WHITE PAPER

WHITE COATS AND WHITE HATS—WORKING TOGETHER TOWARDS A UNIFIED APPROACH TO SECURITY AND DATA PROTECTION

TRANSFORMING CYBERSECURITY IN HEALTHCARE
# TABLE OF CONTENTS

White coats and white hats............................................................................................................3

A MATTER OF PATIENT SAFETY ................................................................. 3
  WannaCry warning..........................................................................................................................3

A HIGH-VALUE, HIGHLY VULNERABLE TARGET ........................................... 4
  Valued information.....................................................................................................................4
  Many attack vectors..................................................................................................................4
  Complex ecosystems..................................................................................................................4
  The human factor......................................................................................................................5
  Limited resources.....................................................................................................................5

CYBERSECURITY AS A HEALTHCARE ENABLER ........................................ 5
  Stakeholder collaboration........................................................................................................5
  Parallel progress .....................................................................................................................6
  Connected device safety..........................................................................................................6
  Using technology to protect technology................................................................................6
  Designed in ..............................................................................................................................7
  Virtual advantage....................................................................................................................7
  Proactive, intelligent security operations ................................................................................8

EVERYONE’S JOB: PATIENT SAFETY ............................................................. 8
  Holistic, mission-driven strategy .............................................................................................8
  Unified risk management .........................................................................................................8
  Broad stakeholder participation ...............................................................................................8
  Multilayered security ...............................................................................................................9
  Triage and good hygiene .........................................................................................................9
  Prepare for the worst ...............................................................................................................9
  Put on a white hat ...................................................................................................................9
Medical technology has never been more powerful. It’s also never been more vulnerable. Rapidly evolving digital technologies are bringing unprecedented promise—and risks—to healthcare data. As a result, there is growing urgency for new approaches to cybersecurity that will enable the best possible care while protecting patient safety.

Keynote speaker Jeff Tully, MD, at the first ever CyberMed Summit held this past summer at the University of Arizona College of Medicine, put it this way: “We have incredible medical technology that allows us to care for our sickest and most desperate patients, and we are so thankful for that. It has saved countless lives, with the promise to save even more—and maybe, one day, even eradicate disease.” But he noted, “This incredible gift doesn’t come without costs.”

The message of the summit was simple: the healthcare industry must be able to protect patients against cyberattacks, and doing so will take the concerted efforts of many.

**White coats and white hats**

Dr. Tully, who wears a white coat as a pediatrician, is also a "white hat" hacker. In contrast to "black hat" hackers, who seek to exploit vulnerabilities to steal or do harm, Tully probes medical technology and systems for weaknesses in order to strengthen them. He and his colleague Christian Dameff, MD, an emergency medicine physician, have been working together for years to raise the alarm about the risks to patient safety in increasingly connected and digital healthcare delivery. They are working to help identify threats by also collaborating with a wide variety of stakeholders.

Patients too are playing the role of white hats by hacking to uncover and publicize potential safety issues. Type 1 diabetic Jay Radcliffe made news in 2011 when he successfully hacked into his own insulin pump. More recently, security researcher Billy Rios, after emergency surgery, found himself connected to the very type of intravenous drug infusion pump he had begun investigating. The pumps, with their dosage limits and alerts, are designed to help reduce the risk of medication errors in hospitals. But Rios showed he was able to hack into online dosage libraries remotely to change dosage levels—a vulnerability that could lead to serious or even fatal harm through under- or overmedication. And by hacking into the pump’s display, he could force the device to falsely show that the correct dose was being delivered. According to the manufacturer, they have since taken measures to address these issues, but the vulnerabilities raise a new kind of alarm.

A MATTER OF PATIENT SAFETY

As you can see in both of these examples, there is growing recognition in the healthcare ecosystem that the very digital infrastructure and connectedness that enable more effective and efficient care also expand risk, and the consequences of a security breach in healthcare go beyond theft of identity or personal data. The more critical issue is safety; compromised data or devices can put a patient at risk.

**WannaCry warning**

“There needs to be a higher degree of vigilance among boards and executive suites as attacks become much more sophisticated, especially as doctors need to share information to improve quality and as connected medical devices and wearables proliferate,” says KPMG Healthcare Advisory Leader Dion Sheidy. “The WannaCry ransomware hack in May was a warning shot against our collective ability to protect patient safety and privacy.”
As a result of the attack, unavailable or blocked access to data forced providers to postpone patient procedures.\(^\text{5}\) Other recent ransomware attacks targeting healthcare facilities have led to similar blocked access to medical records, pharmacy data, lab results, and imaging scans.

"In the event a cyberattack is shown to cause physical harm, hospitals will be scrambling to usher in a new era of healthcare cybersecurity," says Dr. Dameff. "That's not the time to do it. The time to do it is now."

**A HIGH-VALUE, HIGHLY VULNERABLE TARGET**

A number of factors make healthcare both an attractive and a soft target for cyberattack.

**Valued information**

Hospitals and healthcare facilities store and share large amounts of personally identifiable health and financial data, which is especially lucrative for hackers. On average, hackers can sell credit card numbers for 10 to 15 cents each but a medical record could be worth anywhere between $30 and $500.\(^\text{6}\) Hackers have also found an even more lucrative value stream with ransomware—holding data hostage until a ransom is paid. Not surprisingly, healthcare data has become the most desired information sought by hackers.\(^\text{7}\)

**Sophisticated threats**

The number and sophistication of cyberattacks targeting healthcare keep growing.

- **90%** of healthcare organizations reported at least one data breach in the past two years, and almost half experienced five attacks or more.\(^\text{7}\)
- **320%** more hacking attacks targeting providers in 2016 vs. 2015.\(^\text{5}\) and in 2017, healthcare data breaches have become an almost daily occurrence.\(^\text{2}\)

Experts predict there will be a 4-fold increase in the number of ransomware attacks targeting healthcare by 2020.\(^\text{10}\)

Despite widespread warnings, **63%** of breaches exploited weak or stolen credentials, and **30%** of phishing messages were opened by the targets last year.\(^\text{7}\)

**Many attack vectors**

Healthcare information systems present a broad attack landscape with multiple attack surfaces and vectors, especially with over 80% of medical records now digitized.\(^\text{12}\) Areas of concern include:

- **Electronic medical record (EMR) systems:** Vulnerabilities include publicly available application program interfaces (APIs), increased integration with other applications to improve workflow, and access by multiple people in multiple roles using many different types of devices. EMR applications typically run on many servers in flat networks and may have numerous inbound ports open at any point in time.

- **Black box medical devices:** A rapidly growing medical device market finds many entrepreneurs competing, focused on delivering purpose-built functionality, typically with nonstandard software. According to a Ponemon Institute study, only 17% of these medical device makers that were surveyed take significant steps to prevent attacks.\(^\text{15}\) With this in mind, there may be medical devices that remain black boxes to hospitals that have limited capabilities to monitor or control for malware threats or that have limitations in patch/upgrade methodologies. Older medical equipment, such as MRIs, never intended to be Internet-accessible, need to also be considered within the context of today’s cybersecurity environment. In the same Ponemon report, results indicated that only 9% of manufacturers and 5% of health delivery organizations test medical devices at least once a year.\(^\text{13}\)

- **Growing IoT:** With the Internet of Things (IoT), the endpoint threat extends beyond medical devices and IT infrastructure. Connected sensors and building systems are all vulnerable. It’s worth noting that a recent attack at a large healthcare system did not just affect computers, but MRI machines and storage refrigerators as well.\(^\text{5}\)

**Complex ecosystems**

Healthcare in the United States involves a complex ecosystem incorporating players ranging from health systems to individual physician practices and includes public and private payers, public and private research institutions, pharmacies, laboratories, and many types of contractors, device manufacturers, and health IT providers. Adding to the complexity are federal, state, and local agencies with overlapping laws and regulations.

As healthcare extends digital interoperability to improve care coordination and efficiency, risk management must expand to consider all stakeholders involved in a patient-care episode that may stretch beyond an organization’s control.
The human factor
A recent Identity Theft Resource Center (ITRC) data breach report identified human error / negligence / improper disposal as the second biggest reason for data breaches across all industries, including healthcare. The number of people—patients, families, visitors, clinicians, support-function teams, staff, vendors, volunteers—in involved in daily care is enormous. The potential sources of compromise range from good intent to bad, from error to manipulation, including passwords written on sticky notes, unlocked and unattended workstations, mistakenly sending files to the wrong recipients, third parties that have access to patient data that may not have the same level of security controls, email phishing hacks aimed at healthcare staff, and even disgruntled employees or contractors with access to sensitive data or devices.

Black-hat-turned-white-hat hacker Kevin Mitnick educates organizations on “how easy it is to trick people” into sharing usernames, passwords, or other credentials or otherwise taking action that enable a hacker to gain access to data, devices, or systems.

Limited resources
Budget allocations set aside for security remain a challenge for many healthcare organizations. Meeting Meaningful Use digitization and EMR requirements has consumed considerable HIT funding, while adding to security and operational overhead.

Even if healthcare organizations were willing and able to make the investment, a shortage of qualified security personnel forecasted to last through 2020 makes hiring staff with the right skills difficult.

Four reasons why a new approach to cybersecurity is imperative for healthcare:

1. To protect patient safety and brand reputation
2. To ensure regulatory compliance
3. To improve operational practices and efficiency
4. To enable clinical transformation

CYBERSECURITY AS A HEALTHCARE ENABLER
As technical advances in everything from sensors and mobility to decision support and machine learning redefine what’s possible in medicine, healthcare requires a new approach to cybersecurity, one that recognizes it as an integral and indispensable enabler of the core mission: better health outcomes and patient and caregiver experiences at lower cost.

To enable the full and confident use of new medical and digital technologies, cybersecurity must provide effective, reliable protection against threats to data and safety. It must be able to keep pace with rapid changes in both technical innovation and cyberthreats. And it must protect without getting in the way of care delivery or operational efficiency.

Stakeholder collaboration
Responsibility for cybersecurity cannot fall on providers or IT alone. Effective protection against cyberthreats in healthcare requires more than individual organizations can do on their own. It requires a coordinated effort by government, providers, medical device companies, IT and software solution companies, payers, and other industry stakeholders.

Recognizing that “healthcare cybersecurity is in critical condition,” the U.S. Department of Health and Human Services (HHS) assembled a broad task force to address the emerging challenges of cybersecurity. The team included representatives from the federal government, hospitals, insurers, patient advocates, security researchers, pharmaceutical companies, medical device manufacturers, health IT companies, and laboratories.

The resulting Health Care Industry Cybersecurity Task Force report emphasizes that “healthcare cybersecurity issues are patient safety issues” and “calls for a collaborative public and private sector effort to protect our healthcare systems and patients from cyber threats.”

The task force also stressed the importance of a uniform approach for addressing and sharing cyberthreat information and proposed the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST) as the foundation for “consistent, consensus-based healthcare cybersecurity framework” for improving security and identifying gaps across the healthcare ecosystem.
The framework provides a common language and guidance for helping to align and make cybersecurity part of an overall risk-management policy, process, and technology strategy. It defines a “framework core” of five concurrent and continuous functions—identify, protect, detect, respond, recover—to help organizations manage cybersecurity risks and facilitate collaboration.

Rather than adding to the regulatory landscape, the framework is proposed as a voluntary standard to provide a basis for stronger, more collaborative and coordinated cybersecurity. It has been endorsed by the HITRUST CSF Advisory Council and incorporated into FISMA Metric Reporting. Initial feedback on the framework from some healthcare industry groups calls for more work to better address “medical device risks and strained resources at smaller care providers.”

Parallel progress
As efforts to unify policies and fortify industry-wide approaches to healthcare cybersecurity move forward, it’s important to note progress has been made in multiple areas to reduce risk and improve threat protection.

Connected device safety
Growing awareness and market forces are pushing improved security in connected medical devices. Clinicians, health systems, and government agencies are demanding that medical devices be better protected against malware threats and other vulnerabilities.

Providers want greater transparency to be able to see that security has been built into devices and to make sure that devices fit into enterprise infrastructure and security strategies. They want devices to be “patch-able.” They want the ability to proactively monitor threats and for manufacturers to deliver timely patches and upgrades that internal teams can administer.

In late December 2016, the FDA released its recommendations for how medical device manufacturers should maintain the security of Internet-connected devices. They recommend that cybersecurity be an integral part of the entire product life cycle, from initial design to post-market monitoring for threats and vulnerabilities. Manufacturers are also advised to establish processes to quickly address threats and vulnerabilities before they can be exploited to cause harm.

Using technology to protect technology
IT and security companies have also made progress in delivering solutions and services that make it easier for health systems to move from fragmented cybersecurity approaches focused on:

- Reactive infrastructure
- Data center protection
- Specialist intervention
- Technology silos
- Point products

To a holistic, risk-driven approach that is:

- Proactive
- Built-in
- Intelligent and automated
- Business-focused
- With integrated, single-platform capabilities
Traditional data center

Micro-segmentation data center

Figure 1. Traditional data center versus micro-segmentation: Complementing the physical network segmentation traditionally used to comply with regulations such as HIPAA and PCI-DSS, VMware NSX enables micro-segmentation at the individual virtual machine and workload level, such as with EMR and PACS systems, to precisely control the lateral movement of threats across the data center versus the traditional method of protecting just at the edge.

Designed in

While traditional cybersecurity approaches have focused on perimeter protection, such as firewalls, there is growing recognition that since perimeters must necessarily always be somewhat porous in a digitally connected healthcare ecosystem, perimeter protection by itself will be ineffective.

As a result, healthcare organizations are increasingly benefiting from security that has been designed in—to protect data, networks, infrastructure, and endpoints from the inside out. Examples include endpoint intelligence that can analyze files for malware before files run, chips that are built into endpoint devices, and security policies that attach to and follow data and workloads wherever they go.

Virtual advantage

One advantage that many healthcare IT organizations have on their side is a relatively high degree of infrastructure virtualization. Driven by pressures to reduce IT capital and operating costs and reduce operational overhead, many healthcare organizations have virtualized their IT infrastructure. As a result, they are well positioned to exploit the advantages of software-defined security and automation in virtual and cloud-based environments.

For example, the ability to micro-segment virtual networks (Figure 1) has made implementation of a zero-trust approach to security, first introduced by Forrester in 2009, practical. Because software-defined firewalling, switching, and load balancing can be defined in and controlled by the hypervisor, virtual networks can be segmented down to the individual virtual machine (VM), distributing granular, intelligent, and policy-driven security into and across the environment.

Complementing the traditional firewalls and physical network segmentation traditionally used to comply with regulations such as HIPAA and PCI-DSS, virtual network micro-segmentation can dramatically stop the lateral movement of threats within the data center. Even if an attacker makes it past perimeter security and into the network, malware will be unable to move to other servers, thereby dramatically shrinking attack vectors to target data, such as EMR systems.

Micro-segmentation can also be used to isolate medical devices from other systems and to secure virtual tunnels from the data center to virtual desktop infrastructure (VDI). As a result, clinician endpoints, such as virtual desktops and mobile devices, can connect only to the servers that support them. They are prevented from accessing anything else on the network—and so is anything else on the network prevented from accessing them.
**Proactive, intelligent security operations**

Traditional antivirus and anti-malware solutions are reactive, their effectiveness depends on the development and installing of updates to protect against identified threats or attacks. As a result, they are ineffective in stopping zero-day threats (those unknown to the vendor), as well as advanced, persistent, and rapidly evolving attacks, like spear phishing and ransomware. Once into a system, the longer hackers can explore, examine data, and elevate their permissions, the worse the consequences can be. As care becomes more digitally connected, the ability to proactively and intelligently monitor the environment in real time for abnormalities and to quickly and intelligently predict, prevent, detect, and respond to attacks is critical.

That's why advanced threat-protection capabilities that analyze data from multiple sources to intelligently identify and automatically respond to potential threats are vital. By applying big data analytics, machine learning, and artificial intelligence, systems are able to monitor vast quantities of data captured from all kinds of sources—infrastructure, applications, endpoints, logs, threat databases, user activities—to recognize patterns and trigger an appropriate response.

Advanced security operations platforms leverage multiple security, risk management, and compliance frameworks and integrate multiple cybersecurity technologies to provide end-to-end visibility from a single command center. Around-the-clock analysis of real-time data not only enables automated responses to isolate or stop potential attacks but also provides security analysts with rich data for investigation.

**EVERYONE’S JOB: PATIENT SAFETY**

Cybersecurity can no longer be just the responsibility of the IT department or a security team. Maintaining patient trust and protecting patient safety must become the first priority of everyone in the organization.

**Holistic, mission-driven strategy**

Healthcare organizations need to move beyond isolated and fragmented approaches to cybersecurity focused on particular technology silos, functions, or departments. Instead, what’s needed is a holistic, enterprise-wide cybersecurity strategy aligned with the care mission and an organization’s clinical, financial, and operational objectives.

Fortunately, there are more C-level executives and boards actively leading and overseeing such programs. A 2017 CHIME-KLAS Study found that 42% of healthcare organizations now have a vice president or C-level official in charge of cybersecurity and that 62% report that cybersecurity is on the agenda at quarterly board meetings.

News reports about the cost of data breaches and impact of ransomware attacks targeting healthcare institutions—as well as initiatives, such as the Health Care Industry Cybersecurity Task Force and CyberMed Summit—have raised awareness and the standard for what a cybersecurity program needs to be able to do. Only 16% of respondents in the 2017 CHIME-KLAS survey reported having “fully functional” security programs, and 41% said they are undertaking programs to improve their security. Overall, 75% of respondents reported that they are following the NIST Cybersecurity Framework.

**Unified risk management**

Many healthcare organizations are addressing cybersecurity as part of a larger unified risk-management strategy. Such an approach reveals overlaps, gaps, and interdependencies between cybersecurity and business resiliency, IT continuity, compliance, legal, and financial requirements. It helps the organization to build a clear business case and uncover opportunities for efficiency.

In fact, new evidence shows that organizations that invest in the development and deployment of a mission-driven security strategy report benefits that go beyond cyber protection.

**Broad stakeholder participation**

Front-line caregivers, administrators, finance teams, support staff and even contractors and vendors, all have important roles to play in ensuring patient safety and protecting the organization from cyber threats.
insights and perspectives to share on which risks to prioritize, what risks are emerging, and what the potential impacts would be on specific operations.

It takes a cross-discipline approach to effectively identify and assess risks, develop responses, and define the roles individuals can play in protecting cybersecurity and patient safety in their day-to-day tasks as well as in the event of an incident response and remediation.

**Multilayered security**
Just as hardware, software, networks, endpoints, processes, operational practices, and people can all be risk vectors, exposing healthcare organizations to cyberattacks, all can be equipped to provide multiple layers of security that protect data and patient safety.

Cybersecurity strategies and programs should leverage multiple layers of policy, process, physical and virtual technologies, workflows, and social engineering programs—for data loss prevention (DLP), identity and access management (IAM), mobile device management (MDM), and security information and event management (SIEM).

Healthcare providers can look to instill a culture of awareness across the organization about the dangers of too much trust or too little vigilance. Resistance training and penetration testing can play important roles as part of workforce education. And providers should include specific cybersecurity protection and practice requirements, responsibilities, and liabilities in their employment and vendor agreements.

**Triage and good hygiene**
In parallel with enterprise cybersecurity transformation programs, healthcare needs to identify and prioritize risks that need immediate remediation. That means adherence to foundational good cyber hygiene practices, which, like handwashing, are essential to preventing harm.

Privileged credential protection, network segmentation, asset isolation, perimeter fortification, remote data replication, timely backups, patches, and upgrades are areas where many healthcare organization need to take immediate action, not only to catch up, but also to get ahead of the curve. Investment in modern infrastructure, automated tools, and/or on/offsite services to clean up legacy messes and eliminate lingering poor practice vulnerabilities may well be justified through risk assessment.

**Prepare for the worst**
Just as healthcare organizations plan and prepare for threats from disasters to epidemics, they need to have both specific incident response and an overall organization-wide response plan in place. Teams need practice test plans and practice procedures to be as ready as possible to mitigate and work around a potential breach or attack.

**Put on a white hat**
Now more than ever, all healthcare delivery organizations have a responsibility to secure their systems, medical devices, and patient data.

While most medical professionals cannot be expected to also take up white hat hacking, they do need to be prepared to consider and recognize cyberattacks as a potential factor in their diagnosis and treatment options.

Live-action simulations from the CyberMed Summit underscored the criticality of a proper security response in the wake of a cyberattack, depicting situations in which doctors were faced with trying to keep “patients” alive after the mock attack shut down an insulin pump, bedside infusion pump, and pacemaker.

As always, patient safety and well-being will depend on the knowledge, preparation, quick thinking, and dedication of caregivers.

Technology leaders with a wide range of cybersecurity experience are working together to help healthcare organizations of all types and sizes implement practical, robust security that enables safe, high quality, and efficient care.

Dell EMC is working to advance a holistic, intelligent, and
mission-driven approach to cybersecurity in healthcare (Figure 2) by unifying and leveraging industry-leading security technologies and services from various partners, including Dell, RSA, Mozy, SecureWorks, Virtustream, Intel® and VMware.

Integrating and automating end-to-end tools, processes, and solutions and designing security into end-user devices, networks, servers, and cloud platforms make it easier for healthcare to implement the kind of multilayer cybersecurity required to prevent threats, protect data, and mitigate risk. Together, Dell EMC cybersecurity technology leaders are committed to helping healthcare move forward with confidence and take advantage of digital and medical technologies that advance patient care.

Healthcare organizations are using Dell EMC security solutions and services today to:

- **Protect data wherever it goes.** Dell Data Guardian enables organizations to encrypt sensitive data and monitor and control who has access to files and how they are used—regardless of the type of device or network, where data resides or travels, or how data is shared (e.g., email, cloud, FTP, USB).

- **Prevent malware before it can run.** Dell Endpoint Security Suite Enterprise, powered by Cylance uses an integrated client that includes advanced threat prevention and Enterprise-class encryption, all centrally managed via a single console to help healthcare companies reduce IT management costs and complexity. With consolidated compliance reporting and flexible email notifications, healthcare companies can easily enforce and prove compliance for all of their endpoints. Built-in security with features like simplified policy configuration with smart defaults and pre-defined report templates are especially helpful as organizations struggle to protect data. Unique artificial intelligence (AI) and dynamic mathematical models further prevent malware attacks via endpoint devices.

- **Control access while improving workflow and productivity.** RSA SecurID two-factor authentication and role-based identity and access solutions put critical information and applications into the hands of those who need it, where and when it’s needed, while protecting patient safety and privacy and simplifying compliance.

- **Limit attack vectors.** Software-defined capabilities in virtual environments are helping to dramatically reduce vulnerabilities from the inside out. With VMware NSX virtual networking, administrators can define network micro-segmentation and firewall management down to the VM level, enabling a zero trust or least-privileged model for network communication between sources and destinations that prevents the lateral spread of threats throughout the data center.

- **Maintain operational continuity.** Mozy cloud backup and Dell EMC Isolated Recovery Solutions enable healthcare organizations to recover lost, locked, or destroyed data quickly and reliably to maintain operational continuity. One of the industry’s first cloud-based file backup services, Mozy now supports four data-encryption methods, including Key Management Interoperability...
Protocol (KMIP) for automatic generation of per-user encryption keys managed by an on-premises key management server (KMS). Dell EMC Isolated Recovery Solutions use advanced replication and snapshot management to maintain isolated, off-network/air-gapped copies of data and procedures for fast restore and recovery. Dell EMC Cloud solutions and services portfolio—including Virtustream Healthcare Cloud, Dell EMC Hybrid Cloud, and Microsoft Azure—modernizes your infrastructure, reduces costs, and delivers uncompromised and comprehensive security and compliance. Virtustream Healthcare Cloud is a HIPAA/HITECH-compliant cloud purpose-built for mission-critical healthcare applications that maintains the security of PHI, delivers infrastructure availability SLAs up to 99.999%, and provides business-continuity and disaster-recovery services.

- **Replace point solutions with an integrated platform.** RSA Archer provides internal security operations teams with one platform for operational risk management; IT risk management; IT vendor risk management; business continuity management; and governance, risk and compliance (GRC).

- **Take advantage of vendor-neutral security consulting and intelligence-driven managed services to complement in-house expertise and resources.** SecureWorks enables our healthcare clients to focus on their business priorities of improved patient outcomes and patient safety as the industry continues its expansion in a digitally connected environment. The elite team of researchers, engineers, analysts, and consultants that supports the SecureWorks Counter Threat Platform assists in unleashing the value of the client’s cybersecurity investments, enabling better prediction, prevention, detection, and responses to the continuously evolving threat environment experienced by the healthcare industry. The Counter Threat Platform combines artificial and human intelligence to better secure the unique operating environment of that client. Security is the business of SecureWorks, and as a vendor-neutral services provider, the goal with each client is to assist its efforts in its security maturity journey by maximizing the efficiency of existing controls and making investment decisions based on what best complements and strengthens the current security infrastructure. The result is a lower cost to provide 24x7x365 continuous monitoring than what might be realized if the client attempts to meet alone the business security challenges it confronts. SecureWorks Incident Response team assists our healthcare clients in building a plan to meet the challenges of the continuously changing threat vectors, test the response plan, integrate the plan with the Disaster Discovery Plan in order to maintain operations, and conduct the necessary risk assessment of a breach to determine if notification to the Office for Civil Rights must be made in accordance with the Breach Notification Rule.
Dell EMC helps healthcare organizations advance in the digital era, transforming the way they work so that they can transform the lives of the people they serve. We uniquely power this digital transformation by delivering best-in-class technology for applications, data, infrastructure, and security—from the edge to the core to the cloud.

Learn more at: DellEMC.com/healthcare or contact a Dell EMC Healthcare Representative


8. “Not Including all Ransomware Attacks Which, Depending on Certain Circumstances, May or May Not Constitute a PHI Breach.” For more info, see https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf


© October 2017 Dell EMC Corporation. All rights reserved.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks are the properties of their respective owners.