WHITE PAPER • AUGUST 2017

ca technologies

Defend Against Data Breaches With Privileged Access Management: A Guide for Financial Services Organizations

Table of Contents

Executive Summary

Challenge

Financial organizations are under tremendous pressure to secure their financial, customer and other proprietary data against a burgeoning pantheon of internal and external threats. Whether they are obtained maliciously or leveraged inappropriately by a valid user, exploited privileged user accounts are the common thread of most data breaches. And as your environment grows increasingly complex, so does the challenge of defending against ever more sophisticated—and damaging—attacks.

Opportunity

While the nature, extent and technological sophistication behind data breaches continue to evolve, what is needed is a defense-in-depth strategy with multiple layers of security. In this new world, level of access is everything: Which accounts have access, what they are accessing and why they have access are critical elements to understand.

Benefits

Our customers use CA Privileged Access Manager (CA PAM) to provide secure access with enhanced security for authentication and authorization. While most legacy systems in the financial services industry do not have hardened security, with CA PAM, methods for third-party integration such as multifactor authentication and single sign-on tools using role management techniques can easily be deployed, removing the requirement for enhancement to the application while providing a centralized, auditable and repeatable process of access control..

Introduction

Privileged accounts comprise not only employees with direct, hands-on responsibility for system and network administration but also 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 can be applications or configuration files empowered by hard-coded administrative credentials.

According to the 2016 Verizon Data Breach Investigations Report,1 the finance sector reported 1,368 data breaches and was one of the top industries subject to insider and privilege misuse. The sad fact is that exploited privileged accounts are a common thread in many data breaches, regardless of whether those accounts were compromised by external actors with nefarious intent or simply abused by insiders.

As data moves to the cloud, accessed by multiple third-parties and handled by insiders, the threat grows ever larger, as does the challenge of protecting your organization from evolving threats and staying in compliance with internal, industry, local, country and international regulations. These compliance mandates include access control and data security regulations that your organization is legally required to meet. Not doing so could mean everything from fines for non-compliance to actual data breaches from lack of prevention. This is the cost of negligence.

According to 2016 Ponemon Cost of Data Breach Study, the average cost of each lost or stolen record is $158, and with most breaches involving millions of records, the costs of remediation are astronomically high.2 In fact, the average data breach costs an organization approximately $3.8 million to $4 million, the study reported. For example, the JPMorgan Chase data breach that compromised user names, addresses, phone numbers and email addresses in 2014 cost the banking giant $1 billion, and that breach didn't even affect more sensitive information, such as account numbers, passwords, user IDs, birth dates or social security numbers. If it had, the cost would have been even greater. Add to that the intrinsically priceless nature of customer trust and loyalty, both of which can be forever obliterated after a breach, and you can see just how much is at stake.

Your Ever-Expanding Remit

Financial organizations are under tremendous pressure to secure their financial, customer and other proprietary data against a burgeoning pantheon of internal and external threats. In order to reduce risk, they must control the access of privileged users and track their actions. In order to reduce cost and complexity, they must centralize the administration and control of server access as well as automate password management. And in order to simplify compliance, they must be able to provide proof of effective administration controls. The bottom line is that your responsibilities increase as the digital age evolves, more regulations are passed and data moves to the cloud. These responsibilities include, but are not limited to:

1. Preventing data breaches before they happen

The threat from bad actors with compromised privileged credentials is a real and growing threat. Whether they're external (e.g., nation-states, cybercriminals and hacktivists) or internal (e.g., rogue or hapless employees and greedy third-party contractors), intruders with privileged access are at the core of many data breaches.

That's because privileged accounts typically have much deeper access to a corporation's most valuable data, including financial information, customer data and intellectual property, control of which can be lost by being uploaded to the cloud, emailed outside the organization or copied onto a USB drive, for example. Once identified, privileged user accounts can be continuously targeted by socially engineered, advanced persistent threats to steal credentials, and it is likely they will succumb to the attempt even with the best of intentions.

Financial services organizations must do everything they can to ensure that access to that proprietary information is controlled, monitored and audited in order to mitigate the risks associated with privileged users, accounts and credentials.

2. Meeting regulatory compliance and audit mandates and protecting data as required by law

As the role of insiders, compromised accounts and credentials in security incidents have become clear, regulatory bodies and auditors have focused added attention on the controls and processes that financial services organizations must implement to mitigate these risks. Thus, financial services companies are subject to an ever-expanding list of data security regulations and standards, issued by states, countries and industry associations. These include, but are not limited to:

- **Consumer Financial Protection Bureau and National Credit Union Association (NCUA)** regulations, which pertain to the privacy of consumer financial information
- **European Union Data Protection Directive (EUDPD)**, which regulates the processing of personal data
- **Gramm-Leach-Bliley Act (GLBA)**, which requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data
- **Japan's Personal Information Protection Act**, which protects the rights and interests of individuals and their personal information
- **Payment Card Industry Data Security Standard (PCI-DSS)**, which increases controls around cardholder data to reduce credit card fraud
- **Sarbanes-Oxley Act (SOX)**, which protects investors by improving the accuracy and reliability of corporate disclosures
- **State Financial Data Privacy Acts**, such as New York's recent cybersecurity regulation, which require banks, insurance companies and other financial services companies to significantly increase their cybersecurity programs in an effort to further protect consumers' personal and financial information

These regulations are just a few of the legal mandates with which financial institutions must comply, further underscoring the criticality of access control and auditing to prevent security incidents. Failure to comply can result in costly penalties and fines. And if data breaches do occur, the result can be lawsuits, damaged corporate reputation, loss of customer trust and even the possibility of jail time, as well as the potential for the total loss of the business from financial ruin.

3. Securing a hybrid IT infrastructure

As data migrates to the cloud, the scalability and elasticity of cloud computing introduce new challenges. Shared security responsibilities, highly elastic cloud environments and the architecture of the hybrid enterprise require more dynamic protections and controls that address new security risks, comply with regulations and manage privileged users' administrative accounts across traditional, virtualized and cloud IT environments. In fact, a hybrid IT infrastructure is actually more difficult to secure because the attack surface is expanded, requiring ever more vigilance.

What Financial Services Organization Must Do to Secure Access to Data

While the nature, extent and technological sophistication behind data breaches continue to evolve, what is needed is a defense-in-depth strategy with multiple layers of security. In this new world, level of access is everything: which accounts have access, what they are accessing and why they have access are critical elements to understand.

Many financial services organizations are moving to what is known as a zero-trust model, in which it is assumed that a corporate account has already been compromised. That perspective prompts the need to control, monitor and audit user access and activity, ensuring that the right people have the most appropriate, fine-grained level of access: just enough to do their jobs, but no more.

As part of this process, companies are automating the privileging (and de-privileging) process as well as recording and reporting on user activities to prevent breaches before they occur. Automation also helps to defend against privilege escalation that results in access to sensitive resources and prevents the compromise of new systems as well as data exfiltration. The last thing financial services companies need is an angry employee (or 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, financial services institutions can combat insider threats as well as external attacks and secure their most precious asset: corporate information.

How Financial Services Customers Use CA Privileged Access Manager

Whether they are obtained maliciously or leveraged inappropriately by a valid user, exploited privileged user accounts are the common thread of most data breaches. And as your environment grows increasingly complex, so does the challenge of defending against ever more sophisticated—and damaging—attacks. CA Privileged Access Manager (CA PAM) offers a comprehensive solution delivering both network- and host-based controls for the enterprise and hybrid cloud. There are literally hundreds of use cases for CA PAM in the financial services industry.

Our customers use CA PAM to provide secure access with enhanced security for authentication and authorization. While most legacy systems in the financial services industry do not have hardened security, with CA PAM, methods for third-party integration such as multifactor authentication as well as single sign-on tools using role management techniques can easily be deployed, removing the requirement for enhancement to the application while providing a centralized, auditable and repeatable process of access control.

In addition, CA PAM supports compliance of PCI/DSS requirements regarding access control (e.g., Requirements 2, 7, 8 and 10) as well as GLBA's protection of consumer accounts through tracking and reporting user activities as well as configuration changes to the network, enforcing access control to all network devices and network servers and producing audit reports that document and verify this, among other things.

Regardless of the compliance use case, you can count on CA PAM to manage user authentication and authorization, secure access to information and provide comprehensive audit trails for access, usage and password management as part of a solid, defense-in-depth security program.

How One Company Succeeded With Access Control

TIS Inc., is a Japanese company that offers all-in-one support for internationally branded debit card businesses, acting as an application service provider (ASP). In order to continue providing these services, the company needed to demonstrate compliance with the global security standard Payment Card Industry Data Security Standard (PCI DSS 2.0) in just six months.

> "We have established five types of access to servers containing cardholder data and have clearly segmented the authorization that can be executed in regard to servers by engineers, who can only access data relating to the customers for whom they are responsible. This demonstrates a significant improvement in our security levels, without any sense that the burden of work required to operate the system has increased."
>
> —Kyoshi Tsuchida, executive with Financial Solutions Group No. 1

The criteria for PCI DSS 2.0 included Requirement 7, which restricts access to cardholder data by business need-to-know, and Requirement 8, which mandates assigning a unique ID to each person with computer access before permitting access to cardholder data.

By implementing privileged access management solutions from CA, TIS succeeded not only in complying with PCI DSS 2.0, but also in being able to offer services to secondary users, such as its customer Financial Solutions Group No. 1, whose executive Kyoshi Tsuchida commented: "We have established five types of access to servers containing cardholder data and have clearly segmented the authorization that can be executed in regard to servers by engineers, who can only access data relating to the customers for whom they are responsible. This demonstrates a significant improvement in our security levels, without any sense that the burden of work required to operate the system has increased."

Conclusion

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.

Next Steps

Read the **Privileged Access Management Buyers Guide** from CA Technologies to learn more about safeguarding access and what companies can do to prevent data breaches.

To learn more about Privileged Access Management from CA, visit:
https://www.ca.com/us/products/privileged-access-management.html

Connect with CA Technologies

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success. For more information about CA Technologies go to ca.com.

1 Verizon, "Verizon 2016 Data Breach Investigations Report," April 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

2 Ponemon Institute, "2016 Ponemon Institute Cost of a Data Breach Study," June 2016, https://www.ponemon.org/news-2/71

ca technologies

CS200-298270_0817