WHITE PAPER • SEPTEMBER 2017

ca technologies

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

Table of Contents

Executive Summary	3
Challenge	3
Opportunity	3
Benefits	3
Introduction	4
Your Ever-Expanding Remit	4
What Retail Organization Must Do to Secure Access to Data	5
How Retail Customers Use CA Privileged Access Management	6
Conclusions	6
Next Steps	6

Executive Summary

Challenge

Retail 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 retail 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, 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 Verizon "2016 Data Breach Investigations Report," "the Insider and Privileged User Misuse pattern is one of the few that sees collusion between internal and external (or even partner) actors."[1] The sad fact is that exploited privileged user accounts are a common thread in many data breaches, regardless of whether those accounts were used by external actors with nefarious intent or simply abused by insiders. The retail industry experienced 370 breaches in 2016, according to the report.

As data moves to the cloud, is accessed by third parties and is handled by insiders, the threat grows ever larger, as does the challenge of protecting your organization from evolving threats and staying in compliance with industry, state, 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 noncompliance to actual data breaches from lack of prevention.

According to the Ponemon Institute's "2016 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. The 2014 eBay data breach in which hackers compromised its employees' login credentials, allowing them to access passwords of all 145 million users, not only drove down revenue, but also shook consumer confidence. An article in eWeek reports, "The data breach, which allegedly did not breach any user financial information, still led to somewhat of a crisis of confidence in some eBay users. That's an important thing to note about the true cost of data breaches. It's not just about actual dollars stolen in a theft; it's also about confidence and the overall trust that consumers place in a brand. If consumers are less confident about the security of a given site or service, they won't do as many transactions."[3] Given the intrinsically priceless nature of customer trust and loyalty, both of which are forever obliterated after a breach, you can see just how much is at stake.

Your Ever-Expanding Remit

Retail 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:

1. Preventing data breaches before they happen

The threat from bad actors with compromised privileged credentials is real and growing. Whether they're external (nation-states, cybercriminals, hacktivists) or internal (rogue or hapless employees, 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. 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.

Retail 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 retail companies must implement to mitigate these risks. Thus, they 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:

- **European Union Data Protection Directive (EUDPD)**, which regulates the processing of personal 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
- **U.S. state and federal regulations**, such as those of the Federal Trade Commission protecting consumer privacy and data security

These regulations are just a few of the legal mandates with which retail companies 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 and loss of customer trust, and even the possibility of time in jail, 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 Retail Organizations 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 data they are accessing and why they have access are critical elements to understand.

Many retail 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 a retail company needs is an angry ex-employee with the keys to the kingdom that walks out the door with proprietary data.

With this kind of access oversight and activity insight, retail organizations can combat insider threats as well as external attacks and secure their most precious asset: corporate information.

How Retail 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 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 Privileged Access Manager in the retail industry.

Our customers use CA Privileged Access Manager (CA PAM) to provide enhanced security for authentication and authorization. While most legacy systems in the retail 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, repeatable process of access control.

In addition, CA PAM supports compliance of PCI/DSS requirements regarding access control (for example, Requirements 2, 7, 8, and 10) as well as SOX compliance through tamper-proof audit trails, 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. CA PAM also supports the GDPR requirement that U.K. consumer data is secured with limited access.

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.

Conclusions

To guard against costly data breaches, smart retail companies 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 CA Technologies' **Privileged Access Management Buyers Guide** 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 **ca.com/pam**.

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

2 Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," June 2016, https://securityintelligence.com/media/2016-cost-data-breach-study/

3 Sean Michael Kerner, eWeek, "The Real Cost of the eBay Breach," July 17, 2014, http://www.eweek.com/blogs/security-watch/the-real-cost-of-the-ebay-breach