SOLUTION BRIEF
CA PRIVILEGED ACCESS MANAGEMENT

How Can I Defend my Hybrid Enterprise From Data Breaches and Insider Threats?

ca technologies

Privileged credentials have served as a major attack vector in the successful execution of many breaches. Protecting privileged access is an imperative to successfully defend an organization from a breach and is a core requirement of multiple compliance regimes. CA Privileged Access Management helps drive IT security and compliance risk reduction and improves operational efficiency by enabling privileged access defense in depth—providing broad and consistent protection of sensitive administrative credentials, management of privileged identity access and control of administrator activity.

Executive Summary

Challenge

Many breaches happen because of compromised privileged user accounts. Risks spread like wildfire in the dynamic traditional, virtualized and cloud environments common in enterprises today. One improperly authorized privileged account can cause widespread and irreparable damage to an organization's infrastructure, intellectual property and brand equity, leading to sudden drops in market value, broad organizational disruption and costly compliance penalties. Effectively managing privileged access across your hybrid enterprise is an imperative to reducing security and compliance risks.

Opportunity

CA Technologies helps organizations implement a defense in depth strategy spanning all critical elements of the privileged access management challenge. CA Privileged Access Management provides a comprehensive range of both network-based and host-based privileged access management functionality across the entire hybrid enterprise—including resources in traditional physical data centers, software-defined data centers and networks, as well as the cloud.

Benefits

The financial and reputational benefits organizations gain by effectively managing security and compliance risks, preventing the improper use of privileged accounts and safeguarding high value assets can be significant. CA Privileged Access Management provides multiple layers of defense around privileged identities and credentials at the network and host levels across the hybrid enterprise. These capabilities help organizations actively prevent breaches, facilitate audit and compliance and improve staff productivity and overall operational efficiency.

Section 1:

Defend the Hybrid Enterprise from Breach

An increasing number of data breaches happen because of compromises of privileged user accounts. Standards and regulation bodies, as well as auditors, have recognized the risks associated with privileged users, accounts and credentials and have introduced regulatory changes and audit standards to mitigate these risks.

Unfortunately, cobwebs of insecure legacy practices of administrators sharing passwords or embedding them in automation scripts are difficult to find, cleanup and prevent. Changing compliance requirements have further complicated this goal for total privileged access management and make delaying appealing. But enterprises and government organizations cannot wait any longer. Security and compliance risks are increasing rapidly in growing dynamic and distributed virtualized and cloud environments today. A single breach associated with a comprised privileged account can result in extensive and permanent damage to an organization. High profile breaches can damage an organizations IT infrastructure lead to the theft or loss of intellectual property and the loss of brand equity and customer and business partner confidence—leading to sudden drops in market value and broad organizational disruption.

Data Breaches and Insider Attacks—Unthinkable Damaging Impact to the Business

It's impossible for a day to pass in which we don't hear news of yet another data breach with its resulting loss of proprietary secrets, financial records or personal information. These incidents span all sectors of the economy: commerce, education and government. Already an annual drag on the worldwide economy accounting for hundreds of billions of dollars a year in costs, without immediate and aggressive action it's projected the bill for cybercrime will mount to the trillions of dollars in less than a decade. Beyond reckoning is the devastating impact to individuals who have suffered the compromise of the most intimate details of their personal lives.

Security specialists have striven to establish perimeter-based defenses that, in the most simplistic of terms, keep the bad guys out and let the good guys in. The never-ending string of breaches we're witnessing offers prima facie evidence these perimeters have failed at their primary goal. As a consequence organizations are coming to grips with the realization an essential new layer of security, focused specifically on the protection and management of identities, is a critical new requirement in efforts to stem the tide of breaches. Of these identities, none are so critical as those belonging to privileged users. By providing the "keys to the kingdom," the theft and exploitation of these credentials increasingly serves as the principal attack vector in breach after breach.

Compliance Requirements—Increasing the Risks and Cost of "Non-Compliance"

Regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts. High profile insider breaches along with increasingly advanced persistent threat-based attacks have heightened regulator and auditor attention to privileged user threats. The associated threats include lost, stolen or unauthorized sharing of privileged credentials—the passwords and certificates that ultimately open the door for successful execution of data breaches and attacks.

"By 2017, more stringent regulations around control of privileged access will lead to a rise of 40 percent in fines and penalties imposed by regulatory bodies on organizations with deficient privileged access management controls that have been breached. "

-Gartner Research, Market Guide for Privileged Access Management, 2015

Organizations face increasing pressure to comply with a growing number of regulatory requirements—many of which have specific mandates around management, control and monitoring of privileged access to sensitive data. The Payment Card Industry Data Security Standard (PCI DSS) has explicit requirements for multi-factor authentication, access control and logging, particularly regarding privileged or administrative access to the Cardholder Data Environment (CDE). Health Insurance Portability and Accountability Act (HIPAA) security mandates now include controls for 'business associates' specifically in relation to information access, audit, authentication and access control especially for privileged users. North American Electric Reliability Corporation—Critical Infrastructure Protection (NERC-CIP) requirements include cyber security controls for access to sensitive cyber resources, monitoring of user activity within the protected environment and overall account access management processes.

Operational Inefficiency—Suboptimal, Negative Effect on the Bottom-Line

Implementing and enforcing multiple security controls across a growing and diverse enterprise IT infrastructure across the traditional data center, as well as dynamic virtualized and cloud environments can be increasingly complex, time-consuming and cost inefficient. Managing, controlling and monitoring privileged access can be susceptible to these same challenges. Here are a few examples:

- **Password Management.** Using strong passwords and rotating them frequently is a security best practice. However, the task of rotating these passwords can be time consuming. Automating password changes can eliminate this task altogether.
- **Single Sign-On.** One way to make administrators more productive is by eliminating roadblocks toward faster access to systems that they are authorized to use. Enabling administrators to login once (presumably with strong multi-factor authentication) to access various systems or devices they need to manage saves time and increases productivity.
- **Incident Response and Investigation.** Finding out "who was root on the finance database server at two o'clock on Tuesday?" can be very difficult if the only thing you have is a disparate set of network, server, application, firewall and database logs you have to stitch together. The ability to monitor what actions users are taking and stop unauthorized commands while generating alerts not only reduces risks, it also saves time and overall investigation cost.
- **Audit and Compliance.** Audit and compliance can be tedious and time-consuming endeavors. The time and cost involved in proving compliance with regulatory mandates or meeting an auditor's requirement for due care can be enormous. Dramatically reducing the time required proving adequate protection and management of passwords and monitoring of privileged users and accounts can boost productivity.

Section 2:

CA Privileged Access Management

Data breaches are a big problem today—and they are only getting bigger. The stakes are increasingly higher and we face ever more sophisticated adversaries. Regulatory compliance requirements are increasing and organizations are finding it more and more difficult to cope and comply without straining resources. The security and compliance related processes around managing and controlling privileged access are growing more complex and even harder to manage in the most cost-effective manner. In the face of these significant challenges, what can we possibly do to address them?

The good news is there is a common thread in all of these issues—privileged users and, more specifically, the privileged accounts and credentials those individuals use to configure, maintain and operate our information technology infrastructure. Privileged users are not only considered those people inside the organization with direct, hands-on responsibility for system and network administration. The reality is that many privileged users aren't insiders, they're vendors, contractors, business partners and others who have been granted privileged access to systems within the organization. Additionally, in many cases, privileged users aren't actually people. They can also be administrative credentials that are typically hard-coded into applications or configuration files.

Organizations that are able to acquire the capabilities to prevent the theft and exploitation of these credentials, prove the effective implementation of controls in managing and monitoring privileged access and provide efficient privileged access to IT infrastructure are well on their way to defending their hybrid enterprise from breach, as well as addressing growing compliance requirements and improving operational efficiency.

Key Solution Requirements

An effective privileged access management solution addresses the following requirements:

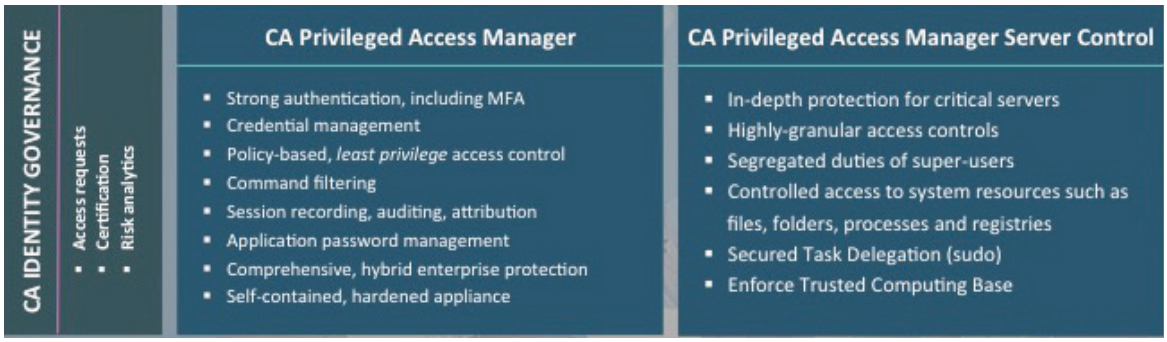
- **Shared account credential management**—managing passwords and ensuring secure storage and access to privileged user passwords; and controlling access to shared accounts
- **Privileged user session management**—establishing privileged sessions (with single sign-on) and monitoring and recording privileged user session activity
- **Application to application password management**—eliminating hard-coded passwords used by applications, automating management of application passwords and providing password audits and activity reporting
- **Privileged user management**—allowing fine-grained filtering of commands and actions by administrators, trusted insiders, third parties and other privileged users

In addition, one key requirement that has gone front and center is the ability **to secure the hybrid enterprise**, as more and more organizations are embracing a combination of traditional computing, virtualization and public-cloud infrastructure to deliver business applications quickly, efficiently and cost effectively. Migrating systems to the cloud or leveraging the scalability and elasticity of cloud computing to deliver entirely new applications, can introduce new sets of challenges. This hybrid cloud changes privileged access management requirements and deployments. An expanded management plane, one that exists beyond traditional perimeter defenses, needs to be protected. Increased reliance on shared security responsibility, calls for a better understanding and use of these models. New technologies and new models over highly elastic, cloud environments require dynamic protection and control. It's clear that securing the hybrid enterprise requires protecting organizations from the security risks and compliance issues associated with privileged users' administrative accounts across traditional, virtualized and cloud IT environments.

Defense In Depth Privileged Access Management Solution

CA Technologies enables privileged account defense in depth, by providing the broadest set of options for customers looking to minimize security and compliance risks by managing privileged identity access and control administrator activity for the hybrid enterprise, delivering:

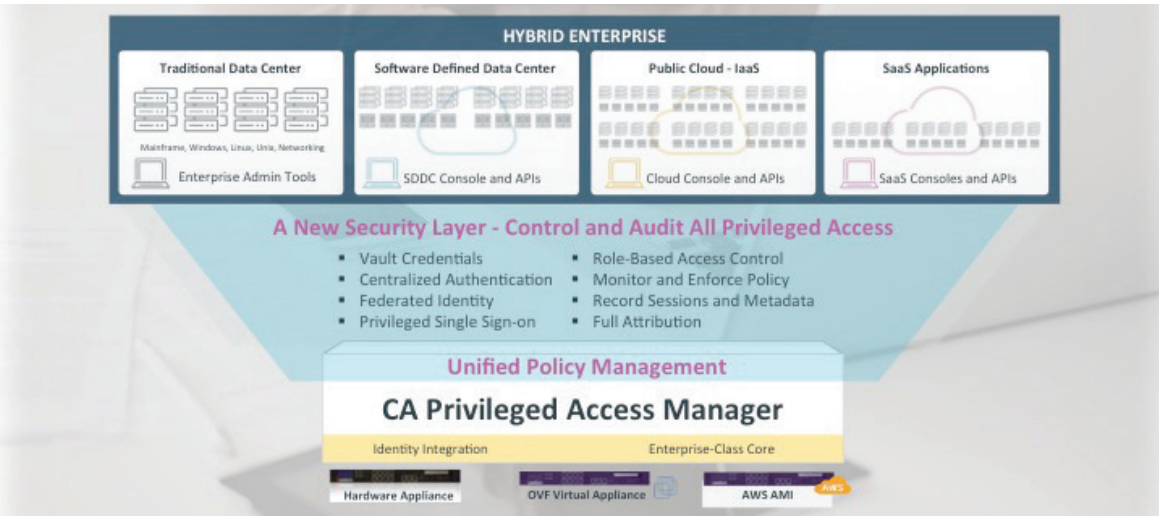
- Centralized, easy-to-deploy privileged access management delivered through a network architecture, enabling credential management, command filtering, session monitoring and session recording
- Localized, very fine-grained access control at the host to further protect high-value resources



Solution Components

CA Privileged Access Manager

CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for privileged access management in physical, virtual and cloud environments. Available as a rack-mounted, hardened hardware appliance, an Open Virtualization Format (OVF) Virtual Appliance or an Amazon Machine Instance (AMI), CA Privileged Access Manager enhances security by protecting sensitive administrative credentials such as root and administrator passwords, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity across all IT resources.



Privileged User Authentication. CA Privileged Access Manager fully leverages your existing identity and access management infrastructure, with integration to Active Directory and LDAP-compliant directories, as well as authentication systems like Radius. Integrated with advanced authentication tools like CA Advanced Authentication and others, it facilitates stronger or multi-factor authentication for privileged users. In addition, CA Privileged Access Manager fully supports enabling technologies like PKI/X.509 certificates and security tokens. Its ability to provide support for Personal Identity Verification/Common Access Cards (PIV/CAC) ensures compliance with U.S. Federal Government HSPD-12 and OMB M-11-11 mandates.

Credential Management. CA Privileged Access Manager protects and manages sensitive administrative credentials. Safely stored in a powerful vault, credentials are encrypted at rest, in transit and in use, limiting the risk of theft or disclosure. All types of credentials, such as SSH keys, not just traditional passwords are vaulted and managed. CA Privileged Access Manager mitigates the risks of passwords hard-coded into scripts and applications, providing its own FIPS 140-2 Level 1 compliant encryption solution and offering integrated FIPS Level 2 and Level 3 solutions.

Policy-based Access Control. CA Privileged Access Manager provides network-based, highly granular and role-based access control for the hybrid cloud. It controls access by network administrators, trusted insiders, third parties and other privileged users. Control begins when privileged users initially authenticate to the system, as CA Privileged Access Manager implements a deny all, permit by exception approach to least privilege access controls. Users are able to see only those systems and access methods to which they've expressly been provided access.

Command Filtering. CA Privileged Access Manager provides network-based, highly granular and role-based access control for the hybrid cloud. It controls access by network administrators, trusted insiders, third parties and other privileged users. Control begins when privileged users initially authenticate to the system, as CA Privileged Access Manager implements a deny all, permit by exception approach to least privilege access controls. Users are able to see only those systems and access methods to which they've expressly been provided access.

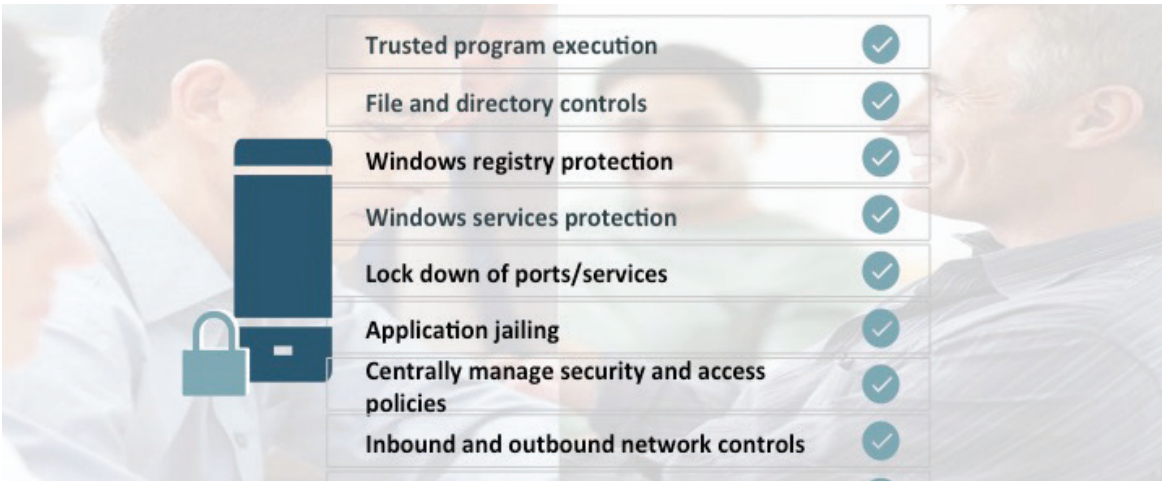
Session Recording. CA Privileged Access Manager provides full resolution capture of privileged user sessions. DVR-like playback controls allow auditors and investigators to review everything that happened during a session, with the ability to jump directly to attempted policy violations. Recording and playback capabilities are provided for graphical RDP sessions, SSH links (including the use of native SSH clients) and Web based applications and cloud management consoles.

Application Password Management. CA Privileged Access Manager eliminates hard-coded, hard-to-change passwords from applications and scripts, providing effective protection and management of these "keys to the kingdom". Application-to-application passwords and other credentials are stored in an encrypted vault, authenticating requesting applications before passwords are released from the vault. Other capabilities include: automation of application password management, encryption of application passwords (in storage, in transit and in use), rapid deployment and integration with application and system infrastructure and detailed password audits and activity reporting.

Hybrid Enterprise Protection. CA Privileged Access Manager delivers tightly integrated privileged identity management capabilities for widely deployed hybrid-cloud computing platforms and traditional systems including: Amazon Web Services (AWS), VMware vSphere and NSX, Microsoft® Online Services and traditional data center systems, including mainframes, servers, databases, networking devices and other infrastructure.

CA Privileged Access Manager Server Control

For organizations with additional security requirements for high-value servers hosting business critical assets, CA Privileged Access Manager Server Control provides localized, fine-grained access control and protection over operating system-level access and application-level access. In addition, it provides agent-based, kernel-level protection for individual files, folders and specific commands based on policy and/or fined-grained controls on specific hosts.



Critical Server Protection. CA Privileged Access Manager Server Control delivers fine-grained controls for critical servers containing sensitive resources by providing file, directory and system process resource protection, kernel-level controls, registry protection and other localized granular server controls, ensuring that high value asset and resources hosted on critical servers are protected from damages caused by either malicious or accidental insider actions.

Host-based Access Control. Operating systems (OS) often lack the ability to restrict and enforce access on high value servers and applications. CA Privileged Access Manager Server Control provides fine-grained access controls that go beyond OS-security, controlling and monitoring how privileged users access and use enterprise data and sensitive resources.

Segregated Duties for Privileged Users. CA Privileged Access Manager Server Control helps organizations implement the security principles of "least privilege" access and "segregation of duties" by providing centralized segregation of duties (SoD) policy management and enforcement and privileged user activity monitoring—ensuring accountability and facilitating regulatory compliance, especially as it relates to SoD mandates.

Secured Task Delegation (sudo). CA Privileged Access Manager Server Control delivers robust, centrally-managed task delegation (sudo) capabilities that help eliminate both the security risk and operational inefficiency associated with sudoers files administration, provide enterprise-class auditing and tracking of user activities and protect against privileged escalation—where sudo restrictions are often times ineffective.

Section 3:

Solution Benefits

CA Privileged Access Management provides a host of capabilities and controls that actively prevent attackers from carrying out key components of their attacks, as well as delivering additional support for reducing risks and improving operational efficiency. More specifically, CA Privileged Access Management provides the following benefits:

- **Reduce risk.** Prevent unauthorized access and limit access to resources once entry is granted to the network. Protect passwords and other credentials from unauthorized use and compromise. Limit the actions users can perform on systems and prevent the execution of unauthorized commands and prevent lateral movement within the network.
- **Increase accountability.** Observe full attribution of user activity, even when using shared accounts. Comprehensive logging, session recording and user warnings capture activity and provide a deterrent to unauthorized behavior.
- **Improve auditing and facilitate compliance.** Simplify compliance by providing support for emerging authentication and access control requirements and limit the scope of compliance requirements through logical segmentation of the network.
- **Reduce complexity and boost operator productivity.** Privileged single sign-on not only helps limit risk, but it can boost the productivity of individual administrators by making it easier and faster for them to access the systems and resources the need to manage. Centralized policy definition and enforcement simplify the creation and enforcement of security controls.

Section 5:

Conclusion

Privileged access, accounts and credentials are core, critical assets for enterprises that must be highly protected through a defense-in-depth strategy that utilizes a combination of technology and processes, which is enabled by privileged access management. Capable of providing multiple layers of defense around privileged users, accounts and credentials—both at the network and host layers, CA Privileged Access Management helps:

- Preserve an organization's reputation by preventing data breaches and by minimizing the impact of any breaches that still occur.
- Address an organization's myriad regulatory requirements, while reducing the cost of compliance with a comprehensive solution that seamlessly integrates with its existing solutions.
- Improve an organization's overall operational efficiency by providing automation and centralized policy management and controls enforcement capabilities.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-169748