A Forrester Consulting
Thought Leadership Paper
Commissioned By VMware

February 2020

To Enable Zero Trust, Rethink Your Firewall Strategy

An Overreliance On Traditional Firewalls Leads To Suboptimal Tradeoffs Between Security Coverage And Complexity

FORRESTER®

Table Of Contents

Project Director:
Lisa Smith,
Principal Consultant Market Impact

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

In the last year, more than half of companies around the globe faced a major security incident.

57% of IT security professionals agree they err on the side of fewer/ broader security policies to allow for more flexibility, despite leaving significant security vulnerabilities open to attackers.

Businesses spend millions of dollars each year to secure customer data, applications, networks, and proprietary information. Yet, these businesses are frequently breached. For example, 58% of companies faced a significant security incident in the last year, as the number of threats and sophistication of attacks grew around the world.[1]

As a result, IT organizations are spending more to secure their networks. In 2019, network security spending was an average of 9% of the security technology spending budget, with 54% of security decision makers expecting to increase their network security spend in 2019.[2] But are these investments paying off? Are internal networks receiving the right kind of protections? Are vulnerabilities being minimized?

In May 2019, VMware commissioned Forrester Consulting to understand the challenges that businesses are facing in securing their internal network's east-west traffic. Forrester conducted an online survey with 224 IT security professionals responsible for their organizations' network, security, and infrastructure. We found that while there are many security technologies and services implemented to protect internal east-west network traffic, most companies are making suboptimal tradeoffs between the extent of security coverage and the simplicity of operations. Organizations across the globe are waking up to the limitations of perimeter-based security approaches and moving to a Zero Trust model. This research details how organizations can improve their security posture and achieve Zero Trust with a new approach that is purpose-built for firewalling east-west traffic.

KEY FINDINGS

- **Security professionals are operating with a false sense of security.** Almost 59% of IT security professionals feel they are efficiently protecting the internal network, yet according to Forrester's Global Business Technographics Security Survey, 58% faced a major security incident in the last year.
- **Using traditional perimeter firewalls to protect the internal network is ineffective.** Seven out of 10 enterprises are handicapped by an overreliance on perimeter firewalls and believed that they were overprovisioning firewalls, which can be expensive. Fifty-seven percent agreed this meant a tradeoff between coverage and operational flexibility and agility.
- **Restrictive firewall policies are blocking developer agility.** Three-quarters of enterprises face challenges with the rapid pace of application changes, and 73% report that firewall policy provisioning efficiency cannot keep up with the pace of development.
- **IT security professionals seek app-centric, built-in, cross-platform security controls.** The future of security depends on application-based security controls. Three out of five respondents prefer built-in security controls over agent-based solutions. In particular, 70% agree that hypervisors should house security controls.

FORRESTER®

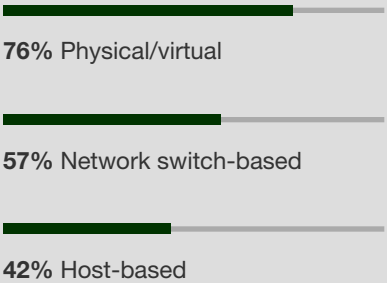
Protecting The Internal Network With Traditional Firewalls Is Not Working

Businesses have a multitude of security products and services implemented to protect the perimeter, internal network, cloud repositories, applications, and legacy infrastructure. Despite massive investments in security solutions, these businesses are often not using the right tool for each environment resulting in cost, complexity, lack of visibility, and compromised security outcomes. In surveying IT security professionals, we identified four common issues with current security environments:

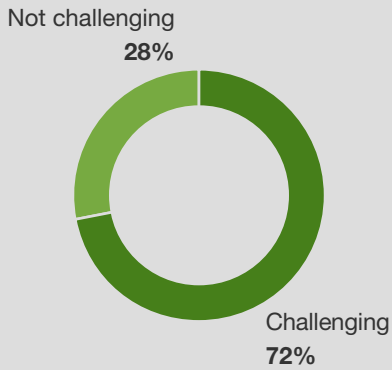
- **Enterprises are not adequately protecting their internal networks.** Over 75% of companies depend on virtual or physical perimeter firewalls to secure internal network traffic. However, 72% believe their overreliance on perimeter firewalls is a significant challenge to the security of their internal network (see Figure 1). Using perimeter firewalls to protect the internal network requires traffic hairpinning and often significant network re-architecture, forcing a tradeoff between coverage and simplicity. This tradeoff leaves gaps in an organization's security posture.
- **Legacy firewalls are an expensive approach to internal security.** Seven in 10 enterprises are overprovisioning firewalls — an outdated paradigm that is expensive when used for east-west traffic. Further, 72% of the respondents believe the lack of adequate network segmentation is creating security vulnerabilities in the organization. Securing east-west traffic is different than securing north-south traffic and requires different solutions.

Figure 1: Majority Of Companies Use Physical/Virtual Firewalls

"Which of the following form factors describe your current internal firewalls?"*



"Overreliance on perimeter firewalls is challenging to my organization."



*Base: 140 IT security and infrastructure decision makers and practitioners at global enterprises who identify as having a firewall
Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

72% of enterprises are challenged by an overreliance on perimeter firewalls when securing the internal network.

FORRESTER®

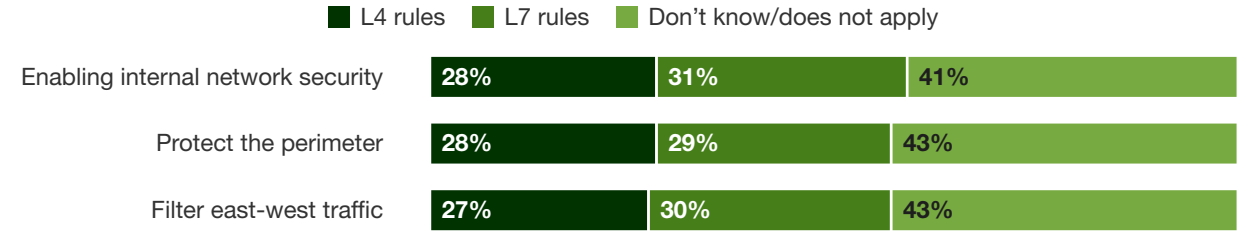
› **Disparate security solutions are creating integration challenges.** The sprawl of devices and the proliferation of different control requirements and tools compromise the security posture. More than three-quarters of companies manage 10 or more security products, and nearly 20% manage 50 or more security products. It's not surprising that a majority of IT security professionals have significant integration challenges. This lack of integration hinders adaptability, creates security gaps due to misaligned controls, and makes management difficult.

› **IT security professionals still lack visibility into activities on the network.** Enterprises are not using advanced features, as less than one-third of companies report they are writing layer 7 rules to filter east-west traffic (see Figure 2). Despite the number of products being used, 73% of IT security professionals feel they lack adequate controls to monitor, filter, and analyze east-west traffic. Nearly three-quarters feel they lack visibility into activities on the network. Ensuring visibility across the entire data center is the first step to a strong security posture, something traditional perimeter firewalls cannot deliver.

76% of enterprises manage 10 or more different security products; 77% face integration challenges.

Figure 2: Less Than One-Third Of IT Security Professionals Are Likely To Use L7 Rules

"Thinking about the firewall rules your organization writes, which rules are you more likely to write for each of the following objectives?"



Base: 123 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

Rapid Application Of Future Deployment Will Magnify The Security Challenges For Internal Networks

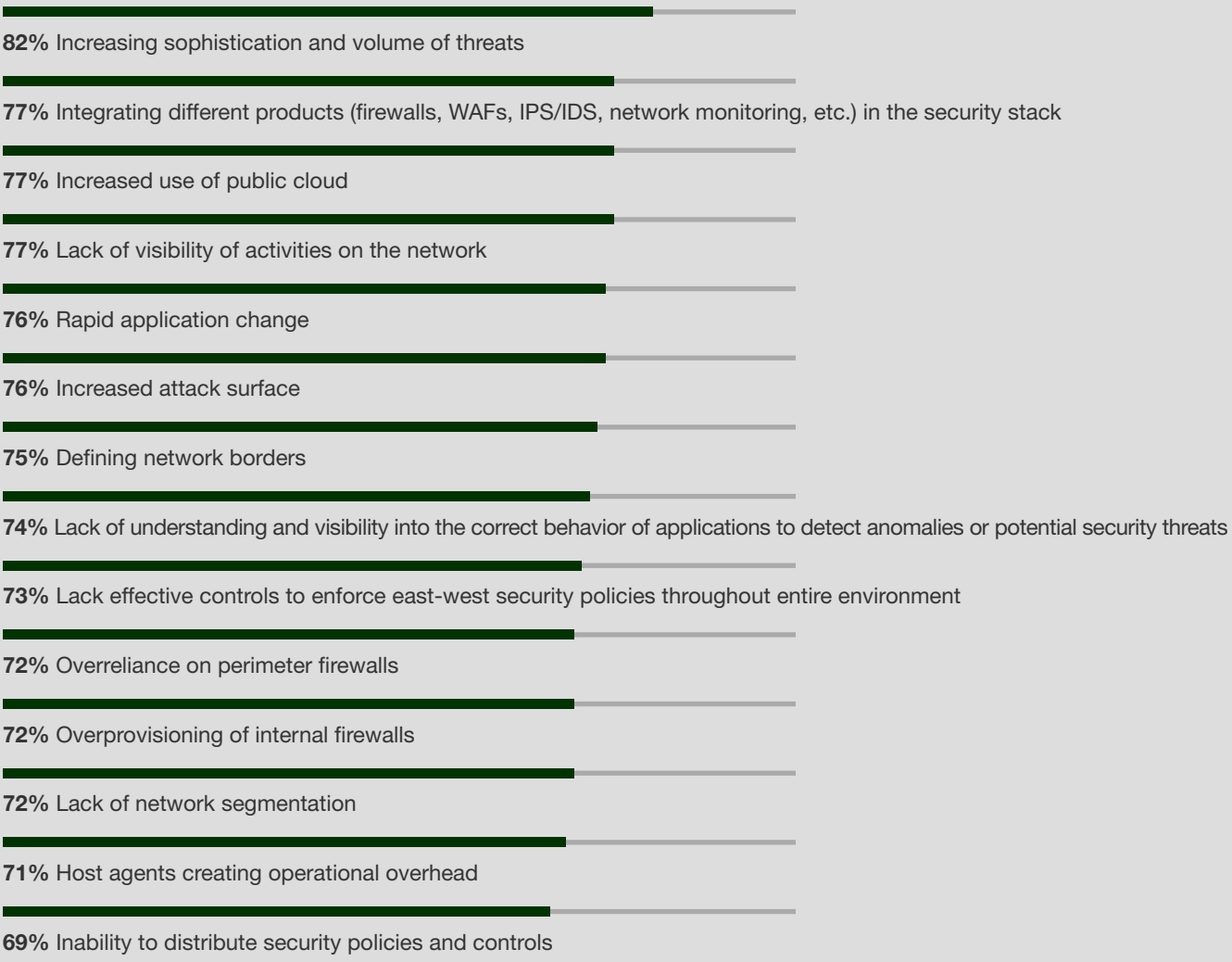
Enterprises are vulnerable because complexity is being driven by the number of different security products and outdated security approaches. Looking forward, the new realities of application deployment will make protecting internal networks even more challenging. IT security professionals face a host of technical and organizational challenges in preparing for the future.

TECHNOLOGY CHALLENGES AROUND PROVISIONING AND INFREQUENT UPDATES LEAVE GAPS IN SECURITY POSTURES

- **Application deployment is outpacing security control provisioning.** Many enterprises find that firewall policy provisioning cannot keep up with the pace of development. Provisioning a new internal firewall takes too long: 41% of organizations report that it takes two or more days to provision a new internal firewall policy change. Companies are working to speed up provisioning and become more agile. Nearly one-quarter of interviewees report they are currently deploying security policies as part of their continuous integration and continuous delivery (CI/CD) process.
- **Distributed applications blur visibility into application communications and behaviors.** The lack of visibility into intra-application communication will continue to challenge organizations as they define comprehensive security policies. Nearly three-quarters of IT security professionals say there's a lack of understanding and visibility into the correct behavior of applications, making it challenging to detect anomalies or potential security threats (see Figure 3).
- **Application changes expose new security threats.** The rapid pace of application development challenges three-quarters of enterprises (see Figure 3). A small group of enterprises (18%) feel they could keep up with continuous updates to security policies.
- **Native security controls in the public cloud are insufficient.** IT security professionals are concerned about security policies as they migrate workloads from on-premises to the public cloud. Eighty-four percent believe that their workloads would fail if they migrated to the cloud. In addition, companies struggle to manage security policies across public clouds and to automate security policies between on-premises and public clouds (see Figure 4). While advanced security services are available, only 42% of companies report using them to protect their public cloud environment.

Figure 3: Companies Face A Multitude Of Technical Challenges

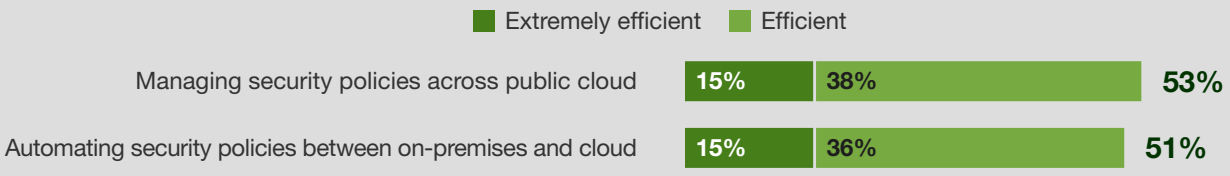
"Thinking about your organization's security vulnerabilities, how challenging are each of the following technical factors?" (Percentages represent top "moderately/very challenging")



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

Figure 4: Not Efficient Managing Or Automating Security Policies Across Public Cloud

"Please indicate how efficient your organization is at doing the following tasks."



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises.
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

FORRESTER®

ORGANIZATIONAL ISSUES CREATE ROADBLOCKS AND SLOW CHANGE

Addressing technical issues may not altogether remove obstacles, as firms cite many organizational and process challenges. Our study found that companies overall:

- **Lack a security strategy.** Nearly three-quarters of IT security professionals report there is a lack of attention on and awareness of possible risks. Many enterprises lack a cohesive security philosophy, such as Zero Trust, to protect the internal network. And more than two-thirds report a lack of executive support and clear ownership of the security strategy (see Figure 5).
- **Cannot respond quickly to infrastructure changes.** The complexity of deployed security tools makes it difficult to react quickly to change — an issue for seven out of 10 companies. To overcome this inflexibility, more than half (57%) of respondents agree that they err on the side of having fewer but broader security policies. This tradeoff creates security gaps and vulnerabilities.
- **Inconsistent policies leave security gaps.** There's a tendency for companies to normalize lenient security policies in the name of flexibility. And without a cohesive security strategy in place or clear ownership/executive support, disparate tools emerge and multiple security control teams proliferate. This loose security posture ultimately makes the organization more vulnerable.
- **IT talent is at a premium, don't count on the workforce.** IT security professionals report that the lack of technical prowess in staff is challenging for their organization. The cloud security space is unfortunately rife with the absence of human capital. Don't rely on scarce human resources as part of your future-state planning. Instead, look to technologies that optimize and integrate with cloud-native solutions. Using more cloud-enabled and security-focused automation solutions will help your organization move to the cloud correctly and safely.

Figure 5: Nearly Three-Quarters Of Companies Are Unaware Of The Risks Posed By Security Vulnerabilities

Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Note: Selected variables shown.
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

FORRESTER®

Stop Making Suboptimal Tradeoffs, Think Differently About Security Controls

Securing the internal network is complex, and IT security professionals can no longer shoehorn traditional application-based firewalls for this use case. They must think differently as they plan for the future. With 73% of respondents reporting a challenge in keeping up with the pace of application change, it's no surprise that IT security professionals plan to shift toward software-based and application-centric security controls that operate at the level of each workload. We identified several key initiatives that companies are pursuing as part of these efforts:

› **Improve agility with application-based security controls.** Sixty-four percent of interviewees agree that the future of security is reliant on application-based security controls, and 61% agree that firewall policies must be application-centric (see Figure 6). Application-based security control is the future, as companies plan to become more agile. Further, 55% of organizations are planning to deploy security policies as part of their CI/CD process within the next two years (see Figure 6).

Figure 6: The Future Of Security Is Reliant On Application-Based Security Controls

Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

Only 24% of companies currently deploy security policies as part of their CI/CD process.

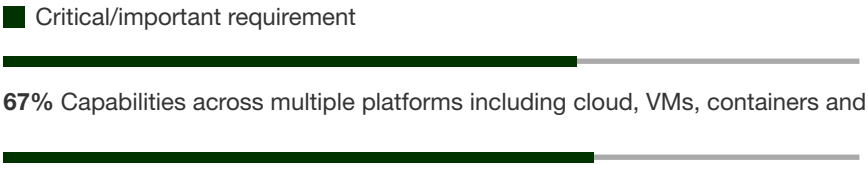
FORRESTER®

› **Deploy security policies consistently across multiple platforms.** Seventy-one percent of interviewees seek consistent enforcement of security policies across private and public cloud environments. And firms want this consistency for security configurations as well, with 69% seeking a standard security policy for all cloud workloads (see Figure 7). This consistency will enable enterprises to mitigate vulnerability gaps.

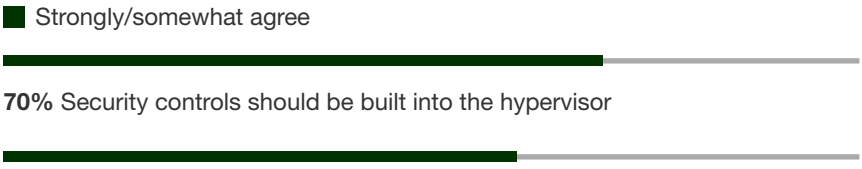
› **Use built-in security controls for each workload.** IT security professionals prefer built-in security controls over agent-based solutions. Approximately half of firms report having 20 or more agents, creating overhead costs related to agent management. And as IT security professionals seek agentless solutions, 70% agree that security controls should be built into the hypervisor. Pushing security controls down the stack into the hypervisor will improve scalability and streamline operations (see Figure 7).

Figure 7: Security Solution Capabilities For The Future

Cross-platform capabilities and standard policies for all cloud workloads are an important requirement.



There is a strong preference that security controls should be built in vs. agent-based.



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

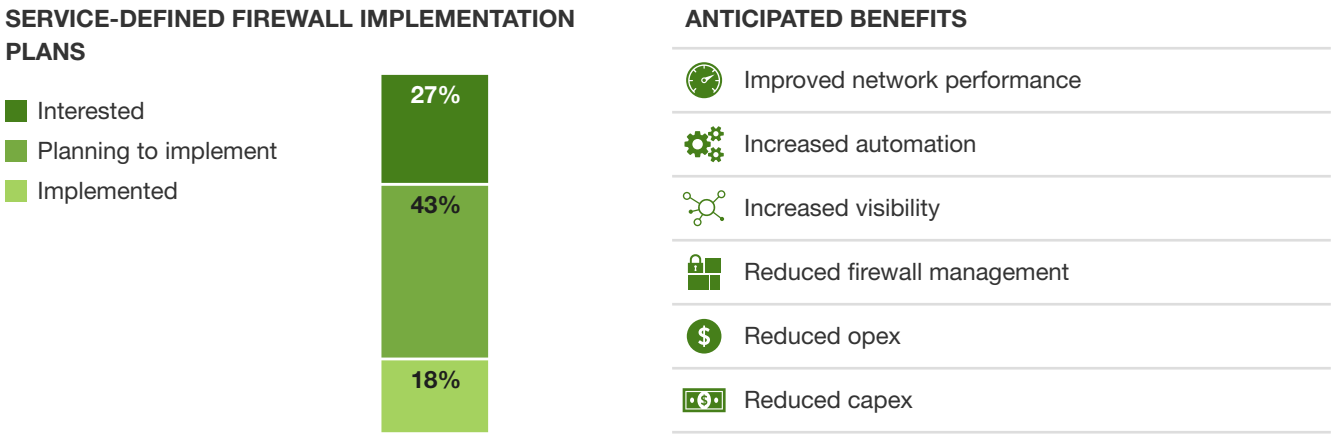
SERVICE-DEFINED FIREWALLS PROTECT EAST-WEST TRAFFIC

As companies look to protect the internal network, we found nearly 20% believe they had implemented some version of service-defined firewalls. Service-defined firewalls are data center firewalls that protect east-west (internal) traffic across private and public cloud environments at the granularity of workloads. Network security professionals use these firewalls to mitigate risk, prevent lateral movement of attackers, and ensure compliance with the stated security policies of their organizations.

Looking forward, 43% of respondents plan to implement service-defined firewalls in the future, and an additional 27% are interested in the technology as a solution to protect their internal network. Service-defined firewalls address the desire for a built-in, multicloud tool that provides layer 7 network controls.

IT security professionals anticipate tangible benefits from service-defined firewalls. The most anticipated technology benefits include improved network performance, increased automation, increased visibility, and reduced firewall management. Further, enterprises anticipate a reduction in operating expenses and lower capital expenditures (see Figure 8).

Figure 8: Service-Defined Firewalls Provide Benefits



Definition: A service-defined firewall is the intrinsic stateful layer 7 firewall that underpins a virtual cloud network. It is purpose-built to reduce the attack surface of applications inside the network perimeter of hybrid and multicloud environments. The service-defined firewall binds security controls to services and applications to prevent lateral movement and other attack vectors specific to the internal network.

Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

Key Recommendations

The frequency and sophistication of attacks are advancing at an unprecedented pace, and companies can no longer rely on traditional security practices to keep the internal network safe. They must invest in the right capabilities to protect internal networks now, i.e., they need to use the right tool for the job. However, striking the right balance between coverage and simplicity is critical for security professionals. To meet these growing challenges, Forrester recommends the following:

Set a strategy for survival. Cyberspace is a war zone. That means every packet your business and customers send is actively transiting a live battlefield. To attempt crossing this battlefield without an actionable strategy is a guarantee that sooner or later your organization will be a casualty. Define a strategy and set a plan in motion for survival, and let your plan guide your technology selection.

Zero Trust requires granular security controls. Applications and networks exist everywhere in today's technology landscape. Organizations need granular security policies across their infrastructure and down to the level of workloads to ensure blind spots are eradicated. A complete suite of granular controls can make it possible to gain the upper hand in this dynamic environment.

Inspect more east-west traffic. To reduce the attack surface visible to potential attackers, inspect all east-west traffic. Inspecting east-west traffic makes it possible to detect lateral movement early and reduce damage. Where possible, choose inspection tools that don't require a network redesign yet minimize the impact on the network.

Move at the speed of application development. The speed of application development has created a massive challenge for security teams wedded to traditional appliance-based security architectures. To prevent developers from compromising on security in favor of speed, choose software security controls that track the lifecycle of applications, are automatable, and can integrate with orchestration systems.

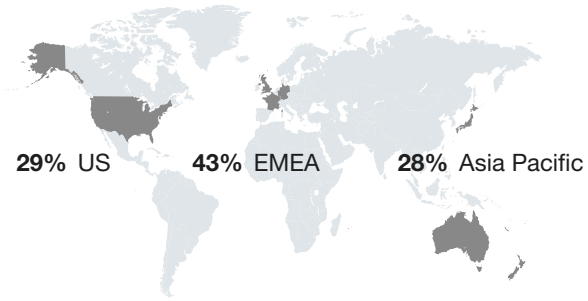
Simplify both the security stack and operations. Thanks to innovations over the last few years, it is possible to have a simple but robust security solution. Look for solutions built into the infrastructure to make security provisioning and management more effortless. Simplicity enables the consistent application of security controls while limiting misconfiguration.

Appendix A: Methodology

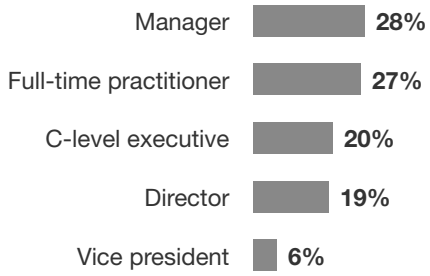
In this study, Forrester conducted an online survey of 224 IT security professionals in the US, Europe, and Asia Pacific. Survey participants included decision makers in security, network security, and infrastructure and operations. The study began in June 2019 and was completed in July 2019.

Appendix B: Demographics

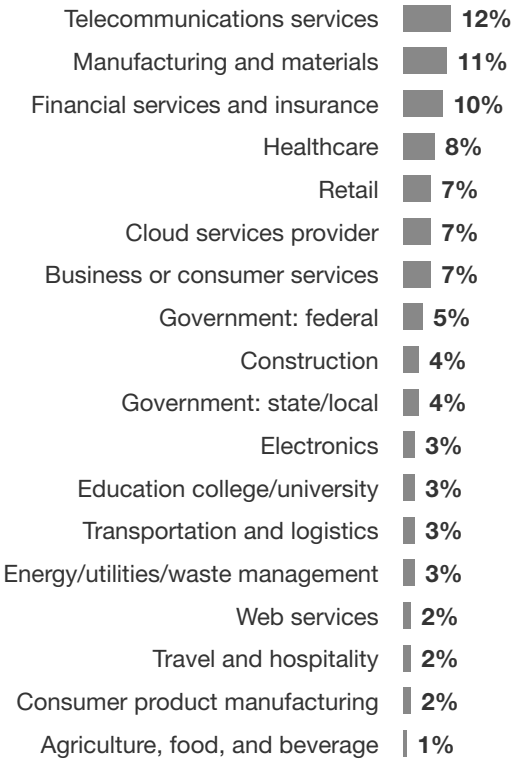
REGION



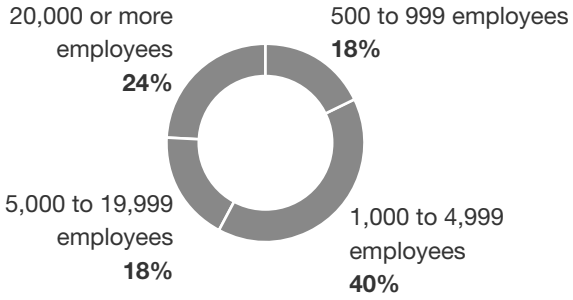
RESPONDENT LEVEL



INDUSTRY



COMPANY SIZE



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

Appendix C

ENDNOTES

[1] Source: Forrester Analytics Global Business Technographics® Security Survey, 2019.

[2] Ibid.

FORRESTER®