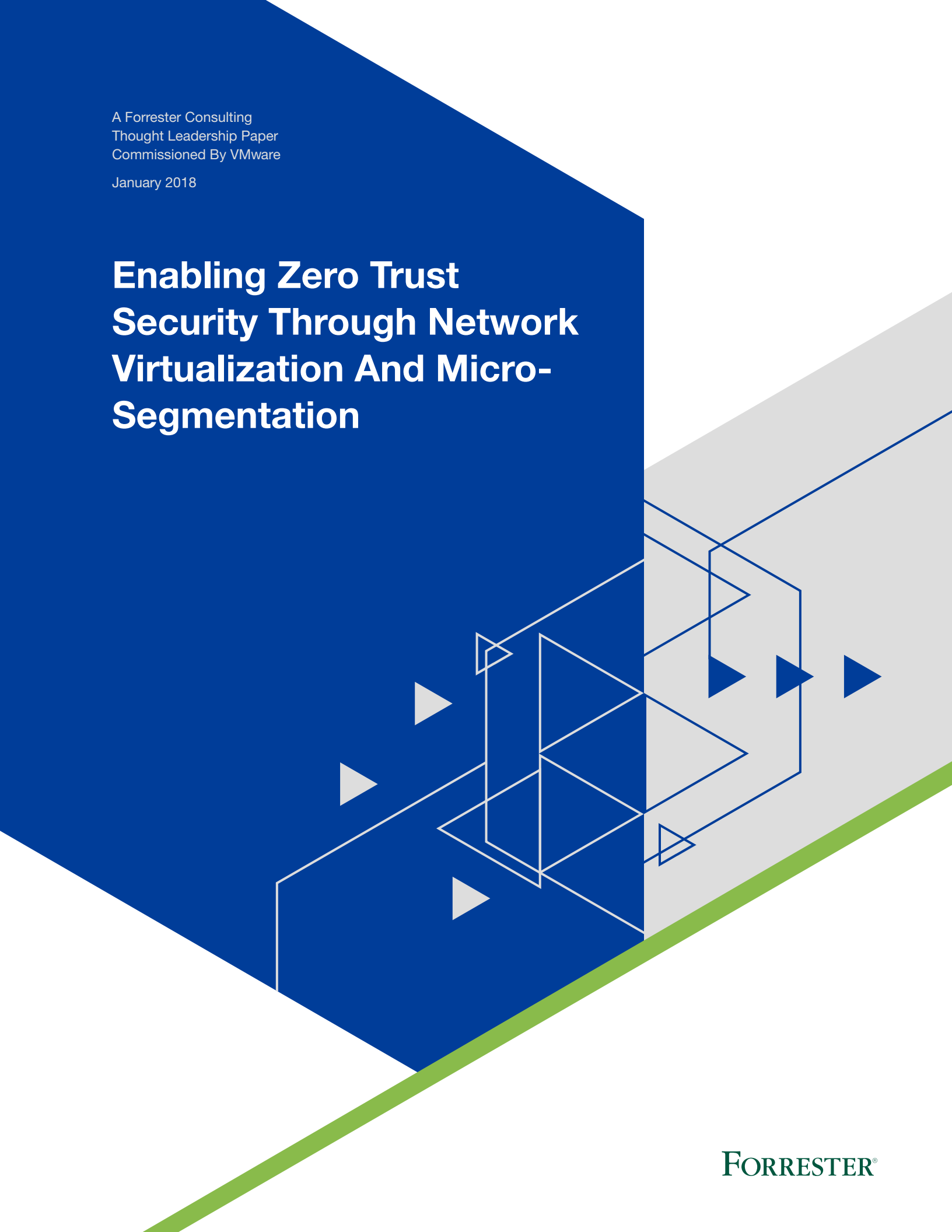
A Forrester Consulting
Thought Leadership Paper
Commissioned By VMware

January 2018

Enabling Zero Trust Security Through Network Virtualization And Micro-Segmentation



FORRESTER®

Table Of Contents

1 Executive Summary

2 Security Management Gets Tougher As Threats Become More Pervasive

3 Addressing Security Vulnerabilities With The Zero Trust Security Model

6 Enabling Businesses To Be Successful With Micro-Segmentation

7 Benefits Of Network Virtualization And Micro-Segmentation

8 Key Recommendations

9 Appendix

Project Director:
Chris Taylor,
Sr. Market Impact Consultant

Contributing Research:
Forrester's Infrastructure & Operations 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

IT and security pros feel as though security threats are now more ubiquitous and damaging than ever before — and they're not wrong. Historically, companies have invested a lot of time and effort in building awareness around security threats so that they know how to protect themselves, but that approach is no longer viable. Today, hacking has become a commodity that anyone anywhere can buy or learn. Organizations must work to change how they defend their networks by countering the proliferation of the attack vectors. The time to turn inward is now.

In November 2017, VMware commissioned Forrester Consulting to evaluate how organizations today are improving the security of their infrastructure through network virtualization and micro-segmentation. The study also included a comparison of the results of a similar study Forrester conducted for VMware in 2015. Through our analysis, Forrester found that companies today attribute more of their security issues to improper network segmentation than the volume of threats overall. In response, network virtualization is becoming a key piece of the security apparatus for leaders across industries as organizations leverage the power of virtual capabilities to enable strategic security initiatives.

KEY FINDINGS

- **For IT pros, dealing with security threats is now a fact of life.** It's a given that today's IT workers will confront security threats multiple times throughout a year. It's no longer about wondering *if* threats will come, instead the more relevant question is how equipped are companies to defend themselves when threats *do* come? No organization is immune to threats, and all companies must be prepared, as 92% of respondents report having faced minor incidents in the last 12 months alone, while 65% of respondents have endured a major incident in the same time span.
- **Network virtualization is the first step in reducing the severity of incidents.** Eighty-seven percent of respondents agree that virtualization is the key component of any next generation infrastructure, with eight in 10 respondents citing network virtualization as a key strategic initiative for the company. Greater virtualization will provide better security and enable more accelerated network provisioning. While the frequency of incidences will remain high, network virtualization will curtail the harm an attacker can inflict.
- **The next step is micro-segmentation.** Savvy IT and risk decision makers reap a multitude of benefits from micro-segmentation of their network, including improved network security controls, data protection, and containing the spread of threats.

Security Management Gets Tougher As Threats Become More Pervasive

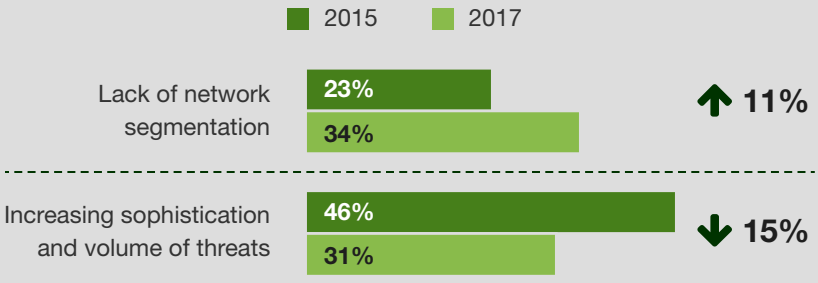
These days, managing security is getting harder, not easier. Business technologies continue to improve at breakneck speeds — unfortunately, so do cyberthreats. Despite advances in security technologies, cybercriminals seem to stay one step ahead thanks to accessible and easy-to-use hacking tools. The numbers show that this is more than just a baseless impression, as 66% of respondents have faced a major security incident such as a data breach or DDoS attack in the last year alone. Nine in 10 firms have fallen victim to minor incidents (a phishing attempt, malware infection, or lost/stolen asset), not to mention 16% of companies have dealt with over 10 minor incidents in the last 12 months alone. Furthermore, these threats come from all directions; most come from external sources, but 40% of companies reported incidences that originate from internal sources as well. The result of these ongoing threats is that today's IT risk and compliance decision makers consider their organizations to be more susceptible to threats today, compared with two years ago when Forrester conducted a similar study.

In trying to understand why companies feel more susceptible today than two years ago, we asked companies to specifically identify what they attributed their main security vulnerabilities to be. We found that today, in 2017, companies are seeing their own network security as the vulnerability point, whereas in 2015, companies were putting the blame on the growing volume of threats and not necessarily their own security measures (see Figure 1).

The increased emphasis on network segmentation suggests that the issue for today's IT teams is no longer *if* they'll face a security threat but how often — and how damaging. Rather than worrying about the growing volume and changing nature of threats, companies are turning their attention to getting the right control over their networks.

Figure 1

Perception of where security vulnerabilities originate is shifting internally



Base: 225 IT and risk and compliance decision makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, November 2017

As threat activities become more pervasive, companies must put greater focus on network security.

FORRESTER®

Addressing Security Vulnerabilities With The Zero Trust Security Model

To create a more secure network, companies must restructure their infrastructure in a way that allows all data to be protected regardless of where it sits in the network. This is the premise of the Zero Trust security model — where there is no longer a trusted and untrusted network, but rather all networks are untrusted and need to be secured equally. The Zero Trust model supports the argument that traditional, perimeter-based security configurations are no longer a sufficient measure for protecting the network, and highlights steps companies can take to better secure their network, starting with network virtualization and micro-segmentation.

NETWORK VIRTUALIZATION

Whether or not the end goal is a Zero Trust security model, network virtualization is an important step that many organizations are taking to better protect their network from security threats: It creates the foundation upon which other security measures can be implemented. That is why nearly 75% of respondents are pursuing network virtualization as a key strategic initiative. Network virtualization is seen as important for several reasons:

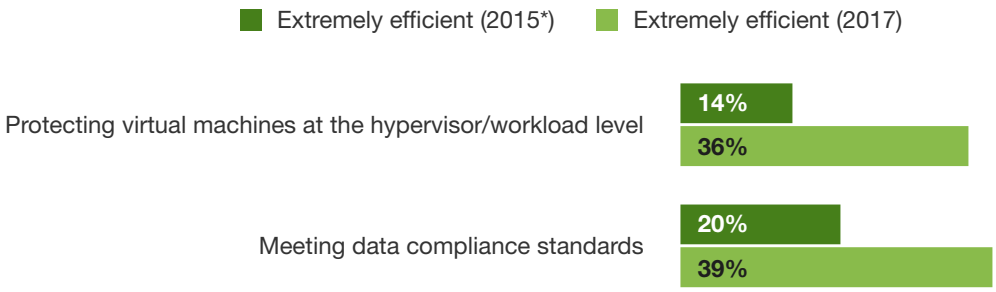
- **Improved security.** Network virtualization enables easier control and isolation of environments and assets. Using this technology correctly empowers the micro-segmentation of potential areas of concern and is a key piece of an overall security strategy.
- **Improved network visibility.** Being able to see all assets, devices, and components of the network is pivotal to situational awareness. No defender can stop threats when they don't know what is actually present on the network. Using virtualization technology to enhance isolation improves control within those protected network segments, and thusly empowers security teams to respond more intelligently to attacks.
- **Improved business continuity.** Organizations are bound to get hacked and assets will be attacked. Expecting and preparing for the inevitable security threat can help limit the impact those attacks have upfront, thus minimizing any disruption to the business. As well, network virtualization technology can enable a more adaptable recovery mechanism for leadership and is a key piece of any redundant system.

With these expected benefits top of mind, 59% of companies surveyed report already having network virtualization implemented to some extent, with 30% more planning to do so soon. In fact, companies believe so much in the value that virtualization provides, that 95% of companies are interested in moving toward full virtualization of their technology infrastructure (including servers, storage, etc.)

The desire for greater virtualization comes as companies become more confident in working with virtualized environments. For example, in 2015, only 14% of companies felt that they were very efficient at protecting virtual machines at the hypervisor level, and only 20% felt very efficient at meeting data compliance standards. In 2017, however, the number of companies who felt very efficient with those processes nearly doubled to 36% and 39%, respectively (see Figure 2). While not fully efficient yet, companies are gaining greater confidence in working with virtualized networks, and as they do their ability to virtualize a greater amount of their network infrastructure increases.

Figure 2

"How efficient is your organization at doing the following tasks?"



Base: 225 IT and risk and compliance decision makers at organizations with 500 or more employees
*Base: 210 IT and risk and compliance decision makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMWare, June 2015 and November 2017

MICRO-SEGMENTATION

As networks become virtualized and micro-segmentation becomes a strategic advantage for security teams, data inherently becomes segmented into buckets to allow security and network teams and managers greater visibility and control over all information on the network. Businesses use this segmentation to separate the day-to-day business data from the sensitive or proprietary data within the organization. From there, security and risk teams can place the proper security and access controls on sensitive data segments, i.e., micro-segmentation. The primary ways companies can leverage micro-segmentation include (see Figure 3):

- **Enabling network security controls.** Network admins can more quickly identify privileges for certain data types through micro-segmentation, thus enabling business users to work with network data faster and more efficiently. Micro-segmentation allows for businesses to quickly respond to changing security needs by increasing security or privileges on certain segments of the network based on immediate needs — improving security agility.
- **Better data visibility and protection.** The segmentation provided through virtualization fosters business agility by allowing businesses to respond more quickly to changing business and security needs. If organizations understand where data exists, and which users are supposed to have access to it, then data and services can be better monitored and flow more quickly through an organization to the appropriate users, thus improving overall data security and agility.
- **Stopping lateral spread of threats.** Network segmentation automatically interweaves connections and services to create micro-perimeters around specific sets of data and information. The micro-perimeters inhibit the spread of threats by separating business processes and associated data in specific and protected segments.

Figure 3

Micro-segmentation is leveraged in many ways

Base: 225 IT and risk and compliance decision makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMWare, November 2017

FORRESTER®

Enabling Businesses To Be Successful With Micro-Segmentation

Roughly 44% of respondents stated that their organization was already using micro-segmentation, with a additional 40% planning to implement within the next year. This statistic shows both the adaptability and versatility of this approach within virtualized networks. However, due to a variety of factors there are often challenges that impede companies from fully adopting micro-segmentation (see Figure 4). In order to overcome these barriers companies are making the following changes:

- **Establishing clear ownership for managing virtualization.** Lack of ownership stems from there being too many stakeholders around virtualization decisions. We found that most companies have two to three different departments considered to be key decision makers, but no clear leader. While having consensus and input across the different teams is important, there also needs to be a clear, singular entity who can drive and own the overall virtualization strategy. In response to this challenge, 70% of companies see the need for dedicated virtualization engineers or a virtualization team to manage the virtualized environments, and approximately a quarter of companies already have a team in place.
- **Hiring or training employees with the right expertise.** Lack of proper skills or training is an issue for one-third of companies. To address skills gaps, 63% of companies are hiring more dedicated security staff. By coupling these new hires with the need for a dedicated virtualization team, companies can build out strong virtualization teams with the know-how to handle greater levels of virtualization and growing security threats.
- **Improving network maturity.** Micro-segmentation is impossible without a network virtualization layer to build on. Companies must continue to advance their virtualization efforts and then look to build micro-segmentation capabilities on top of those layers as they become accessible.
- **Increasing budget.** Establishing a team to manage virtualization, hiring the right staff, and further developing networks all require additional funding to properly execute. Considering the potential cost impact of a data breach, it made sense that 80% of companies expect security budgets to increase. Given the greater focus on network segmentation compared to 2015, it was validating to see that security budgets are growing even more so than they were 2 years ago.

Figure 4

Challenges with virtualization highlight key opportunities for improvement

Base: 225 IT and risk and compliance decision makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMWare, November 2017

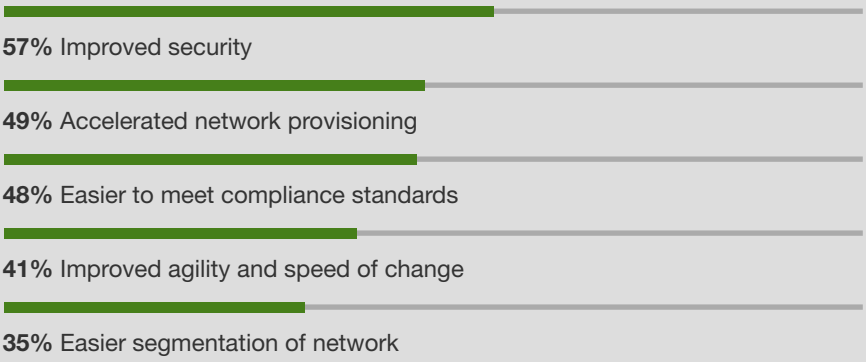
Benefits Of Network Virtualization And Micro-Segmentation

As companies overcome barriers to adopting network virtualization and micro-segmentation, their new infrastructure will yield a number of key business benefits, namely (see Figure 5):

- **Improved security.** Network virtualization and micro-segmentation are a key piece of a strategy to move toward Zero Trust. Companies will be better prepared to fend off the growing volume of both external and internal threats through tight controls of their data and the use of virtualization as a security tool.
- **Accelerated network provisioning.** It's hard to effectively manage sprawl and growth of networks in today's mobile, cloud, and bring-your-own-device (BYOD) world. Trying to maintain positive command and control of those disparate systems without using network virtualization is next to impossible. Properly leveraged micro-segmentation and virtualization greatly improves management and effective growth of any network.
- **Better ability to meet compliance standards.** Compliance is hard enough to do correctly with old technology. It's nearly impossible to achieve without closely managed and segmented networks. Using the tenets of Zero Trust, combined with micro-segmentation and network virtualization, enables compliant networks and is pivotal to achieving the checkpoints needed for compliance requirements.
- **Improved business agility.** Nothing is static in today's business world, particularly your networks. Network virtualization enables businesses to automate the provisioning and management of their infrastructure to respond quicker to business demands (for new apps, etc.) This also helps maintain business continuity and redundancy as systems constantly evolve.

Figure 5

Benefits of network virtualization and micro-segmentation



Base: 225 IT and risk and compliance decision makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMWare, November 2017

FORRESTER®

Key Recommendations

The world that our businesses operate in today is mandated by compliance needs, confused by the demands of an evolving series of technologies, and confounded by user demands for never ending access, and subsequently under constant threat of cybercriminal manipulation and conflict. To put it bluntly, it's a nightmare to manage. Without the use of newer technologies and tools as part of a Zero Trust strategy, the possibility for failure increases exponentially. The only real hope any team has is to embrace network virtualization and micro-segmentation and take back control of their network and ultimately their future.

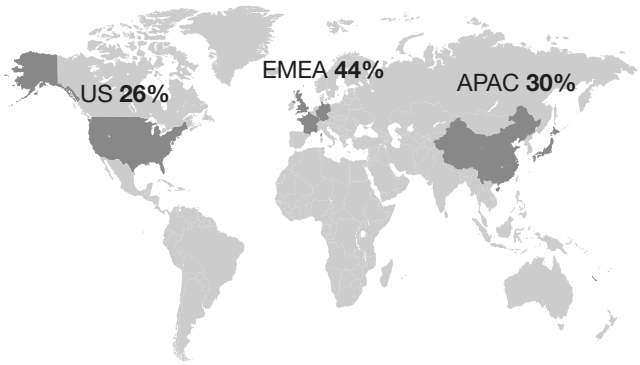
Go virtual, now. Are you planning to move to a more virtual infrastructure in the near future? Stop waiting. Move towards a virtualized network carefully but expeditiously. Stop worrying about how your team can keep up with all the threats that are present today, and instead focus on the needs of your evolving workforce by utilizing the power of virtualization technology sooner rather than later.

Platform is power. The truth of this sector of the market is that you get what you pay for. To really get the "bang for the buck" from your team's investment in virtual technology you need to go with a trusted provider that is a leader in the industry. Only a few vendors can truly claim to be industry leaders for these technologies and techniques. These are the vendors that your team needs to use. Taking the cheaper, homegrown path might sound enticing, but it will lead to longer rollouts and increased expense overall. Spend wisely but spend strategically: Use a vendor that has legacy knowledge and pedigree in this space.

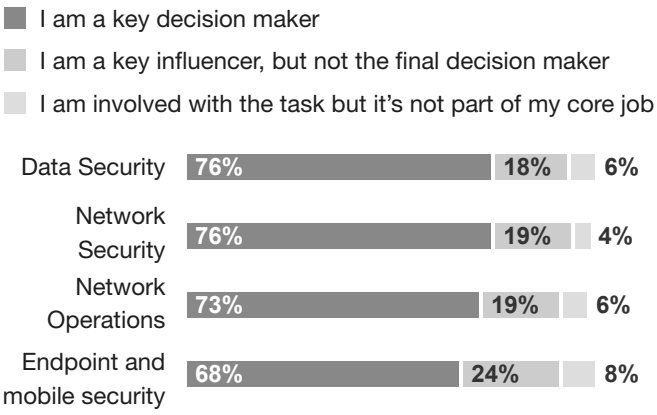
Appendix A: Methodology

In this study, Forrester interviewed 225 IT and risk and compliance decision makers at organizations who have implemented network virtualization or have plans to do so soon. Questions provided to the participants asked about how security in virtualized environments has changed since a similar survey was launched in 2015. Companies surveyed were from the US, UK, Japan, Germany, France, and China and had employee counts of 500 or more. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was completed in November 2017.

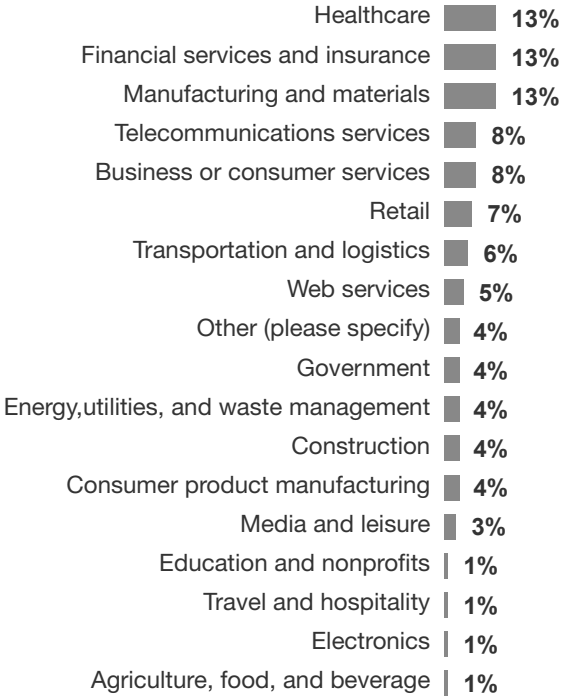
Appendix B: Demographics/Data



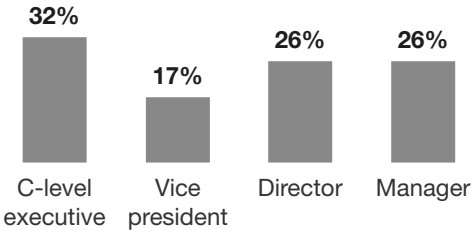
SECURITY AND OPERATIONS INVOLVEMENT



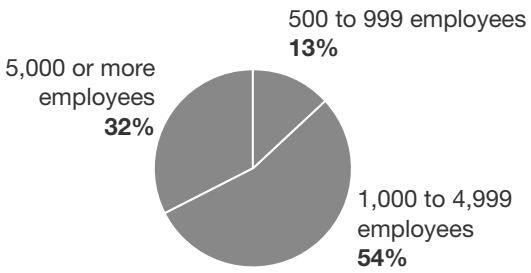
INDUSTRY



RESPONDENT LEVEL



COMPANY SIZE



Base: 225 IT and risk and compliance decision -makers at organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of VMWare, November 2017

FORRESTER®