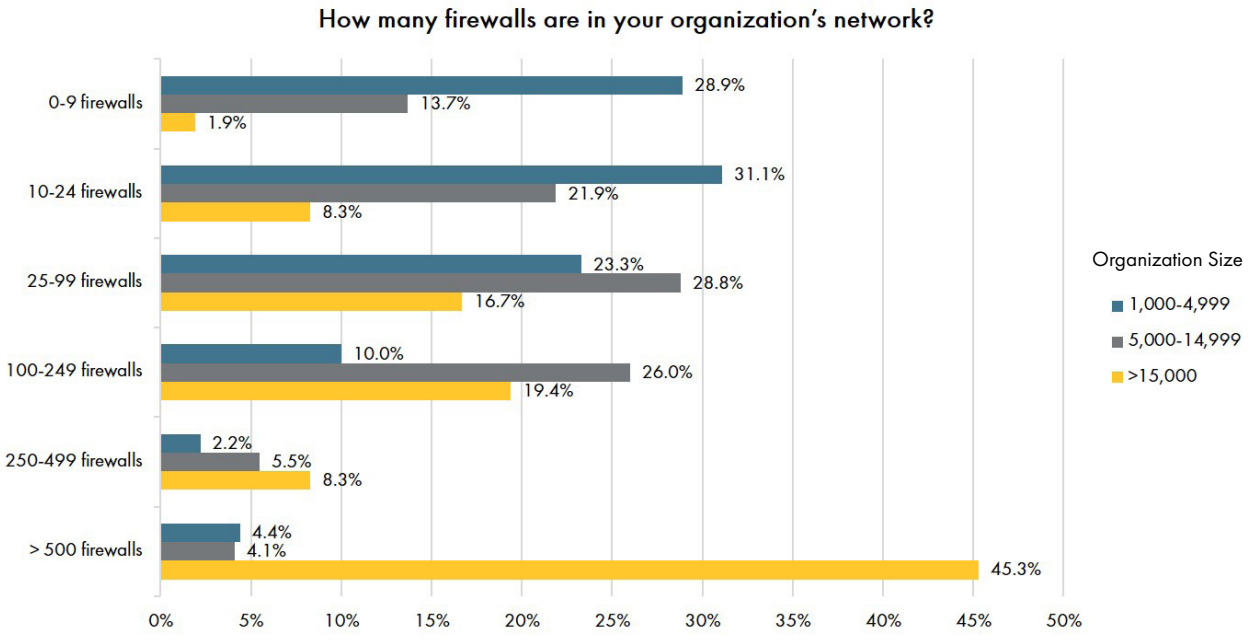


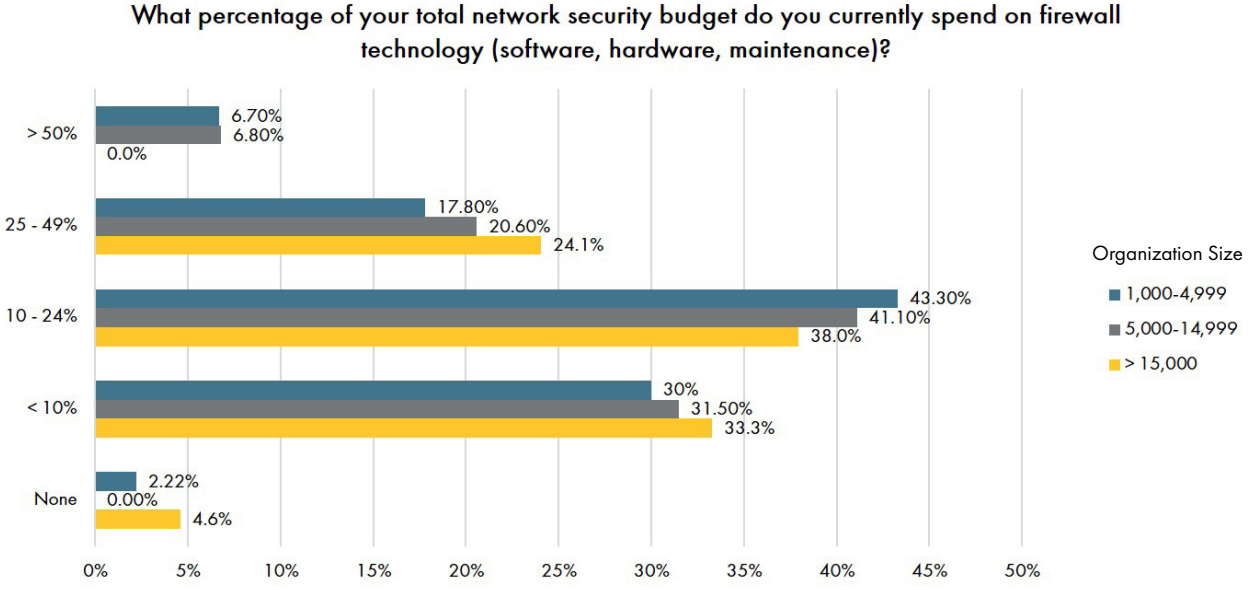
Firewalls continue to support it all.

No matter which route organizations go down to meet their networking requirements, firewalls continue to support it all, from traditional to next-generation to native or cloud options. For a third year in a row, organizations overwhelmingly agree that the firewall will remain critical over the next five years.



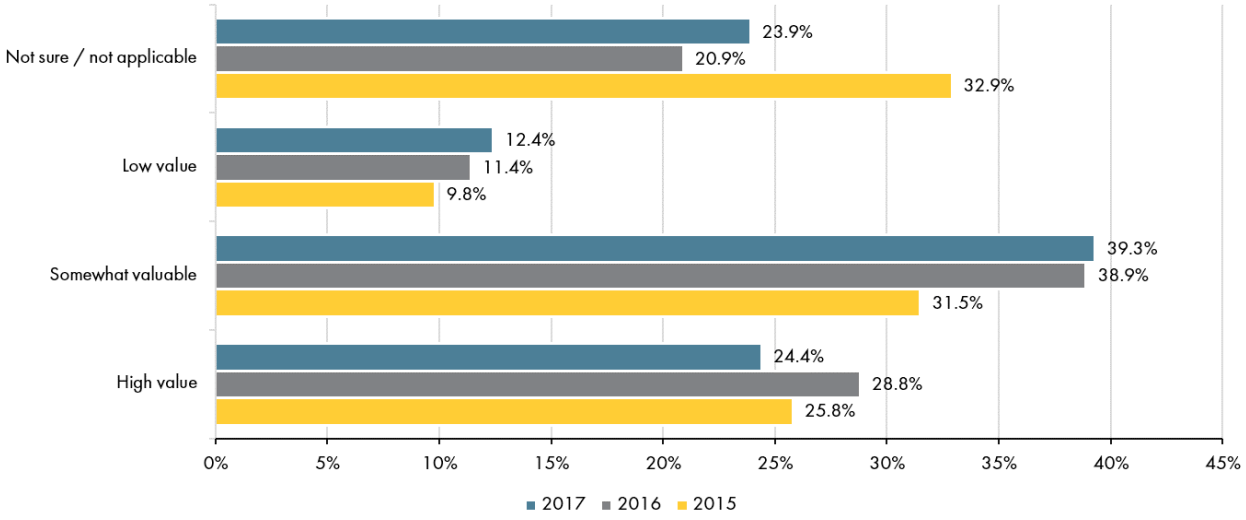
The majority of organizations surveyed have ten or more firewalls, and for 25% of respondents, firewalls make up at least a quarter of their security budgets.



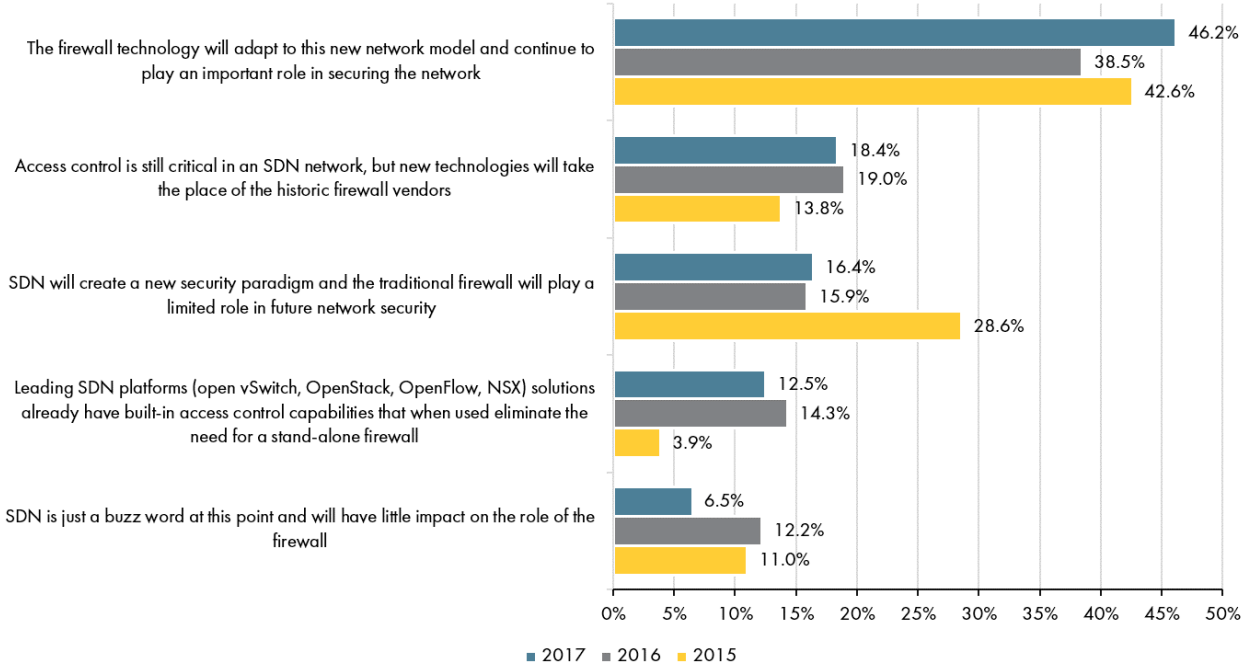


More than half of respondents said that firewalls have a place in securing cloud environments, and by and large, respondents believe traditional firewalls will adapt to SDN models. In addition, six out of ten will use NGFWs in virtualized environments. Four out of ten will use traditional firewalls.

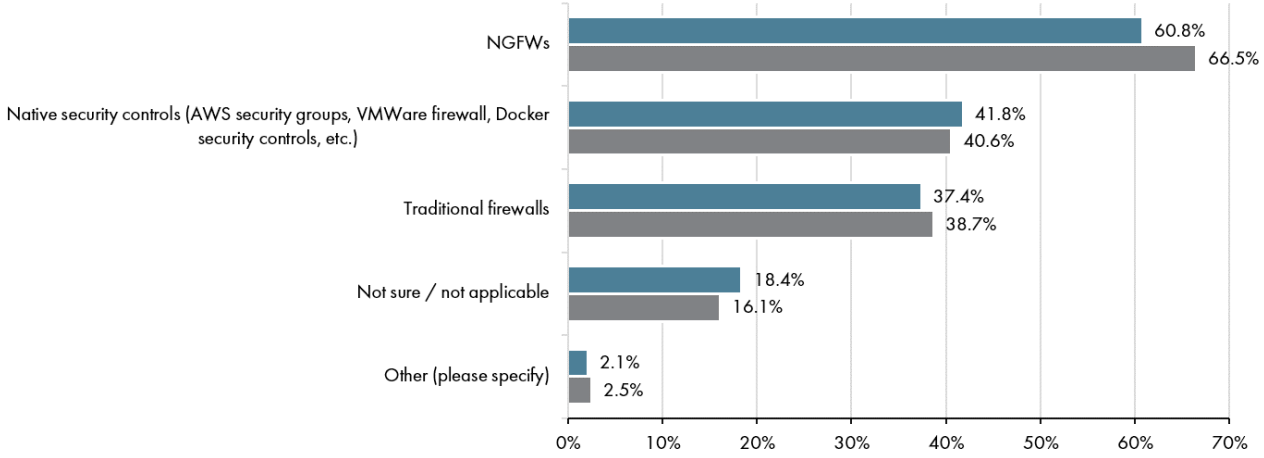
How much value do firewalls - traditional or NGFWs - provide for the cloud services you manage?



What impact will SDN have on the firewall?

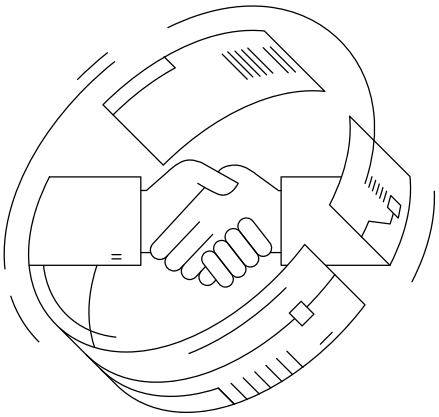


Within your virtualization environment, which of the following do you plan to use for security controls? (Select all that apply.)



Conclusion

From the data collected in this survey, FireMon believes that network complexity is and will continue to be a top concern for security professionals. The adoption of new networking paradigms, such as cloud and SDN, will continue to increase this complexity, requiring management processes to adapt to a faster, more diverse environment.



The firewall, according to survey respondents, isn't going anywhere. In fact, its role is expanding to include protection of cloud and SDN environments, and organizations continue to spend a significant portion of their budget on the firewall. The key to improving security will be effectively managing the inherent complexity of the technologies and keeping pace with the environments in which they reside.

With only 40% of large enterprises using automated processes for change management, there is untapped opportunity for operational efficiency improvements that will set organizations up to support the shift. A recent study conducted by Forrester Consulting found that "Managing and auditing firewall rules on a manual basis can expose an organization to greater risk of a breach, not to mention the additional time and senior resources needed to add new rules and address change requests."

For security organizations looking to reduce the likelihood of breaches and adapt their practices to meet networking demands, they need a global view of their policies that spans infrastructure types. Manual, device-by-device management is not sustainable. Automation will be critical to enabling dynamic management - from automating data intake to automating workflows to automating intelligence-based action.

As networking evolves to meet the needs of an "on-demand" society, security will have to evolve too or risk becoming a bottleneck or, worse, ignored altogether.