EXECUTIVE BRIEF
AUGUST 2018

Preventing Healthcare Breaches

How CA Technologies Can Help You

Privileged accounts and access are not granted just to employees with direct, hands-on responsibility for system and network administration but also to vendors, contractors, business partners and others who have been granted privileged access to systems within your organization. In many cases, privileged accounts aren't even people—they may be applications or configuration files empowered by hard-coded administrative credentials. These represent targets for external hackers or malicious insiders to compromise and exploit.

Background

Healthcare organizations are under tremendous pressure to secure their patient, financial, employee and other proprietary data against a burgeoning pantheon of threats. To reduce their risk, they must focus on the attack vectors that can do the most damage. The reality is that exploited or compromised privileged accounts are the cause for almost 50 percent of all data breaches,[1] regardless of whether those accounts were used by external actors with nefarious intent or simply abused by insiders. In fact, there are two primary challenges to healthcare organizations.

Challenge 1: Prevent data breaches

The healthcare sector continues to be a primary target for external attackers. According to the 2018 Verizon Data Breach Investigations Report, healthcare organizations reported 536 data breaches, the most of any sector.[2] In addition, over 75 percent of respondents in the 2018 HIMSS Cybersecurity Survey indicated that their organization experienced a significant security incident in the past 12 months.[3] And ironically, even though Verizon found that almost three-quarters (73 percent) of cyberattacks were perpetrated by outsiders, its report also stated that "healthcare is the only industry where the threat from inside is greater than that from outside."[2]

The average cost of a data breach is approximately $3.86 million, and within healthcare, the estimated cost per patient record is approximately $408 per record.[1] You do not just need to be concerned about the immediate cost of the breach itself. If a data breach does occur, the result can also lead to lawsuits, damaged corporate reputation and loss of customer trust.

Challenge 2: Address regulatory compliance

As the role of compromised privileged accounts and credentials in security incidents has become clear, regulatory bodies and auditors have focused their attention on the controls and processes that healthcare organizations must implement to mitigate these risks. Thus, healthcare organizations are subject to an ever-expanding list of data security regulations and standards. These include but are not limited to:

- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA).** The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI), while the HIPAA Security Rule defines administrative, physical and technical security safeguards required for compliance.

- **The Health Information Technology for Economic and Clinical Health (HITECH) Act.** The HITECH Act requires entities covered by HIPAA to report data breaches that affect 500 or more people to the U.S. Department of Health and Human Services, the news media and the people affected.
- **Payment Card Industry Data Security Standard (PCI-DSS).** Healthcare organizations do not just need to worry about PHI data—many accept payment via credit card and therefore are also required to implement security controls around cardholder data to reduce credit card fraud.

These regulations are just a few of the legal mandates with which healthcare institutions must comply, further underscoring the criticality of access control and auditing to prevent security incidents. As noted earlier, failure to comply can result in costly penalties and fines. Since 2016, approximately 25 healthcare organizations have paid over $50 million in fines for HIPAA violations.[4]

What Organizations Must Do to Secure Access to Data

While the nature, extent and technological sophistication behind data breaches continues to evolve, healthcare organizations need to adopt a defense-in-depth strategy with multiple layers of security. In this new world, level of access is everything: which accounts have access, what data are they accessing and whether they need that level of access are critical elements to understand. This is even more critical when users and systems are granted elevated or privileged access.

Many healthcare organizations are moving to what is known as a zero-trust model, in which all access is removed and then is granted back when needed—just enough for users to do their jobs, but no more. For privileged accounts, this unique perspective requires organizations to control, manage and audit all privileged user access and activity. As part of this process, organizations are also looking to implement privileged identity governance, so that provisioning and de-provisioning of privileged access is automated, and periodic reviews and certification of this access are performed. The last thing healthcare organizations need is an angry ex-employee with the keys to the kingdom who walks out the door with proprietary data.

With this kind of access oversight and activity insight, healthcare companies can combat insider threats as well as external attacks and secure their most precious asset: information. And they can also address their two primary challenges discussed in the background section: prevent data breaches and address regulatory compliance.

Preventing data breaches before they even happen

To reduce risk, healthcare organizations must control the access of privileged users and track their actions. Privileged access management technologies focus on providing granular authorization of users to systems and accounts, auditing and recording attempts to access, and vaulting and rotating the privileged account's credentials, including passwords. In addition, when a privileged access management solution is integrated with user behavior analytics, organizations can detect risky activity and automatically trigger mitigations that limit the damage, which can be inflicted by a malicious insider or an external attacker leveraging a compromised privileged account.

Implementing controls that auditors are seeking

Privileged access management technologies are not just good for combatting targeted breaches and insider threats. They can also help organizations meet regulatory requirements.[5]

Regulation Requirement	HIPAA	PCI-DSS	Comments
Identify and track the location of privileged account credentials		7.2.1	CA Privileged Access Manager (CA PAM) stores and manages privileged account credentials.
Enforce rules for password strength, uniqueness, change frequency	45§164.308(5)(D) 45§164.312(2)(i)	8.5.5 8.5.8 8.5.9	CA PAM automatically changes privileged passwords and enforces rules for strength and uniqueness.
Delegate so that only appropriate personnel can access	45§164.308(3)(i) 45§164.308(3)(B) 45§164.308(3)(C) 45§164.312(a)(1)	2.1 6.3.6 7.7.1 8.5.4 8.5.6	CA PAM issues privileged access credentials only to authorized users and can control what activities users can perform.
Audit and alert to show requesters, access history, purpose, duration, etc.	45§164.308(5)(C)		CA PAM audits and can record all privileged account activity.

Summary

To guard against costly data breaches, smart financial institutions are protecting and automating access to privileged accounts across both physical and virtual systems. Whether your company's data is on premises, in the cloud or within a hybrid infrastructure, it's critical to protect, monitor and audit privileged access everywhere. Employing a zero-trust model with a defense-in-depth approach to security that includes privileged access management offers your organization the best chance of protection against ever-evolving threats.

For more information, please visit **ca.com/PAM**

1 Ponemon Institute, "2018 Ponemon Cost of Data Breach Study," July 2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

2 Verizon, "2018 Data Breach Investigations Report," April 2018, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

3 Healthcare Information and Management Systems Society (HIMSS), "2018 HIMSS Cybersecurity Survey," 2018, https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

4 Compliancy Group, "HIPAA Fines Listed by Year," 2018, https://compliancy-group.com/hipaa-fines-directory-year/

5 Table Source: Barbara Filkins, "The Case for PIM/PAM in Today's Infosec," June 2016, https://www.sans.org/reading-room/whitepapers/analyst/case-pim-pam-todays-infosec-37072