SOLUTION BRIEF

How Can I Cost-Effectively Defend My Hybrid Enterprise From Data Breaches and Insider Threats?

ca technologies

Theft and exploitation of sensitive administrative credentials lead to breaches and operational disruption.

CA Privileged Access Manager improves IT security, operational efficiency and compliance with regulations by protecting privileged credentials, defending privileged resources and efficiently monitoring, controlling and managing privileged activities.

Executive Summary

Challenge

To gain access to unauthorized resources, hackers explicitly target privileged user accounts—in part because extra privileges equal more power. Without proper controls, a knowledgeable hacker with just one compromised privileged account can cause widespread and irreparable damage to an organization's infrastructure, intellectual property and brand equity. A single breach can lead to sudden drops in market value, broad organizational disruption and costly compliance penalties. To reduce risks, you need to effectively manage both privileged accounts and privileged resources everywhere.

Opportunity

CA Privileged Access Manager (CA PAM) is a comprehensive privileged access management solution that spans all types of credentials and resources. The solution provides an extensible range of physical, virtual and cloud-based privileged access management capabilities across the entire hybrid enterprise. Unlike other solutions that run on general-purpose servers and require IT staff to purchase and maintain software updates and patches, CA PAM is a complete, highly scalable, certifiably hardened appliance that delivers exceptional performance, reliability and efficiency at the lowest TCO.

Benefits

Organizations can retain or gain significant financial and reputational benefits by effectively managing risks, preventing the improper use of privileged accounts and safeguarding high-value assets. CA PAM provides multiple layers of defense around privileged identities and credentials at all layers of the technology stack to prevent breaches, facilitate audit and compliance, and improve staff productivity as well as overall operational efficiency across the entire hybrid enterprise.

Section 1:

Defend the Hybrid Enterprise From Breach

As evidenced by recent hacks on the U.S. government, the Democratic National Committee and many companies, attacks are getting more sophisticated. Well-organized attackers are funded by organizations seeking political or industrial espionage, disruptions and terror. Privileged identities and credentials are frequently used in successful breaches, which is why regulators have been raising the information security bar with more comprehensive requirements for privileged credentials and protection of critical resources.

The movement to the cloud exacerbates problems with privileged accounts, as the number of privileged accounts and resources increase.

Organizations often have a portfolio of IT resources composed of internal systems, external private and public cloud resources, and hosted applications to cost-effectively solve business problems. For example, one large financial services organization with hundreds of thousands of employees and thousands of systems has operations and data centers distributed around the world. The company is using UNIX®-based, on-premise core banking applications; others are virtualized using VMware vSphere. Some applications are available over Citrix XenDesktop Virtual Desktop Infrastructure. Others are running native on Microsoft® Windows® servers and Windows desktops. The company's application developers use Amazon Web Services (AWS) and various development tools and services. IT operations use a number of deployment, monitoring and automation tools. The end users use Microsoft Office 365®, WebEx and other hosted applications. Protecting this heterogeneous environment is a huge challenge.

The many forms of privileged accounts

Each resource and application has its privileged users and each presents a new attack surface. Infrastructure management tools, such as VMware vCenter, Amazon Management Console, Microsoft Management Console and respective APIs present the biggest challenges. The automation achieved with these platforms to speed up resource deployment has increased velocity and scale of changes in the hybrid infrastructure, making it more difficult to protect. These complex infrastructure and application landscapes require new, industrial-strength tools designed to effectively protect privileged accounts and to automatically respond to suspicious activities.

Compliance requirements—increasing risks and cost of non-compliance

As attack vectors increase, regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts in all environments. As a result, 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.

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

—Felix Gaehtgens, Gartner, "Market Guide for Privileged Access Management," Aug 2, 2016

For example, the Payment Card Industry Data Security Standard (PCI DSS) has explicit requirements for multifactor authentication, access control and logging, focusing on privileged or administrative access to the cardholder data environment (CDE). Health Insurance Portability and Accountability Act (HIPAA) security mandates include controls for access, audit, authentication and access control, especially for privileged users. North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) includes controls for access to sensitive cyber resources, monitoring of user activity within the protected environment and overall account access management processes. In fact, most regulations mandate authorization, authentication, audit and centralized management.

Regulatory Mandates

	PCI DSS	HIPAA	NERC CIP
Authentication and credential management	✔	✔	✔
Authorization and restriction of privileges	✔	✔	✔
Audit, monitoring, compliance reporting	✔	✔	✔
Management and integrations	✔	✔	✔

Piecemeal security increases costs and inefficiencies, reducing effectiveness

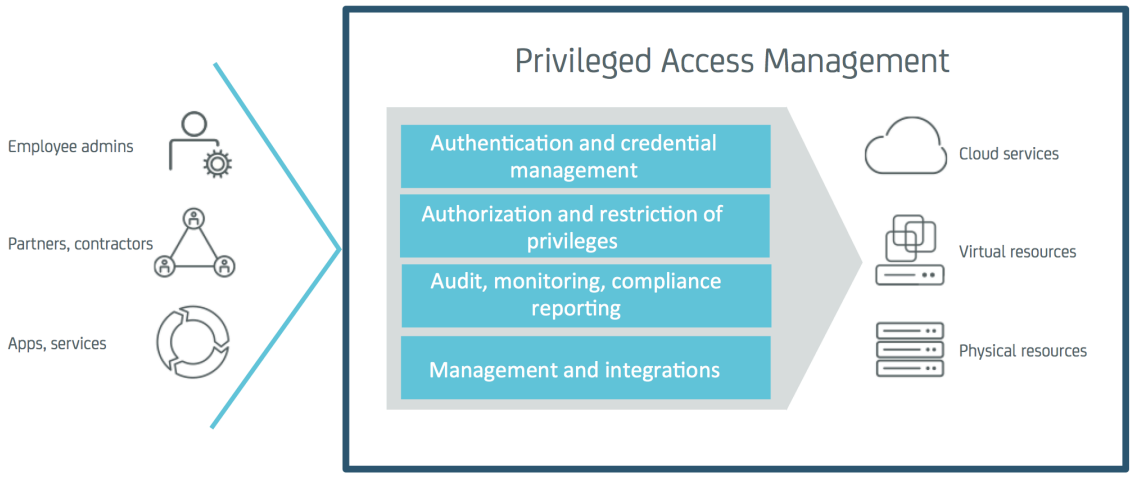
As IT architectures continue to evolve to include software-defined data centers (SDDCs) and other more complex hybrid environments, knitting together point solutions for each environment can be a costly and risky proposition. More and more organizations are embracing a scalable, industrial-strength privileged access management solution that efficiently protects privileged identities and critical resources across the infrastructure stacks (physical, virtualized, cloud-based), applications and web services.

Section 2:

The Solution: CA Privileged Access Manager

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

The four broad areas of capabilities include authentication, authorization, audit and management. The next sections will explore each of these areas in more detail.



Authentication and credential management

CA PAM protects and manages sensitive administrative credentials. Safely stored in a vault, credentials are encrypted at rest, in transit and in use, applying best practices and limiting the risk of theft or disclosure.

Privileged user credentials. You can vault passwords and other sensitive credentials, including SSH keys, AWS credentials and PEM–encoded keys in a credential safe, so they're not revealed to users or exposed to potential malware. Instead, securely vaulted credentials are passed directly between CA PAM and target resources, eliminating the risks of stolen or compromised passwords. CA PAM can enforce password strength, mandate lifecycle management (frequency of password changes) and require multifactor authentication based on the user's role or application sensitivity.

Credential storage and management
▪ Stores encrypted credentials (passwords, etc.) so users don't know them
▪ Provides the credentials to authorized users
▪ Rotates credentials, based on policy
▪ Provides an API for applications and automation scripts

Shared account and full attribution of actions. Shared accounts are typically used for administration, operation and maintenance of shared resources. But, shared accounts, such as "root," don't provide accountability, resulting in increased security risk as well as compliance challenges. CA PAM enables full attribution for shared account activities to individual privileged users. The system separates user authentication from shared account access, linking session–based clicks, commands and entries to individual users, not just system–based admin accounts. Compliance with regulations becomes simpler because each action can be associated with a single identity, providing full accountability for privileged actions.

Application–to–application credentials. CA PAM eliminates hard–coded, hard–to–change passwords from applications and scripts, providing effective protection and management of these so–called "keys to the kingdom". Application–to–application passwords and other credentials are stored in an encrypted vault. CA PAM authenticates requesting applications using optional multifactor authentication before releasing passwords from the vault. The solution automates application password management, encrypts application passwords (in storage, in transit and in use) and integrates with applications and infrastructure, capturing detailed password audits for activity reporting.

Privileged user and privileged application authentication. The solution ensures privileged users are accurately authenticated, leveraging existing identity and access management infrastructure. Through integration with directories, authentication systems and devices, CA PAM facilitates compliance with maximum–security protections.

Supported authentication schemes, identity stores and federation services
▪ Amazon AWS Identity and Access Management (IAM)
▪ CA Advanced Authentication
▪ CA Directory
▪ Federation using Active Directory Federation Services (ADFS) and Security Assertion Markup Language (SAML)
▪ Hardware security modules (HSM)
▪ LDAP v3 compliant directories (e.g., Open LDAP, RHDS, Novell eDirectory)
▪ Microsoft Active Directory®
▪ PKI/X.509 certificates and security tokens
▪ Radius
▪ Red Hat Enterprise Linux 389
▪ RSA SecureID
▪ TACACS+

Federation. CA PAM federates identity and attributes between you, your suppliers, customers and business partners, eliminating inefficiencies, improving user productivity and experience, and enhancing overall security. Support is available for popular standards such as SAML, as both a service provider and an identity provider, simplifying interoperability between organizations.

Authorization and restriction of privileges

IT shops have been consolidating, virtualizing, outsourcing and moving to the cloud to improve efficiency and costs. These initiatives introduce additional information security challenges for controlling privileged accounts and management consoles. With centrally managed, fine-grained access control policy, CA PAM simplifies enterprise-wide authorization across all of the hybrid enterprise resources for suppliers, customers and business partners.

CA PAM provides highly granular and role-based access control for physical, virtual and cloud resources using command filtering, socket filtering, CA PAM Server Control and extensions for VMware, AWS and other applications.

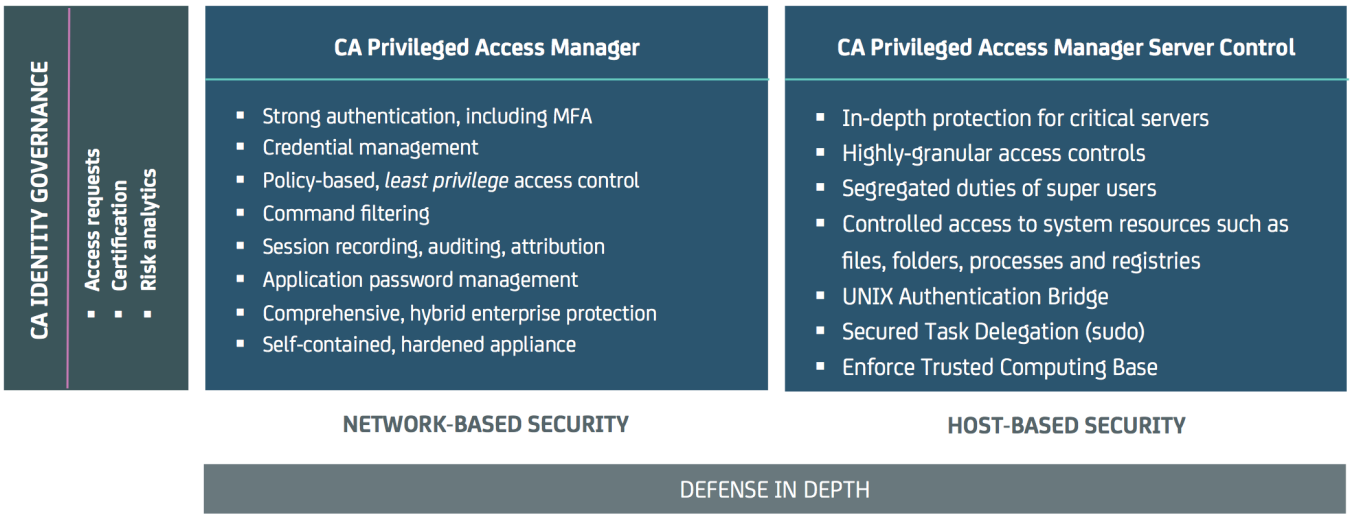
Command filtering. Control begins when privileged users initially authenticate to the system, as CA PAM implements a deny-all, permit-by-exception approach to least-privilege access controls. Using predefined black and white lists, privileged users see only expressly permitted systems and access methods. Unauthorized commands are blocked and logged, non-complying users may be warned and the security team alerted about policy violations.

Socket filtering: When a user attempts to open a socket to an unauthorized device or server on the network using interactive protocols such as Telnet, SSH, re-login, Remote Desktop Client, the solution detects the attempt to create an outbound socket and blocks it. With socket-level monitoring capabilities, CA PAM detects leapfrog attempts, regardless of the command used, effectively detecting and terminating a program establishing an unauthorized connection to another device on the network.

CA PAM Server Control for extra protection. CA PAM Server Control delivers localized, fine-grained controls required for regulatory compliance and risk management. Using centrally managed task delegation and platform-specific software restrictions, CA PAM Server Control provides file, directory and resource-specific protection, kernel-level controls, registry protection and other localized granular controls to ensure that high-value asset and resources hosted on critical servers are protected from damages caused by either malicious or accidental insider actions.

- SoD for shared root and admin accounts. Similarly, the use of shared accounts (such as root and admin) frequently results in privileged users having unnecessary access to critical servers, systems and data. Operating systems do not have the ability to restrict actions and access for multiple people using a shared account. CA PAM provides centralized SoD policy store to ensure that administrators have only the privileges they need. A combination of CA PAM and CA PAM Server Control enforces SoD policy, generating a granular audit trail—including tracing actions made using superuser accounts back to the individual users.
- Centralized and secure replacement of sudo for both *nix and Windows environments. The sudo command on UNIX and Linux® systems allows users to run commands with elevated privileges. Additionally, Windows runas does not provide the same level of control as sudo provides, and is generally managed on a per-system basis. CA PAM Server Control provides a secure and centrally managed replacement for sudo and provides equivalent capabilities for both *nix and Windows platforms.

The combination of CA PAM and CA PAM Server Control provides a comprehensive defense in depth against breaches and improper administrator actions. Only CA offers both network-based and host-based security in a unified, integrated solution. When used with CA Identity Governance, the solutions provide not only management but governance of privileged users. So, improper entitlements are identified and remediated quickly, while improper administrator actions are also prevented.



VMware vSphere, NSX and the private cloud. CA PAM for VMware is available as an OVA and is fully integrated with VMware management environments. The solution enhances VMware's native security capabilities and adds fine-grained access control and privileged credential management to VMware vSphere server management console and guest systems. CA PAM for VMware NSX extends its broad support for VMware by enhancing the security of VMware NSX Manager and NSX REST APIs.

AWS, AWS APIs and the public cloud. CA PAM for AWS and CA PAM for AWS Management APIs are available as an AMI and fully integrated with AWS Management Console. These CA products enhance AWS' security groups and network access control lists to better protect AWS EC2 environment by monitoring and recording privileged user activity and access to AWS Management APIs. By proactively enforcing separation of duties, the CA solution provides full password and credential management, and enables a single point of privileged access management—either on premises, in AWS Virtual Private Cloud (VPC) or in AWS EC2 instance with CA PAM and AWS Direct Connect.

Physical, virtual and cloud access control
▪ On-premises infrastructure support – Controls which systems the user can access with privileged credentials – Automatically logs the user into the protected resource – Makes video recordings of the session – Provides PAM administrator with ability to terminate sessions
▪ VMware support – Automatic discovery of VMware vSphere and NSX resources – Protection for vCenter Server management console and vSphere workloads – Protection of VMware NSX Manager and Controllers – Dynamically link security groups – Service Composer integration – Restrict access via NSX Distributed Firewall – Protect and audit NSX REST APIs
▪ AWS support – Automatic discovery of EC2 instances – Protect AWS Management APIs – Federate AWS Management Console – Record AWS Management Console sessions – Apply unified, cross-platform privileged user credentials protection

SaaS and other applications. CA PAM provides out-of-the-box session and credential management support for Microsoft Online Services Office 365 administrative console, IBM DB2®, Microsoft SQL Server®, Oracle database, MySQL, and PostreSQL, as well as Apache, IBM and Oracle web servers. Interfaces are available for BMC Remedy, ServiceNow, HPE Service Manager, Salesforce, ServiceCloud and Sybase. APIs can be used to quickly and easily create other security-compliant interfaces.

Audit, monitoring and compliance reporting

CA PAM provides extensible, enterprise-wide recording, controlling, auditing, threat detection and automated response capabilities for a wide variety of environments, including cloud management consoles and web-based systems, to simplify monitoring, prevention, audit and compliance.

Definitive record of monitored activities. CA PAM establishes and controls a remote session, while monitoring and recording privileged user activity over common protocols. Captured recordings are immediately available for real-time analysis and response. Similar to best practices in physical security, video monitoring with DVR-like playback controls are increasingly used by auditors and investigators to review everything that happened during the suspicious session, with the ability to jump directly to attempted policy violations, which helps simplify and accelerate responses and investigations.

Analytics for automatic detection and mitigation of threats. CA Threat Analytics for PAM leverages user behavior analytics to detect and stop external hackers and insider threats. The solution enables enterprises to detect and stop privileged user account breaches using technology similar to what banks use to detect and stop credit card fraud. The machine learning and advanced algorithms provided by CA's threat analytics solution continuously assess the behavior of privileged users and compares it to their own historical actions, as well as to the behavior of other users, to accurately identify attacks and high-risk activities. For example, identifying and mitigating the risk posed by users who are surveying high-value assets or trying to exfiltrate data off of sensitive servers. When high risk or malicious activity is detected, the solution uses automatic controls—including triggering session recording, forcing session re-authentication and real-time alerting—to mitigate the issue and protect the enterprise.

Management and integrations

CA PAM can manage information security policy for hundreds of users quickly and efficiently. It's designed with clustering, load-balancing and fail-over capabilities to provide reliability, performance and scalability.

Quick deployment and provisioning. During initial deployment or when consolidating a merger or an acquisition, you accelerate time-to-value by preloading users, devices, roles, services and policies using simple CSV files, imports and autodiscovery features.

Efficient management and deprovisioning. CA PAM automates ongoing user and system management, scanning your infrastructure for unmanaged systems, services and accounts. The solution facilitates ongoing, regular reviews of all privileged accounts and credentials, including orphaned accounts, passwords and new accounts with excessive privileges. New privileged accounts can be quickly and efficiently provisioned and obsolete accounts are quickly deprovisioned.

Efficient privileged user governance using CA Identity Governance. An interface between CA PAM and CA Identity Governance automates and streamlines the process of reviewing each privileged user's elevated privileges for each resource, improving overall security and simplifying removal of unneeded privileges.

APIs for custom integration for increased automation. CA PAM supports most common environments out of the box. Additionally, fine-grained access control capabilities can be easily added to your custom applications and unique systems using APIs.

Key integrations
▪ Identity and access management (IAM) – User provisioning and deprovisioning – Orphaned account discovery – Account certifications and accreditations
▪ Security information and event management (SIEM) – Privileged user activity logging and forwarding onto SIEM tools – Real-time monitoring, correlation, alerting, response and remediation – Historical reporting and forensics investigation
▪ IT service management (ITSM) – Validate administrative access requests using ITSM tools – Control authorizations or incident reports using ITSM tools

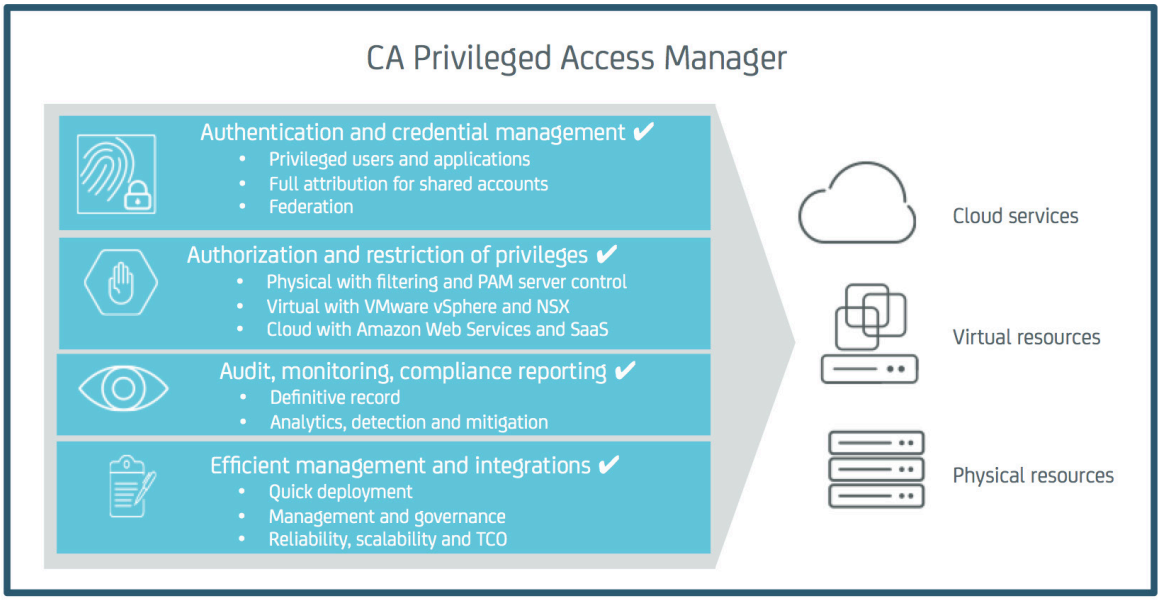
Reliability, scalability and TCO. CA PAM is designed to provide high availability, performance, scalability and disaster recovery capabilities, addressing situations where enterprises need to change hundreds of passwords quickly due to mergers, joint partnerships, divestitures or outsourcing arrangements.

Section 3:

Solution Benefits

CA PAM provides the capabilities and controls necessary to prevent breaches, while reducing risks and improving operational efficiency. The solution controls the actions of your privileged users, while providing full monitoring and auditing capabilities for improved compliance. Along with CA PAM Server Control, CA PAM provides a comprehensive defense-in-depth platform that can help reduce the risk that your organization will become the next victim of a high-profile breach.

In addition, in August 2016, CA PAM was the first and only security solution for controlling, monitoring and auditing privileged user access to attain Common Criteria certification outlined in the National Information Assurance Partnership (NIAP) Protection Profile for Enterprise Security Management-Policy Management. This certification confirms that CA PAM meets rigorous predefined security requirements, giving organizations a well-defined and clearly articulated level of confidence in the solution.



The success of our customers speaks for itself. For example, the large financial services organization mentioned earlier had outsourced its IT operations to a third party. To comply with appropriate policies and regulations, the organization chose CA PAM to ensure that the outsourcer's staff only performed authorized activities. The financial services firm achieved its cost-cutting, efficiency, security and compliance goals, and is now expanding its CA PAM deployment outside of North America. Your organization can achieve similar results.

Section 3:

Conclusion

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

To learn more about CA PAM, visit ca.com/PAM

ca technologies

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.

CS200-243452_1216