TRANSFORM SECURITY

A Strategic IT Priority

Security Is Top of Mind for Every Business

As people, devices, and objects become more connected, protecting all these connections and environments have become more critical than ever. IT organizations need to secure each and every interaction between users, applications, and data—however and wherever they are connecting. They need to do it in an environment that is constantly changing, and increasingly dynamic.

Security risks are high for businesses in every industry, and they are continuing to escalate. According to a recent study, the average total cost of a data breach increased from $3.52 million to $3.79 million in just one year.[1] For organizations that are embracing cloud and virtualized environments, maximum visibility and control are key to mitigating this risk.

THE STAKES ARE HIGH FOR SECURITY

Cybercrime represents the fastest-growing cause of data center outages, rising from 2 percent in 2010 to 22 percent in 2016.[2]

Average cost of a data center outage rose to $740,357 in 2016.[3]

Changing IT Needs in a Dynamic Threat Landscape

Every business has become a digital business, and this transformation has led to significant changes to the IT landscape. Application infrastructures have evolved from on-premises data centers running physical infrastructure, to highly dynamic environments that reside on public and private clouds.

Applications themselves are changing, too. Organizations are moving away from monolithic application stacks to distributed, multi-tiered apps based on microservices. As the workforce becomes more mobile and distributed, end-user environments are evolving as well. They are no longer limited to corporate-managed desktops, but are centered around mobile devices, Bring Your Own Device (BYOD) initiatives, and the Internet of Things (IoT).

For IT, traditional network perimeter security models are no longer sufficient to protect a fast-growing sprawl of applications and users, and meet escalating compliance requirements. Environments and users aren't neatly contained behind perimeter firewalls, but require more flexible, agile protection. Attackers are more sophisticated, and cyberspace has become increasingly weaponized. Today, using toolkits like Zeus and BlackPoS, even an inexperienced hacker can target a business with advanced attacks that can do real damage to its productivity, resources, and reputation.

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

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

[3] Ibid.

Effective Security Spans Multiple Areas

Protecting an organization with a robust, compliant security solution isn't easy when the infrastructure and its users are rapidly changing. The old ground rules of network security simply don't apply anymore, and IT teams need to keep pace with:

- Changing infrastructures—The infrastructure used to run applications such as web and database servers is evolving from on-premises environments to support cloud and distributed apps.
- Increasing mobility—IT needs to expand its security policies to support a flood of new devices and models.
- Escalating compliance—The regulatory compliance environment has become increasingly complex as organizations face new requirements.

VMware enables IT to transform security environments and operations to meet today's challenges. Here's how:

- **Secure Application Infrastructure –** Abstract infrastructure from applications, improving visibility and better aligning security to apps.
- **Secure Identity and Endpoints –** Employ a ubiquitous software layer across all users and endpoints for better visibility and control, without impacting the user experience.
- **Streamline Compliance –** Apply software across the app infrastructure, identity, and endpoints to simplify compliance.

Deliver Visibility and Context to Transform Security

VMware can help organizations achieve the insight they need to stay ahead of their changing security needs. At the heart of VMware solutions is a ubiquitous software layer across application infrastructure and endpoints that's independent of the underlying physical infrastructure or location. This approach puts VMware software in a unique position within the infrastructure to provide IT with deep visibility into every interaction between users and applications. Just as importantly, it offers context to understand what those interactions mean. Together, this visibility and deeper context enable organizations to better align their security controls and policies to the applications they are protecting.

Effective security requires multiple layers of protection, and VMware's location within the infrastructure provides the best possible control point for IT to enforce policy and insert third-party services for additional intelligent protection.

Secure Application Infrastructure

As application infrastructure models evolve, the traditional perimeter-centric network security approach cannot provide enough visibility and control inside the data center. At the same time, stored data at rest has become a much more valuable target for attackers. To address these problems, organizations need to transform the way they secure their application infrastructure.

The solution starts with virtualization and the ability to abstract the underlying infrastructure from the applications running on top of it—whether that infrastructure is on-premises or in the public cloud. This layer of abstraction provides full visibility into the data path and an ideal enforcement point to compartmentalize applications through micro-segmentation of the network. Employing micro-segmentation in software lets organizations simplify security policy, and align it more closely to the application needs. It also lets the policy follow the application as it moves across private and public clouds. And an abstraction layer provides a platform for IT to insert additional third-party services for more advanced security protection.

Micro-segmentation helps IT prevent security threats from breaching defenses by enabling the principle of application-centric least privilege, which reduces the infrastructure's attack surface.

An abstraction layer between applications and the underlying infrastructure not only helps IT avoid attacks; it provides an ideal point to encrypt stored data. By encrypting data at rest, at the workload level, organizations can ensure that application infrastructure data is safe, even if it falls into the wrong hands.

"With VMware NSX®, we now make critical patient data more readily available to hospital medical professionals and to patients while keeping it segmented and secure."

CHRISTOPHER FRENZ
DIRECTOR OF IT INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

Secure Identity and Endpoints

As businesses go digital, mobile devices are proliferating fast. Organizations are employing devices based on everything from Android and iOS to Windows and macOS to empower their workforce and re-imagine traditional business processes. Supporting all these devices and platforms is challenging, especially as companies embrace enterprise mobility, BYOD, and IoT initiatives.

VMware helps IT address this challenge by applying a ubiquitous software layer across all users and endpoints to verify user identity and device posture. This approach provides end-to-end visibility and control of the user and endpoint, extending all the way into the data center or cloud, where the application infrastructure resides. VMware software lets IT add an adaptive, conditional layer of security at each transactional level, from the user to the resources they're accessing. It helps secure corporate data and reduce the cyber-attack surface, without impacting the user experience.

Organizations can employ a single VMware solution to protect all their endpoints, including smartphones, tablets, laptops, wearables and IoT devices. It enables IT to seamlessly deploy any app—including native, web, remote, virtual apps and Windows desktops—through a single app catalog with built-in single sign-on, data security, and endpoint compliance. Built for today's dynamic workspaces, the VMware solution also lets businesses extend security beyond the virtual desktop interface (VDI) and mobile endpoints into the data center with micro-segmentation.

Because every business has specific security needs, the solution helps organizations customize their environments to align with their priorities. It delivers a foundation for VMware's security partners, who can leverage the visibility and control points the VMware solution provides to complement the solution with their own service offerings.

Streamline Compliance

Managing risk and maintaining continuous compliance is always a major concern. It's especially important for industries such as financial services, government, and healthcare, in which organization face strict requirements such as PCI, FISMA, HIPAA and more. Regulations and requirements are growing, while the digital landscape and advanced persistent threats continue to evolve, making it more difficult than ever to ensure and demonstrate compliance.

To complicate matters, organizations are rapidly transitioning from on-premises data centers and adopting the cloud, making it even more challenging to meet business, regulatory, and policy demands.

VMware provides a ubiquitous software layer across application infrastructure and endpoints, taking a holistic approach to compliance. This unique approach provides an ideal location to implement compliance controls, and gain the visibility necessary to demonstrate compliance. The solution provides a technology platform in which IT can dynamically insert validated tools and services from VMware ecosystem partners to further streamline the compliance process.

A Compliance Reference Architecture Framework from VMware links integrated software and hardware capabilities and specific regulatory controls with independent audit validation. Organizations can leverage this independently validated program to securely run highly regulated workloads. Whether they are employing a private or public cloud environment, organizations can rest assured

LEARN MORE

Learn more about this strategic IT priority and its corresponding IT initiatives at vmware.com/it-priorities/transform-security.

that they remain continuously compliant. VMware delivers the speed, efficiency, and agility that businesses demand, while streamlining the compliance process for the organization.

VMware Delivers Security for a Changing Landscape and Needs

Robust security has always been essential for business networks, and as the pace of digital transformation accelerates, it's more necessary than ever. As traditional infrastructure, applications, and workforce models evolve, IT is under increasing pressure to protect the business from emerging new threats.

VMware enables organizations to transform security by providing a ubiquitous software layer across application infrastructure and endpoints. It lets organizations maximize the visibility and context of the interaction between users and applications, so they can align their security controls and policies to the applications they are protecting. And VMware makes it easy for them to complement their solution with third-party security services for additional intelligent protection.

vmware®

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

1/17