CYBERARK

SOLUTION BRIEF

PRIVILEGED ACCESS SECURITY PROTECTS INNOVATIVE PATIENT CARE

How CyberArk helps you Protect ePHI

The application of innovative technologies continues to change the face of healthcare around the globe. Healthcare providers on the frontlines are using new models of care and technologies to offer advanced patient services and improve clinical outcomes. Cloud-based applications, use of mobile devices, distributed points of care, telemedicine or virtual care, IoT enabled medical devices and patient portals have all helped create larger, more complex integrated care delivery networks.

While it is understood these networks generate increasing amounts of patient data, or electronic Personal Health Information (ePHI), they also rely upon the expanded use of privileged access. Interoperability – the sharing of ePHI – would not be possible without the use of privileged credentials. Fundamental capabilities such as cloud-based Electronic Health Record (EHR) applications, integrating patient diagnostic data from third party services, or seeking reimbursement from a payer organization all require privileged access.

Privileged access is needed for an administrator, application, or device to access a system (such as applications, servers, switches, firewalls, routers) whether located in your on-premises data center or in the cloud. Privilege is a term used to designate special access or abilities, above and beyond that of a standard user. They can be super user type accounts such as Windows Admins or Linux Root accounts, or credentials used for application to application or IoT device communications. Privileged accounts and credentials extend to cloud and Software as a Service (SaaS) providers. Modern enterprises cannot function without privileged access and it must be monitored and defended.

Compromised privileged credentials can threaten the ability to deliver care, one's reputation within the community, and basic financial health. Vulnerable privileged access is the vector of choice for cyber attackers targeting ePHI and installing ransomware, whether from within or outside the expanded network. As systems become more complicated, risks from human error, mistakes or lapses managing privileged credentials can also inadvertently expose ePHI. CyberArk Privileged Access Security Solution provides proactive, end-to-end detection and protection for all privileged accounts that have access to the systems containing ePHI.

More Cyber Risks from Expanded Care Delivery Systems

Cyber-attacks targeting healthcare providers are increasing in volume, scope and sophistication. The European Commission has recognized the need for stronger security and dedicated €1.2B in cybersecurity investments by 2020 to protect industries with sensitive personal information, like healthcare. In the U.S., healthcare providers are also working to address their vulnerabilities. In 2017, "there were 477 healthcare breaches reported to the U.S. Department of Health and Human Services (HHS) or the media... which affected a total of 5.579 million patient records."

Extended delivery care networks, encompassing new technologies and more partners, offer additional points of potential privileged access to ePHI:

- Cloud-based EHR and other Software-as-a-Service (SaaS) applications, hosted by a third party;
- Financial applications like billing, e.g. Revenue Cycle Management (RCM) solutions, scheduling and insurance eligibility;
- Mobile diagnostics and telemedicine, such as Electrocardiography (ECG or EKG) systems, connected to your EHR;

Cyber criminals are looking to exploit any weak point along the continuum of care. They target providers and their partners of all sizes.

- Employees of Alaska's Department of Health and Social Services were duped into loading Trojan horse malware on two computers storing ePHI of more than 500 individuals;
- A former employee of Kentucky-based Med Center Health, part of Commonwealth Health Corporation, mis-used their privileged access to steal the ePHI of up to 697,800 individuals;

- A ransomware attack on Nuance's eScription service impacted Beth Israel Deaconess in Boston and the University of Pittsburgh Medical Center. The outage obliterated doctors' instructions to patients and 10 other services, including those used for radiology, billing and software that tracks quality of care.

In addition to the expanding threat surface of healthcare providers, increased value of ePHI is also attracting attackers. One estimate places the value of a stolen medical record at ten times more than a credit card number.

Attacks are not limited to the U.S. This was amply demonstrated in May of 2017 when at least 16 regional hospitals in the U.K, part of within the National Health Service (NHS), were crippled by Wanna Decryptor ransomware:

"Staff were forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones. Hospitals and doctors' surgeries in parts of England were forced to turn away patients and cancel appointments…. People in affected areas were being advised to seek medical care only in emergencies."
– Chris Graham, The Telegraph

Sources, attack vectors and payloads are all key parameters to consider when defending against attacks; however, securing privileged credentials is key, in any scenario, to protect ePHI and avoid devastating attacks.

The Burden on IT: How are We Doing?

Much of the burden of protecting ePHI in networks falls on already struggling healthcare IT departments.

A global survey of 1,300 IT decision makers found some sobering realities for healthcare providers:

- 59% of healthcare respondents believe that customers' PII could be at risk because the organization does not go beyond legally mandated controls
- 85% agree that security should be discussed more frequently at the board level in healthcare
- 52% state that their organization cannot prevent attackers from breaking into their internal network

The U.S. Department of Health and Human Services (HHS), alarmed by the increase in ransomware targeting healthcare, added a Ransomware and HIPAA Fact Sheet to its Security Guidelines. The fact sheet noted there have been 4,000 daily ransomware attacks since early 2016, up 300 percent over the 1,000 daily ransomware attacks reported in 2015. It went on to state: "The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."

Not only must IT monitor an expanding threat surface with less resources, they must also work with – and secure – a greater number of vendors, contractors and third parties. An effective privileged access security solution has to be as automatic as possible, alleviating repetitive, time-consuming and error-prone "manual" processes. Defense mechanisms need to extend easily and quickly to accommodate new applications and third party services.

Increasing Regulations and Harsher Penalties

Regulations regarding ePHI are increasing around the globe; and non-compliance is bringing stiffer penalties. Strong, documented, auditable privileged access security can make or break your ability to demonstrate compliance and avoid financial penalties.

In 2016, the U.S. HHS collected a record $23.5 million in settlement payments. This was up from $6.2 million in 2015. And this is only at the national regulatory level.

In the E.U., the May, 25th 2018 enforcement deadline for the General Data Protection Regulation (GDPR) has significant implications for personal health records. The financial penalties are severe—up to 4% of revenue for non-compliance. And for the first time, E.U. residents are given the explicit right to compensation for the misuse or compromise of their personal data – meaning lawsuits.

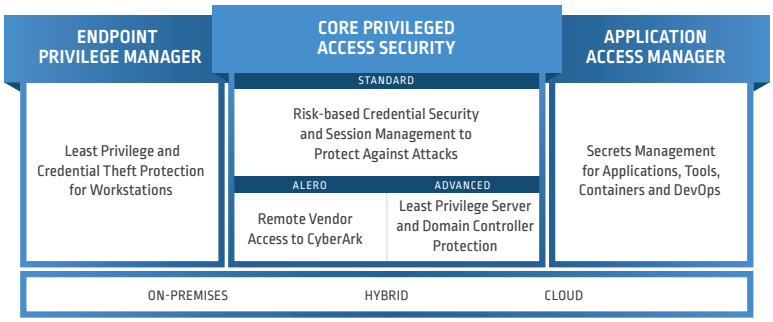
In addition to penalties, there are operational costs to recover from a data breach – whether criminal or inadvertent. A global study of 419 organizations by The Ponemon Institute found that a healthcare data breach costs on average $380 per record, more than 2.5 times the global

average across industries of $141 per record. The study also called out third party involvement, extensive migration to the cloud, compliance failures, and extensive use of mobile platforms as contributing to the increased costs.

CyberArk Protects Your Investment in an Integrated Care Delivery Network

Strong Privileged Access Protection

Healthcare providers require strong privileged access security to protect against growing external threats, such as ransomware, and internal threats to ePHI, both malicious and those resulting from human error. The CyberArk Privileged Access Security Solution ensures your ability to protect ePHI and secure a broader, more complex delivery network, protecting your investments and allowing you to continue to deliver quality patient care.



- End-to-end protection of all privileged access across on-premises, cloud, and DevOps environments. This includes cloud-based EHR applications and diagnostic partners.
- Full lifecycle management of passwords, SSH keys and credentials, regardless of whether they are used by interactive users (employees, contractors or vendors) or applications for on-premises and in cloud-based applications.
- Detection and protection for 1,000,000+ malware variants and advanced attacks (including ransomware) on distributed endpoints with out of the box, comprehensive privileged security policy control.

Future-Proofing Privileged Access Security

Healthcare networks continue to expand and evolve. CyberArk's Privileged Access Security Solution extends capabilities to accommodate new infrastructure and applications, whether on-premises, from the cloud or the DevOps pipeline. The best way to keep up with constantly evolving threats is a comprehensive, time-tested privileged access security solution – with a proven vendor and clear roadmap.

- A comprehensive solution that's extensible and enables interoperability:
  - All functionality built to share common resources, a common UI, organically designed to work well together, including credential management and security, session monitoring, isolation and threat analytics from one platform;
  - Distributed architecture proven to scale in complex environments, including multiple network segments across multiple sites of care;
  - Wide variety of available integrations; with support from 170+ vendors out-of-the-box, with over 200 connectors and plug-ins;
- Time-tested and proven market leader:
  - 3800+ customers globally;
  - Nearly 20 years of experience and a strategic focus on privilege protection: 200+ dedicated R&D engineers dedicated to innovation;
  - Consistently rated as leader by analysts such as Forrester, IDC and KuppingerCole.
- CyberArk Marketplace provides integrations with security, IT operations and business applications to extend the reach of privileged access security

Domain controllers represent one of the highest value targets in your infrastructure. If an attacker can gain access to a domain controller admin's credentials, they can move across the organization and compromise sensitive systems. For this reason, domain controller attacks are commonly referred to as "golden ticket" attacks."

Prove Compliance More Easily

To demonstrate compliance healthcare providers must have documented, auditable proof of their efforts to control privileged access. This extends beyond regulations such as HIPAA in the U.S. or GDPR in the E.U. It includes privileged access monitoring and audit logging to achieve certification for Common Security Frameworks (CSF) such as HITRUST and NIST. The CyberArk Privileged Access Security Solution provides rapid access to detailed and comprehensive user session activity, which is increasingly valuable to meet audit and compliance requirements.

- Comprehensive monitoring, recording, and isolation of all privileged user sessions, and activity on critical ePHI database or application, e.g., cloud-based EHR application.
- Fully searchable audit logs (including meta-data) and DVR-style recordings of all privileged user session activities, including contractors and vendors.
- Full audit trail data protected by same, hardened security (multi-layered encryption and other proactive measures) as credentials themselves.

Proactive and Automated Privileged Access Security to Enable IT

To respond to threats rapidly and free IT to focus on initiatives that improve efficiency and the quality of care, privileged access protection of healthcare systems must be as proactive and automatic as possible. The CyberArk Privileged Access Security Solution is the premier solution to analyze end-to-end, privileged user and account behavior to detect, alert and respond to critical privileged security threats. Real-time session monitoring enables rapid detection of abnormal activity and remote termination of sessions to disrupt potential privileged access security attacks.

- Protect delivery of care, save time and money with CyberArk automated detection and protection of privileged access:
  - End-to-end automation of privileged access security tasks across the delivery of care network;
  - Detects malicious activity (e.g. Kerberos attacks) on Domain Controllers in real-time;
  - Thwart attacks in real-time by automatic suspension or termination of privileged sessions based on risk analysis;
- CyberArk helps IT stay in control while maintaining productivity:
  - Reduces risk by removing local admin rights from endpoints while keeping users productive and limiting IT support costs;
  - Enforces least privilege policies yet enables users to elevate privileges when needed for business purposes – in accordance with policies – strengthening security while keeping IT users productive;
- Leverage CyberArk's privileged access security expertise:
  - CyberArk Services help expedite the development of a best practices privileged access security program by providing the expertise and experience where and when needed;
  - 500+ Trained CyberArk Delivery Engineers at CyberArk and leading system integrators.

Getting Started Fast

To help you get started building a best practices privileged access security program and protect your ePHI, CyberArk recommends that you:

- Run a cost-free CyberArk Discovery & Audit (DNA) scan to uncover potential sources of risk in your network right now. Identify your privileged user and application accounts, including those used by third-party users;
- Find out how CyberArk's Privileged Access Security Hygiene Program helps you "think like an attacker." The program was developed based on CyberArk's engagement with thousands of customers who have implemented privileged access security programs. The Privileged Access Security Hygiene Program focuses on the seven controls that reduce the most relative risk to the level of resources and effort you expend.
- Engage the CyberArk Red Team to simulate adversary behavior and test the security team's ability to respond to threats. By using a variety of tactics, techniques and procedures (TTPs) CyberArk Red Team services are designed to provide a safe way for security operations to uncover vulnerabilities in their cloud environments, test security procedures and identify areas of improvement.

Click here to read Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials White Paper.

For more information contact one of our sales consultants or visit us at: www.cyberark.com