TRANSFORM HEALTHCARE SECURITY

Increase protection in a dynamic threat landscape

The protection of patient information is top of mind for every healthcare organization. As people, devices, and objects become more connected, a compromised connection in one system can negatively impact the bottom line and customer loyalty of a trusted brand. Healthcare information technology (HIT) organizations need to secure every interaction between users, applications, and data—however and wherever they are occurring—in increasingly dynamic environments.

A Ponemon Institute report revealed for six years in a row, data breaches in healthcare were consistently high in terms of volume, frequency, impact, and cost. Nearly 90 percent of healthcare organizations represented had a data breach in the past two years, and nearly half, or 45 percent, had more than five data breaches in the same time period. Based on the study, breaches could be costing the healthcare industry a walloping $6.2 billion.[1] For healthcare organizations embracing cloud and virtualized environments, maximum visibility and control are key to mitigating risk.

"Using VMware software allows us to lessen the risk and keeps us compliant, keeps our sacred trust of keeping patient information safe."

BRENDA WILLIAMS
VP OF TECHNOLOGY SERVICES
MOSAIC LIFE CARE

Changing IT Needs in a Dynamic Threat Landscape

Patient care is quickly becoming digital—transforming healthcare organizations into digital businesses. This disruption has led to significant changes in the IT landscape, for example, applications becoming cloud-native, application infrastructures evolving from on-premises data centers to public and private clouds, and the introduction of the digital workspace.

Healthcare organizations are moving away from monolithic application stacks to distributed, multi-tiered apps based on microservices for greater agility. As caregivers and patients become more mobile and distributed, end-user environments can no longer be limited to corporate-managed desktops, but must be centered around PCs, tablets, Bring Your Own Device (BYOD) initiatives, and Internet of Things (IoT) sensors.

For HIT teams, 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 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 hospital with advanced ransomware that can do real damage to productivity, resources, and reputation.

[1] Ponemon Institute. "Nearly 90 Percent of Healthcare Organizations Suffer Data Breaches, New Ponemon Study Shows," May 12, 2016.

Effective Security Spans Multiple Areas

Protecting a healthcare 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 on physical infrastructure is evolving to highly dynamic environments that reside on clouds and manage distributed apps.
- Increasing mobility—Requirements now include adding 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.

Deliver Visibility and Context to Transform Security

VMware enables healthcare organizations to achieve the insight they need to stay ahead of their changing security needs. At the heart of VMware's comprehensive and transformative security solution 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 HIT teams 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 healthcare 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, HIT staff 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 HIT 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 HIT staff avoid attacks; it provides an ideal point to encrypt stored data. By encrypting data at rest, at the workload level, healthcare organizations can ensure that application infrastructure data is safe, even if it falls into the wrong hands.

Next-generation healthcare provider **Mosaic Life Care** sought a way to ensure its entire organization participated in security while enabling providers to have access to the data they needed to provide the highest quality patient care. It deployed VMware solutions to meet regulations and reduce risk by enabling a secure environment as it introduced alternative methods of providing urgent and minor health care to the population it serves, including using a mobile bus in parking lots for portable service and top-notch telemedicine services with small and large providers in the private and public sectors.

Secure Identity and Endpoints

As healthcare goes digital, mobile devices are proliferating fast. Healthcare organizations are employing devices based on everything from Android and iOS to Windows and macOS to empower caregivers and patients with the goal of improving care outcomes. Supporting all these devices and platforms is challenging, especially as HIT staff embrace enterprise mobility, BYOD, and IoT initiatives.

VMware helps HIT teams 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 HIT staff 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 caregiver or patient experience.

Healthcare organizations can employ a single VMware solution to protect all endpoints, including smartphones, tablets, laptops, wearables and IoT devices. The solution enables HIT staff 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. Purpose-built for today's dynamic workspaces, the VMware solution also lets HIT teams extend security beyond the virtual desktop infrastructure (VDI) and mobile endpoints into the data center with micro-segmentation.

Because Healthcare has specific security needs, including compliance with the U.S. Healthcare Insurance Portability and Accountability Act (HIPAA) and National Institute of Standards and Technology (NIST) requirements, the solution helps customize environments to align with priorities. It delivers a foundation for VMware's security partners, who leverage the visibility and control points the VMware solution provides to complement the solution with their own service offerings.

For example, **Interfaith Medical Center** used VMware transformative security technologies to provide the most advanced security posture for the hospital to share medical information via a patient portal, meet NIST compliance regulations, and prepare for the increasing use of IoT to enable connected medical devices.

Streamline Compliance

Managing risk and maintaining continuous compliance is always a major concern. It's especially important for healthcare where regulations and requirements are increasing, 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, healthcare organizations are rapidly transitioning from on-premises data centers and adopting the cloud.

VMware, with a ubiquitous software layer across application infrastructure and endpoints, takes a holistic approach to compliance. This unique model 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. Healthcare HIT 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 that they remain continuously compliant. VMware delivers the speed, efficiency, and agility that healthcare businesses demand, while streamlining the compliance process for the organization.

Teaming with VMware on Transformative Security

Robust security has always been essential for healthcare. As traditional infrastructure, applications, and patient care models evolve, HIT teams are under increasing pressure to protect environments from emerging new threats. VMware enables healthcare organizations to transform security by providing a ubiquitous software layer across application infrastructure and endpoints. It helps healthcare organizations maximize the visibility and context of the interaction between users and applications, so they can align security controls and policies to the applications they are protecting. VMware also makes it easy to complement the solution with third-party security services for additional intelligent protection.

Learn more at https://www.vmware.com/go/healthcare.

vmware®

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