WHITE PAPER – **FEBRUARY 2018**

HOW MIDSIZE ORGANIZATIONS CAN MEET COMPLIANCE REQUIREMENTS AND ENHANCE CYBERSECURITY WITH MICRO-SEGMENTATION

vmware®

Table of Contents

Few issues are more important to top executives than cybersecurity and compliance. Despite a lot of publicity and attention on how to address those two issues, surveys show there is still much to do. A recent study by Fortinet found that nearly half of senior IT professionals believe their boards and management teams need to do more to protect the organization.[1]

Yet for many small and medium-size enterprise-class organizations, there is a troubling dichotomy: They have all the security and compliance demands of the largest Fortune 500 enterprises but far fewer resources to meet those challenges. As a result, it's critical they choose a security and compliance approach that is more efficient and delivers far more bang for the buck than legacy solutions. The old approach of buying many different and unique security and compliance products that each solve just one problem doesn't work. Further, it adds tremendous complexity and requires a greater number of expensive head count to monitor and manage.

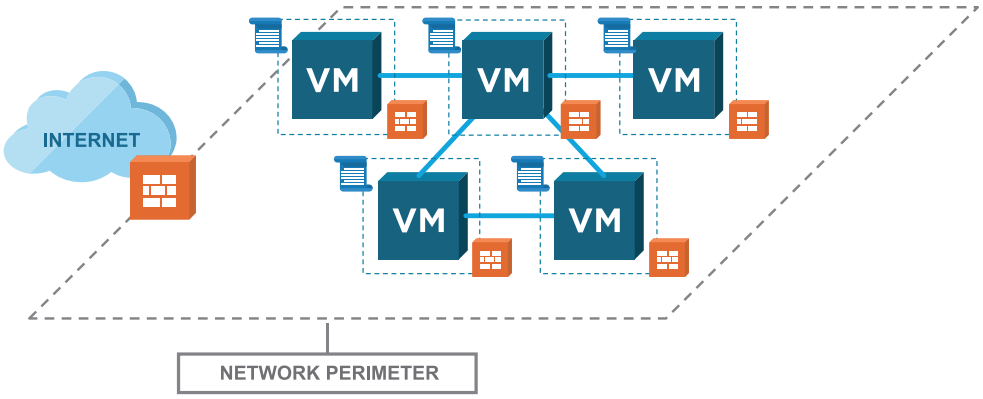
To address the need for improved security and compliance efficiently, many small and midsize enterprises are evaluating and moving toward deploying virtual network technology that supports micro-segmentation, such as VMware NSX. This technology provides a true secure and compliant platform that delivers many of the necessary capabilities to meet both current and future demands. It's a foundational approach that is not only effective, but also highly efficient.

A short technology overview

Although it might seem complex, the technology is straightforward, with network virtualization as the starting point. VMware NSX abstracts all of the underlying network hardware and links via an administrative software platform that is consistent across all aspects of the network. All of the physical network's complexity is represented in the virtual software layer. This simplifies management and operation of the network, and allows any network administrator to easily see the entire network, its traffic, and its performance. Most important, it lets the IT team secure the network in a foundational, holistic way, eliminating different and unique network segment silos that can create blind spots and risks.

Micro-segmentation builds upon the virtual network by allowing the IT team to protect applications by enforcing security policies at the most granular level of the application: the individual workload. This protects your IT resources inside the perimeter firewall. One of the biggest problems with today's cyberdefenses is that once hackers get inside the firewall, there are few defenses to stop them from accessing your most sensitive applications and data. Micro-segmentation provides that protection inside the perimeter, specifically for each application, database or workload.

1 "Fortinet Survey Reveals Almost Half of IT Decision Makers Believe Board Members Still Do Not Treat Cybersecurity as a Top Priority," Fortinet, Oct. 9, 2017



How micro-segmentation solves security and compliance problems

Today's business management teams, particularly those at small and midsize enterprise-class organizations, face stringent and numerous compliance and security demands. In the simplest terms, the organization must ensure secret things remain secret. Micro-segmentation provides a foundation for meeting that goal.

The key security and compliance benefits of micro-segmentation include the following:

- **Separation of zones** — One critical compliance requirement is the separation of "zones," or the need to restrict communications between applications and data that are within the scope of compliance directives and those that are not. Some organizations believe there is physical segmentation of these key systems, but with network sprawl and unplanned additions, this is often no longer true, leaving organizations out of compliance.
- **Elimination of the "boiling the ocean" approach** — Many organizations cannot effectively deploy security and manage compliance by focusing on just the most important systems. Rather, they try to protect or manage everything with a single security or compliance process. That rarely works. With micro-segmentation, compliance and security teams can focus on the most sensitive systems, providing them with better protection.
- **Reduced impact of a cyberbreach** — The older and less effective approach of focusing on protecting the perimeter between internal and external systems is fatally flawed. Once hackers penetrate the defenses, they can now access any system or data. With micro-segmentation, the organization now has defenses inside the perimeter that can stop or disrupt an attacker who has breached perimeter defenses.
- **Consistent security and policy enforcement** — Many of the various compliance directives require that businesses create and consistently apply appropriate security and management policies to protect data and applications. With a highly fragmented network, this is simply not possible—nor cost-effective. Using a virtual network with micro-segmentation, an organization can not only create the policies, but also ensure they are consistently deployed on the network. Further, it is now possible to easily modify and enhance these policies to meet new compliance or security demands.

- **Ability to take advantage of cloud computing faster and with less risk** — Cloud computing offers many new capabilities that are highly attractive to businesses. However, without the proper protection in place, using the cloud can create new compliance and security problems. Virtual networking and micro-segmentation can protect cloud-based resources with the same safeguards as those used to protect on-premises resources. This allows organizations to get the benefit of the cloud without additional risk.
- **Documentation of compliance activities** — The policies and processes that are defined for micro-segmentation are often used as documentation for compliance bodies, proving protection is in place. Proving that the business is implementing processes that are critical to meeting compliance guidelines can be problematic if an organization doesn't have a consistent and comprehensive solution, such as micro-segmentation running on a virtual network platform.

Network virtualization and micro-segmentation provide benefits beyond compliance

The focus of this white paper is on the compliance and security functionality in network virtualization and micro-segmentation. However, there are additional benefits to the organization and its IT team that have zero or marginal cost. These additional benefits are important in that they mitigate the need for other high-cost technology solutions and improve the return on investments in virtual networking and micro-segmentation.

The most noteworthy of these additional features is the disaster recovery capability that is part of the virtual network solution. With a virtual network, it is easy and fast to move workloads from a network that is experiencing downtime to another that is functional. This can be done almost "automatically" to ensure that a network outage doesn't have a large impact. That is an important feature because network outages are now more common due to older networks that are complex, poorly documented and often frail. Not only that, but the complexity of older networks results in longer recovery times. Virtual networks, on the other hand, are hardware-agnostic, allowing the business to use any underlying network hardware and even change it over time.

Another additional capability included with virtual networks is network load balancing. It's essential that an organization be able to identify and remediate situations where one network segment is overloaded and hurting application performance or website performance. Some businesses buy additional products to do this. With a virtual network solution, though, there is no need to incur this expense. Further, using load balancing provided by the virtual network makes operations more efficient, saving staff time and possibly head count.

Finally, the virtual network is a platform for simplifying operations and reducing OpEx. The virtual network provides a single management console for all the network segments, eliminating the need to manage different parts of the network with different tools. This saves network administrators substantial amounts of time. In addition to these time-savings, the virtual network provides a common platform for facilitating the integration of systems operations, security operations and network operations teams. Using the same tools enables them to work together seamlessly and much more efficiently, and to focus on real business priorities, not administrivia.

Virtual networking and micro-segmentation are particularly valuable for midsize enterprise-class companies

Small and midsize enterprise-class companies have all the demands of the very largest Fortune 500 organizations but far fewer resources. As a result, they have to choose technology solutions that are more efficient to own, operate and modify. Network virtualization and micro-segmentation security meet those challenges.

Micro-segmentation is truly a state-of-the-art, modern cybersecurity solution that is designed to mitigate many of the most recent cyberthreats organizations face. And unlike many other security products, micro-segmentation is simple enough that organizations don't have to find and hire the most expensive IT security staff or try to hire the very small number of individuals conversant in the latest technology. Deploying and operating virtual networks with micro-segmentation is not difficult or time consuming.

Another budget-friendly element of virtual networking is that it provides a solution for additional IT requirements without more expense. Getting disaster recovery and load balancing for basically free can save a great deal of budget dollars that can be put to work elsewhere.

Many smaller enterprise-class companies also have limited IT staff. Virtual networking eliminates many of the redundant tasks required to manage unique network segments or installations. There is just one console and one set of management activities. This reduces the scope of operational tasks and lessens demands on network administrators, so organizations can do more with the same level of staffing. Greater staff efficiency and time-savings are also found by improving the collaboration and speed of communication between security, networking and data center teams. A virtual network provides a single consistent platform that all three teams can use, and it acts as the coordinating force for projects that require all three teams to work together.

Finally, virtual networking allows the business to take advantage of the economics and agility of cloud computing faster and with better security. In fact, virtual networks make it easier to adopt cloud services, both public and hybrid, than is possible with most legacy network implementations. Virtual networks foster agility and speed, rather than inhibit it.

Conclusions and key takeaways

As the breadth and demands of compliance directives and cybersecurity protection increase almost daily, businesses must ensure they are meeting the necessary requirements. However, the legacy approach of buying several single-function products to meet the demands is no longer appropriate. The cost, complexity and likelihood of hidden vulnerabilities in the old approach demands new thinking.

Modern approaches such as virtual networking and micro-segmentation technology provide a better and more efficient way to meet these requirements. If you'd like to learn more about this important security and compliance solution, you can refer to:

- The Total Economic Impact™ of VMware NSX
- Micro-segmentation for Dummies, 2nd Edition

These resources will help you better understand and support the move to virtual networks and micro-segmentation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

2/18