SOLUTION OVERVIEW

# SECURE APPLICATION INFRASTRUCTURE

Applying Innovative New Models to Transform Security

## Evolving Threats Require New Security Models

Over the past few years, businesses in every industry have experienced numerous high-profile data breaches that have compromised sensitive information, costing organizations billions of dollars and inflicting immeasurable brand damage. Although the specific methods varied, most breaches employed a common strategy that exposes the fundamental weakness of the perimeter-centric network security model. Traditionally, organizations focused on securing the data center with perimeter firewalls. However, today's modern threats are increasingly penetrating perimeter security and then spreading laterally from server-to-server (east-west).

To attempt to solve this problem, many organizations have deployed an array of point products, creating a complex, disconnected web of systems. These ad hoc solutions are inflexible, difficult to provision, and don't align with the applications they are intended to protect. At the same time, attackers are becoming increasingly sophisticated—while the tools available to them are also becoming more powerful and easier to use, enabling a broader range of actors to carry out malicious attacks.

### Businesses Need Agility to Drive Growth

As organizations seek to accelerate time to market and time to value for lines of business and other internal stakeholders, they also need to control security and manage risk more effectively. It's more important than ever for businesses to not only reduce the risk of a data breach, but also reduce the impact if an issue does occur. However, security and compliance can impact business agility. IT teams may not always have the tools and resources they need to keep pace with the speed of business operations while maintaining infrastructure security.

### IT Needs Both Security and Agility

To meet business leaders' expectations, IT organizations must be able to deliver the necessary services and applications quickly, yet securely. However, as they strive to secure the business, IT teams face numerous obstacles, including:

- Changing application architectures, from on-premises monolithic applications toward distributed applications and microservices
- Lack of visibility and context of network traffic
- Rigid, perimeter-centric security models and policies
- Difficulty in achieving, maintaining, and demonstrating compliance

**SECURITY THREATS ARE SERIOUS BUSINESS**

- Cybercrime represents the fastest growing cause of data center outages, rising from 2 percent in 2010 to 22 percent in 2016.[1]
- The cost of global cyber espionage is approximately $500 billion annually, hitting $1 Trillion, if the costs associated with stolen intellectual property are included.[2]
- The average cost of a data breach rose to $4M in 2016, or $158 per lost or stolen record.[3]

[1] Cost of Data Center Outages, Ponemon Institute, January 2016

[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/

[3] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, June 2016

## Abstracting Applications from Infrastructure Delivers Advantages

To address these problems, organizations need to fundamentally transform the way they secure the application infrastructure. VMware offers a complete portfolio of solutions that enable IT to deploy a virtualized platform, which abstracts their infrastructure from the applications running on top of it—whether that infrastructure is on-premises or in the public cloud. With VMware vSphere® and VMware NSX®, organizations can take advantage of flexible, robust virtualization platforms to support their new and existing apps—without compromising security and compliance. VMware vRealize® Network Insight™ enhances their capabilities through enterprise-ready cloud management for additional visibility and protection.

### Three Fundamentals to Securing the Application Infrastructure

Employing a fresh approach to securing the application infrastructure lets IT organizations position themselves to take advantage of several powerful capabilities:

#### *Abstraction of Applications from Infrastructure*

Abstracting applications from infrastructure unlocks full visibility into the application data path, for a better understanding of traffic patterns. It lets IT dramatically increase contextual understanding of how infrastructure and applications interact with one other as well as with data. With a complete and unified view of data, applications, and infrastructure, organizations can create policy and respond to threats more effectively.

#### *Granular Application-Aligned Security Policy*

A virtualized approach lets organizations closely align security policy to the applications they are meant to protect, and follow them as they move across public and private clouds. It enables network micro-segmentation to prevent the lateral spread of threats (from east to west) between workloads and applications. And it makes it easier to intelligently insert third-party security services into the platform when new capabilities are needed.

#### *Hypervisor-Based Infrastructure Protection*

A model that abstracts applications from the underlying infrastructure also provides an ideal point within the infrastructure to protect against compromising the infrastructure itself. Organizations can protect data at rest through workload-level encryption on each hypervisor host. And they can encrypt data in flight to mitigate the risk of compromised networking components like routers and switches.

## A Portfolio of Solutions to Secure Application Infrastructure

No matter where organizations are on the virtualization journey, VMware offers them industry-leading solutions that enhance application security environments.

### VMware vSphere

To protect critical business resources in a virtualized environment, organizations need streamlined administration and operationally simple, policy-driven security capabilities.

VMware vSphere, the industry-leading virtualization platform, provides a powerful, flexible, and secure foundation for business agility that helps organizations accelerate the digital transformation to cloud computing. The solution supports both existing and next-gen apps through its simplified customer experience for automation and management at scale; comprehensive built-in security for protecting data, infrastructure, and access; and universal app platform for running any app, anywhere. With vSphere, organizations can run, manage, connect, and secure their applications in a common operating environment, across clouds and devices.

VMware vSphere includes rich security features that help organizations protect their environments and mitigate issues if a breach does occur.

- Security-at-Scale—Policy-driven security makes securing infrastructure operationally simple.
- Encryption—VM-level encryption protects unauthorized data access both at rest and in motion.
- Audit-quality logging—Enhanced logging provides forensic information about user actions.

An ecosystem of leading third-party vendors also provides enhanced security support for VMware NSX.

### VMware NSX

To provide protection against today's sophisticated threats, organizations need a virtual network environment that lets them divide the data center into logical segments.

If an attacker penetrates data center perimeter defenses, it's critical to keep the threat from moving laterally within the data center. A virtualized approach lets IT teams define security policies for each workload, based on dynamic security groups, so they can respond immediately to threats inside the data center. VMware NSX is the network virtualization platform that delivers the operational model of a virtual machine for the data center network. With VMware NSX, organizations can programmatically create, snapshot, store, move, delete, and restore entire networks with the same point-and-click simplicity and speed of a virtual machine—delivering a level of security, agility, and availability that was unavailable with hardware-centric or traditional operational approaches. The solution lets organizations enforce security policies down to the individual virtual machine level.

VMware NSX supports organizations that want to unleash the security and performance advantages of virtualization. Key capabilities include:

- Security—Embedded security functions within the hypervisor, delivering micro-segmentation and granular security to the individual workload.
- Automation—Network and security services are attached to workloads using a policy-driven approach, for automation and improved performance.
- Application Continuity—Networking is abstracted from the underlying hardware and attaches networking and security policies to their associated workloads.

### vRealize Network Insight

To manage a heterogeneous, hybrid cloud environment, organizations need an enterprise-ready cloud management platform that's purpose-built for the environment.

vRealize Network Insight delivers intelligent operations for Software-Defined Data Center (SDDC) networking and security, with converged visibility across virtual and physical networks, and provides micro-segmentation planning recommendations and operations management for VMware NSX.

vRealize Network Insight provides a wide range of features that can help organizations optimize security.

- Visibility—Provides converged visibility across overlay and underlay, virtual and physical, private and public cloud, with integration between virtual and physical layers.
- Micro-segmentation Modeling Application Behavior—Enables users to easily understand who is talking to whom—and what flows need to be allowed or blocked.
- Audit and Compliance—Tracks all changes for audit and compliance purpose.

## Secure Application Infrastructure with VMware

Today's IT organizations are facing unprecedented challenges driven by digital transformation and a fast-changing threat landscape. In this dynamic environment, it's more important than ever to partner with a proven technology vendor to help ensure that business operations stay safe. Coalfire, an independent cyber risk management advisor and assessor, recently recognized VMware's capabilities in its benchmark report. The report concluded that the VMware NSX product "provides granular level security policy control and traffic visibility that operationalizes security and enables clients to meet regulatory compliance requirements." [4]

VMware helps organizations transform their approach to security through a ubiquitous software layer across application infrastructure. By abstracting the infrastructure from the applications that it supports, VMware enables IT to extend its visibility into the data path, for better insight and control. Together with micro-segmentation, the solution helps organizations simplify security policy and better align protection to meet the needs of specific applications. VMware does it through a broad choice of security and virtualization solutions, backed by an extensive partner ecosystem. With a robust security and compliance solution in place, organizations can free their IT teams to focus on driving growth and innovation across the business.

### LEARN MORE

Learn more about additional IT priorities and IT initiatives at vmware.com/it-priorities/transform-security.

[4] "Micro-segmentation Cybersecurity Benchmark Report", September, 2016, Coalfire

vmware®

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

5/17