Unifying Cybersecurity in Healthcare

The end-to-end approach to protecting your agency—across any app, any network, and any device

Introduction
With the rise of digital healthcare, cybercriminals don’t have to look very hard for new places to attack. Telemedicine, EMRs, cloud services, and the use of intelligent devices are all creating more potential entry points for threats. The result is that cyber attacks are increasingly common, with breaches growing in terms of quantity and damage. Studies found that in 2019, there was a surge of ransomware attacks on healthcare providers, with 764 notable attacks.¹

The bad news is that the healthcare sector is highly vulnerable, and the bad actors are taking note. In fact, 61% of cyberattacks target healthcare organizations.² Many providers and payers may be even more at risk due to a patchwork of legacy systems and limited IT budgets.

Meanwhile, when it comes to security solutions, the complexity is higher than ever. Thousands of security vendors promise to have the silver bullet for security, and the landscape is awash with a multitude of products and agents to address different threat vectors. Security and IT teams make their decisions in silos—and with no big-picture view of the environment they’re trying to protect. It’s beyond time for a unified approach.

This white paper will explore why cybersecurity needs to be a team sport, aligning your people, processes, and technology to defend against the latest security threats. We’ll look at the key elements needed for a unified approach, and how the comprehensive security platform from VMware can help.

Security Challenges in the Healthcare Industry
Cybersecurity threats are growing across every industry, but the stakes are even higher in healthcare where patients’ lives could be at risk. Strict government regulations are in place to help protect the privacy of patient information. However, an expanding network of medical devices and end-user services are also vulnerable to attack. The unique security challenges in healthcare span from implantable devices in patients, to ensuring real-time access to data for improving patient outcomes.

Yet, healthcare security professionals can often feel unsupported in their security initiatives. A recent survey showed that 51% of respondents need more budget for security solutions, with 44% reporting a need for a more coherent enterprise approach. Their greatest technical challenge is managing the proliferation of systems and end-user devices. In fact, 40% of healthcare respondents said they have experienced password phishing among their end-users, along with other identity and access issues.³

Unifying Cybersecurity in Healthcare

As attacks grow nationwide, healthcare providers are faced with lots of complexity in securing their infrastructure. Disparate products, agents, and interfaces make it difficult to manage vulnerabilities. The solution sprawl can create more overhead that impacts performance. What’s more, key decisions are made by siloed IT and security teams, reacting to threats without a holistic view of the applications, data, infrastructure, and devices that they’re trying to protect. Network security is approached differently from endpoint security, which is different from cloud security, and so on.

The interesting thing is that IT and security teams are aligned on the greater goals of preventing breaches, increasing efficiency, and speeding incident resolution. The teams just don’t work together very well. According to a recent Forrester study, 77.4% of respondents said their IT and security teams currently have a negative relationship.¹

What’s the solution?

Strengthening Security with a Unified Approach

To strengthen your cybersecurity posture, your entire healthcare organization needs to approach security like a team sport. It’s more important than ever to have unified visibility and control across your critical networks, workloads, and endpoints. Your busy IT and security teams need to be able to work together, using a single source of shared truth. The only way to stay ahead of ever-changing threats is with a unified platform—enabling you to zero in on vulnerabilities and mitigate them, before any damage can occur.

Following are three key tactics for building an effective security playbook.

Tactic #1: Security needs to be built-in, not bolted on

Too often, security is approached like a game of “whack-a-mole,” with isolated solutions being deployed in response to the latest threats. Many organizations have dozens of security solutions that require independent configuration and monitoring.

For maximum effectiveness, security should be built into the infrastructure you already have, creating a superior vantage point for threat detection. Your organization should be able to unite around a single platform—with a holistic view—reducing the number of security products, agents, and interfaces that your teams need to manage, and lowering the chances for error. With distributed firewall rules, you can protect against lateral vulnerabilities as well as north-south threats, whether running applications in VMs, containers, or bare metal. Built-in integration across control points also provides even greater control.

Tactic #2: Security needs the context of what you’re trying to protect

With growing technology risks and evolving mandates facing healthcare providers and payers, a defensive cybersecurity strategy is a must. It’s vital to stay informed about the latest threats and vulnerabilities. But your security policies are more effective if you also have deeper visibility into your applications and data—and what’s “normal” behavior. That way, you can detect anomalous behavior before it can become a threat.

Consider if your security solutions include real-time device assessment and remediation, endpoint detection and response, application control, and support for proactive regulatory compliance. This helps keep EMRs and physician endpoint devices secure, even if BYOD. You can reduce HIPAA and HITECH risks as well as

TOP 5 CYBERSECURITY BEST PRACTICES

1 A baseline security assessment is critical for knowing where vulnerabilities exist, whether you opt for a baseline “Red Team” or “Purple Team” audit and/or cyber hunt exercise. Penetration tests and general audits are also recommended.

2 Network microsegmentation is an ideal strategy for limiting lateral movement across the network. Microsegmentation divides your data center into distinct security segments, reducing the reach of an attack if one occurs.

3 Endpoint detection and response technology, along with application control (whitelisting) on critical servers, can help detect and remediate advanced attacks. Overall, endpoints are the easiest attack surface for hackers.

4 Integration of third-party threat analysis puts your organization in an active position, rather than reactive, and goes well beyond simply responding to alerts. Trusted user communities can also help you get an edge on cybercriminals.

5 Security training and recruitment/retention of talent helps ensure your organization can stay protected, while also knowing how to remediate vulnerabilities.

¹ According to a recent Forrester study, 77.4% of respondents said their IT and security teams currently have a negative relationship.
Unifying Cybersecurity in Healthcare

data loss with context-aware control of sensitive data—restricting where it can be accessed or printed. Continuous diagnostics and monitoring are vital for protecting against external attacks. Plus, your solutions should be backed by real-time threat intelligence that suppresses intrusions before they can be deployed.

Tactic #3: Security needs flexibility to support your unique mission
Every healthcare organization has its own unique goals, needs, and challenges. Taking a “one-size-fits-all” approach to security simply won’t work. Ideally, your organization should have flexible choices for a security stack and prevention protocols. Security solutions need to be effective for your specific workloads, endpoints, networks, clouds, and identity policies—so you can harden potential entry points and proactively immobilize threats.

Your security solutions should also prioritize ease of use and integration. This enables you to break down silos between security and IT teams, while improving visibility across a fragmented IT infrastructure. Whether you need to streamline internal processes or expand telemedicine services, an extensive partner ecosystem is also essential for making the most of your existing security and technology investments.

Transform Security with VMware
In a world of ever-changing threats, VMware is the right partner for protecting your healthcare providers, payers, and patients. VMware helps unify your teams with a comprehensive security portfolio, now including VMware Carbon Black. We provide you with a complete platform approach for continuous diagnostics and mitigation—delivering end-to-end visibility, protection, and system hardening across the network, data center, and endpoint hosts.

Find out how to secure your critical applications, users, and devices, backed by leading threat detection and response capabilities, and be better prepared for what’s next.

Sources

LEARN MORE

Join us online: Twitter Facebook LinkedIn

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-0420-2196_CarbonBlack_HC_1.3_MMT S/19