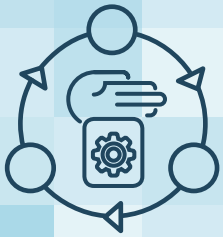
BUYER'S GUIDE | MAY 2016

Privileged Access Management

ca technologies

Table of Contents



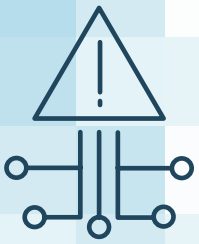
The Privileged Access Management Landscape

Overview:
Privileged Access Management

Over the last few years, privileged access management—a collection of control, monitoring and audit capabilities focused on mitigating the risks associated with privileged users, accounts and credentials—has emerged as a high priority undertaking for organizations of all kinds. This surge of interest and attention has been driven by multiple factors:

- **Data Breach Prevention.** While cybercrime remains a large and growing challenge, security professionals now increasingly face the daunting task of fending off nation state attackers undertaking espionage. Compromised privileged credentials have been revealed as a primary attack vector in many security incidents. Privileged credentials are also a critical requirement for attackers seeking to move about in breached networks in a hunt for valuable assets.
- **Managing Insider Threats.** The relative number of security incidents resulting from rogue insiders is low. But, given the high level of trust and wide-ranging access insiders typically enjoy, the impact of an insider breach incident can be quite high.
- **Regulatory Compliance and Audit.** As the role of insiders and compromised accounts and credentials in security incidents has become clear, regulatory bodies and auditors have focused added attention on the controls and processes organizations implement to mitigate these risks. Failure to address these concerns can result in costly penalties and critical findings to remediate.
- **Hybrid IT Infrastructure.** Virtualized and cloud-based IT infrastructure offer organizations a number of benefits. But the large number and dynamic nature of resources typically deployed in such environments, and the presence of powerful management consoles and APIs, can expand the available attack surface requiring protection and defense.

Today, more than ever before, you need an easy-to-deploy solution that provides comprehensive privileged access management with credential management, strong authentication, zero-trust access control, proactive command filtering, session monitoring and recording, and fine-grained controls over high-value servers. The right privileged access management solution provides protection across the broad hybrid IT infrastructure deployed in most organizations today. This infrastructure includes not only the traditional physical data center (e.g., servers, networking devices, databases, switches and related resources) but also growing virtual and cloud deployments. There, it's essential to provide protection for both the underlying management infrastructure and resources deployed in software-defined data centers and networks, infrastructure as a service (IaaS) environments and software as a service (SaaS) offerings.

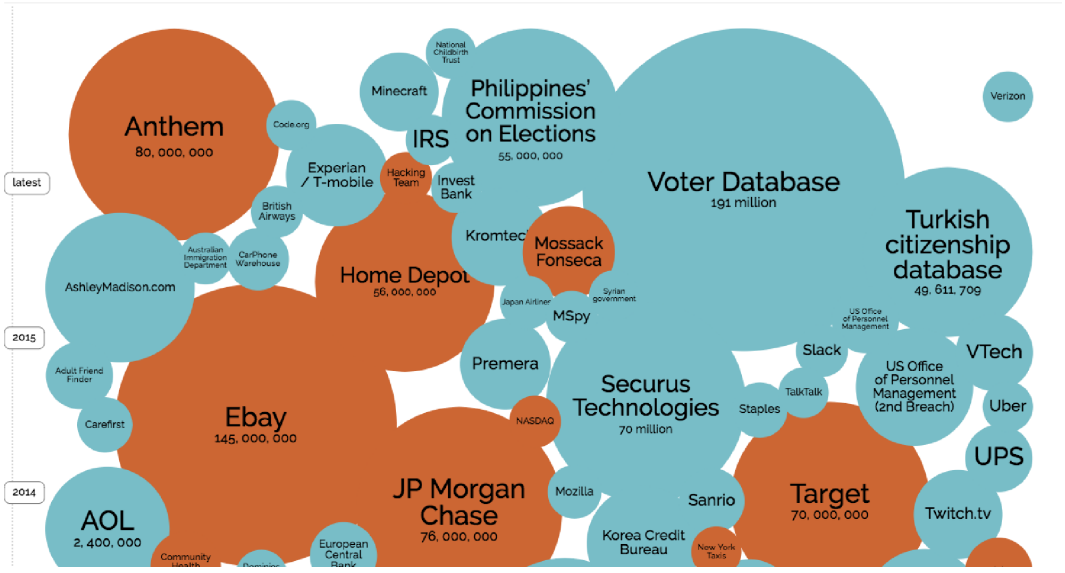


The Continuously Evolving Nature of the Threat

The Continuously Evolving Nature of the Threat

The number and frequency of digital security threats has increased immeasurably over the past decade. And the nature of breaches has also evolved. Today, the most common cause of a data breach is a cyber attack. These attacks are constantly changing. For years, organizations have largely been concerned about incidents driven by criminal undertakings. More recently, a growing number of attacks, frequently driven by political and social concerns, became laser-focused on disrupting business operations. The 2015 U.S. Office of Personnel Management (OPM) attack showed signs of the latest and far more dangerous trend: cyber espionage, where hackers' larger strategy was to gather extensive personal histories of individuals seeking security clearances. As all signs point to the rapid evolution in number, severity and sophistication of attacks, we need to continue developing better defenses.

Millions of identities breached



Breaches and attacks continue to escalate in frequency, severity and impact. Affected organizations may suffer from lost market capitalization, lost sales, lost profits, and damage to customer goodwill and brand equity.[4]

The Threat Actors

Security teams must defend against a wide range of attackers and threat actors—all of whom have varying skill levels:

- **State-sponsored attackers** seek to steal sensitive information and disrupt critical infrastructure and operations of the targeted country or organization. These attacks are generally the most sophisticated. Recent examples of such incidents include the Ukraine power plant hack where hackers cut power to more than 80,000 people;[1] the Sony Picture attack, attributed to North Korea; and the Iranian attempt to hack U.S. banks and a New York dam.[2]

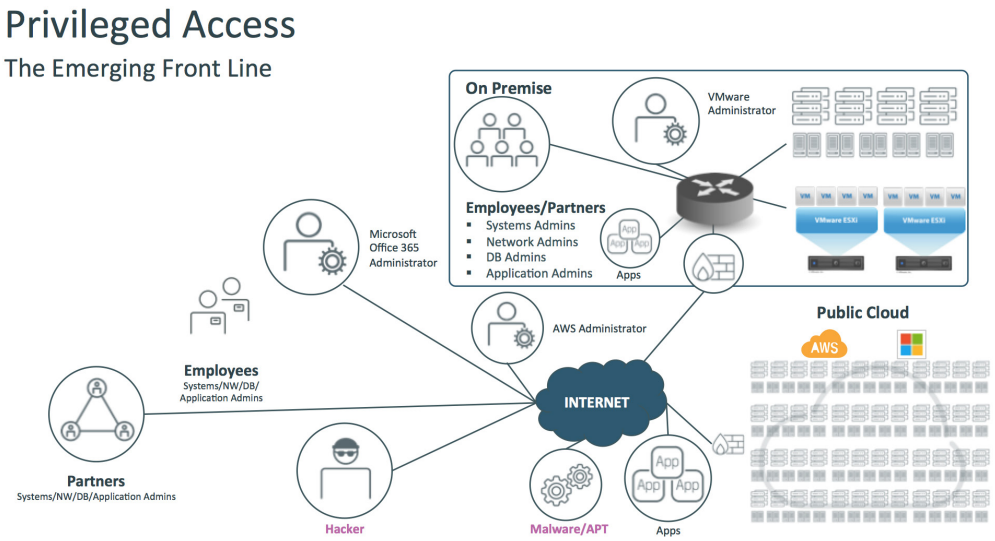
- **Cyber criminals** seek to gain profit by converting stolen data into cash or cash equivalent benefits, which can lead to lost sales, strategic partner hijacking, counterfeit products, patent infringements and negotiation disadvantages, just to name a few. A typical breach could impact an organization's public reputation and stakeholder confidence; its market share, revenue and profit; and reduce return on capital and R&D investments. The Target incident, and a host of other retail breaches, were examples of cyber criminal attacks.
- **Hacktivists** often seek to damage the reputation of an organization. They use the same tools and techniques as hackers, but do so in order to disrupt services and bring attention to a political or social cause. Edward Snowden, who distributed classified information from the National Security Agency, is a well-known example of an insider hacktivist. However, government agencies are not the only targets, as evidenced by a recent hack into university network printers to print flyers with swastikas and anti-Semitic text at several U.S. universities, including Princeton and Brown.[3]

Managing Insider Threats

Malicious Insiders can fall into any of the three categories listed above. Although a relatively small portion of the overall number of breaches is attributed to malicious insider attacks, they do occur and can inflict significant damage, including:

- Modification or theft of confidential/sensitive information for personal gain
- Theft of trade secrets or customer information to be used for business advantage or to give to a foreign government or organization
- Sabotage of an organization's data, systems or network

Privileged access is at the core of many of these incidents because privileged accounts have more authority and access to resources, which simplifies the attainment of intruders' goals. Intruders want the credentials used by privileged users to configure, maintain and operate the IT infrastructure. Armed with greater access to the network, while having fewer oversights and controls, privileged users can access more intellectual property and other high-value or sensitive corporate information. Given the ability to easily get around controls that restrict non-privileged users, privileged users present greater risk.



A critical success factor for attackers, privileged accounts are a common thread among the various attacks over the years. But managing and controlling privileged users can be a challenge to many, because privileged users as a population can be so diverse. They can include privileged insiders, privileged outsiders that represent third-party vendors, partners and contractors, and even privileged credentials that are hardcoded in applications—all of them having superuser access to critical data across your hybrid enterprise.

Regulatory Compliance and Audit: Data Breaches Complicate Compliance

Lost, stolen or inappropriately shared privileged credentials ultimately open the door to successful data breaches and attacks. These high profile insider breaches, along with increasingly advanced persistent threat attacks, have heightened regulator and auditor attention to privileged user risks. As a result, regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts.

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 multifactor authentication (MFA), 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. 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.

Hybrid IT Infrastructure: Raising the Stakes for Security

Known as the combination of traditional computing, virtualization and public-cloud infrastructure, the Hybrid Enterprise is architected to efficiently and cost-effectively accelerate the delivery of business applications. Unfortunately, the hybrid enterprise expands the attack surface. The scalability and elasticity of cloud computing introduce new challenges. Shared security responsibilities, highly elastic cloud environments and the rest 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.

Where To Start

Protecting The Keys to the Kingdom: Privileged Credentials

Threats are widespread and projected to get worse. Faced with pressure to protect the crown jewels of your organization and defend your high value, sensitive resources from cyber threats and attacks, you need to know where to start.

First, you must understand your environment and determine what types of privileged users you have. Because unmanaged privileged accounts are a significant source of risk, you need to know who is involved, who needs to be included and what resources need protecting. To start, answer the following questions:

- Are you concerned about the data center?
- Are you managing resources in the cloud?
- What specific IT environments need protection?
- Who are your privileged users?
- What are the appropriate authentication methods to verify privileged users' identities?

Because shared administrative accounts are commonly used, the ability to support attribution of actions taken using such an account back to a specific individual has become a compliance requirement.

Privileged accounts are not only employees with direct, hands-on responsibility for system and network administration. Many privileged account holders are vendors, contractors, business partners and others who have been granted privileged access to systems within your organization. In many cases, privileged accounts are not people at all. They may be applications or configuration files empowered by hard-coded administrative credentials.

Safeguard Privileged Credentials Using Stronger Authentication

A logical starting point enforces stronger authentication through a network-based gateway that integrates with existing identity management stores, like Active Directory, LDAP directories or even RADIUS or TACACS+. MFA for privileged access significantly increases the level of difficulty for an attacker to gain access to your network and is now a compliance and audit requirement in a variety of compliance mandates, including the most recent revision to the PCI-DSS.

Some systems may not need MFA but still need more protection than static passwords. A privileged access management system can provide a credential safe where passwords and key pairs are stored encrypted, away from prying eyes and malicious users. These credentials can be actively managed by the privileged access management system, interacting with protected systems to change passwords based on standards appropriate to your organization's or resource's level of risk. Automating this process decreases both security and operational risks, because automated password and key updates are less error prone. When combined with privileged user single sign-on, a high level of security can be achieved, providing a user with access to a system but without giving them the actual system credentials.

Next, you need to define acceptable access policies and anticipate possible violations, such as:

- What types of activities are legitimate and which ones are not
- Of the legitimate activities, which ones are the most risky or error-prone
- Alternatively, what types of activities should never occur
- What leapfrog-prevention limits are needed to prevent the use of one system as a launch point for additional attacks

Limit Privilege Escalations, Reconnaissance and Lateral Movement

With zero-trust access control, you can separate authentication from access to the protected system. Users would only have visibility to those systems and resources as defined and permitted by policy. By proxying or brokering sessions between the privileged access management system and managed resources, you can limit the authority people have over a system and control the commands they are able to issue, restricting their ability to escalate privileges or move laterally within the network.

Host-based agents can provide more fine-grained access controls than what's available in the system's native access control scheme. You can restrict access to files and directories or monitor files for modifications. You can also prevent attempts to move laterally within the network. For example, having gained access to a system, an attacker might attempt to issue an SSH or TELNET command or open a remote RDP session to a target system. You may want to develop policies that would prevent these from occurring and log the attempted violation.

Once controls are in place, certain activities need monitoring and controlling, including:

- What actions need monitoring and supervision
- How frequently sessions need monitoring
- Under what circumstances these sessions need to be reviewed
- Who will review the activities and develop an action plan

Monitor, Record and Audit Activity

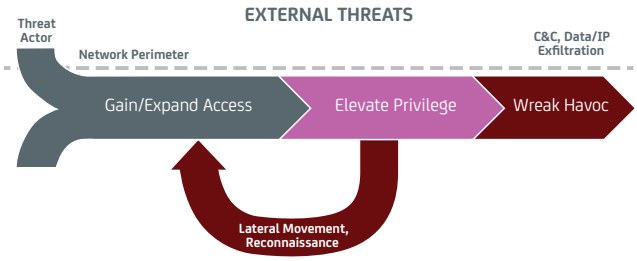
Monitoring, recording and auditing activity is an additional deterrent to breaches. Session recordings are helpful in reviewing activities and determining what actions occurred; immediate playback can speed up investigation, troubleshooting and recovery. Alerts and events can provide immediate warnings of policy violations and attempted breaches, enabling a rapid response. Additionally, logs can be analyzed, either individually or via a security information and event management (SIEM) system, in the context of other activity, enabling investigation and helping to prevent breaches from occurring.

By safeguarding privileged credentials, preventing privilege escalation and monitoring privileged activity for investigations and regulatory compliance, you can break the attack-kill chain and prevent the attack from turning into a breach.

Getting to Know the Kill Chain

What is a kill chain? It's the series of steps an attacker typically follows when carrying out a breach.

While the chain can comprise numerous steps, there are four key ones in which privileged credentials represent the **cornerstone of an attack**. These include:



GAIN AND EXPAND ACCESS: To access the network, insiders might exploit the credentials they already have, while outsiders will exploit a vulnerability in the system (e.g., via a spear-phishing attack) to steal the necessary credentials.

ELEVATE PRIVILEGES: Once inside, attackers will often try to elevate their privileges, so they can issue commands and gain access to whatever resources they're after.

INVESTIGATE AND MOVE LATERALLY: Attackers rarely land in the exact spot where the data they're seeking (e.g., credit card records, personal information, etc.) is located, so they'll investigate and move around in the network to get closer to their ultimate goal.

WREAK HAVOC: Once they have the credentials they need and have found exactly what they're looking for, the attackers are free to wreak havoc (e.g., theft, business disruption, etc.).

Break the Kill Chain and Prevent the Breach

Breaking the kill chain is essential to preventing breaches and limiting damage. A combination of individual utilities for session recording, a password vault and access control system can address pieces of the overall problem. Unfortunately, this piecemeal approach introduces a lack of integration and coordination between the pieces. The lack of cohesiveness of the piecemeal solution has led to the introduction of integrated Privileged Access Management, a critical security discipline with processes, technology and management oversight that make the entire solution work together better as a whole.

Cohesion and integration of strong authentication, access control, filtering and monitoring can detect policy violations and/or data breach attempts anywhere in the hybrid enterprise to protect your sensitive assets. Examples include:

- Stronger authentication and credential management to safeguard privileged credentials
- Policy-based controls to ensure implementation of least-privilege access controls
- Command and socket filtering to limit privilege escalations, reconnaissance and lateral movement
- Privileged session management and recording to monitor, record and log activity for investigations and regulatory compliance

How To Evaluate Privileged Access Management Solutions

Safeguard Privileged Credentials

Careful, complete authentication of privileged users is a critical first step in a privileged access management initiative. Positively confirming the identity of privileged users forms the foundation for subsequent permissions and controls. You can take full advantage of your existing identity access management (IAM) infrastructure to authenticate users, based on group memberships. You can enforce composite MFA techniques to comply with requirements for stronger authentication for privileged access. You can federate user identity to eliminate multiple islands of identity across different parts of the IT infrastructure, enhancing overall security and reducing administrative costs. Support for hardware security module (HSM) options provide higher levels of security and assurance when managing encryption keys. Other enhanced authentication options include one-time passwords (OTPs), delivered by phone or via email, where you can implement advanced authentication capabilities, such as dynamically deciding whether to authenticate or to elevate authentication requirements, based on a new device ID, location, or a combination of factors.

Privileged User Authentication	CA	Others
Leverages your existing IAM infrastructure for authentication	✓	
Supports and integrates with:	✓	
— LDAP v3 compliant directories like Active Directory, Open LDAP, RHDS,	✓	
— MFA systems like Radius, TACACS+, RSASecureID, CA Advanced Authentication	✓	
— PKI/X.509 certificates and security tokens	✓	
— PIV/CAC for HSPD-12 and OMB M-11-11	✓	
— Identity federation including support for SAML and ADFS both as Service Provider and Identity Provider	✓	
— Amazon AWS Identity and Access Management	✓	
— Hardware security modules (HSM)	✓	

Credential management must provide an encrypted and hardened password safe or vault for storing credentials. It manages passwords of administrative, shared and service accounts by changing them at configurable intervals, according to policies. It controls administrators' access to shared accounts, ensuring that passwords for shared accounts are not shared. It keeps an irrefutable audit trail of privileged account document usage. It supports break-the-glass scenarios for emergency and disaster recovery purposes, including firecall accounts.

Many types of keys also serve as credentials or tokens to confirm identity. These tokens operate like passwords and are subject to similar threats, risks and challenges, such as copying, sharing, unintended exposure and unaudited backdoors. Organizations should use many of the same controls to manage and protect passwords to these alternate credentials, moving authorized keys to protected locations, rotating all keys regularly, enforcing source restrictions for authorized keys, and enforcing command restrictions for authorized keys. Privileged access management systems' capabilities to account for alternate credential types, including SSH keys and the PEM-encoded keys used to access AWS resources and management consoles are essential to cover risks and threats. These credentials need to be vaulted, rotated and controlled by configured policies, and retrieved and used to minimize the potential theft or exposure.

Numerous applications and systems access sensitive resources, such as other applications or databases, by embedding associated credentials into automation scripts or by using a run-time configuration file. Neither option is particularly secure. The privileged access management system can protect application-to-application use cases by facilitating interactions between privileged applications. The system registers privileged applications, uses dynamically retrieved passwords to authenticate and verify their integrity prior to facilitating access, and subsequently protects these sensitive passwords while they are in memory on the local system. By leveraging application-to-application capabilities, you can more effectively eliminate insecure application-to-application credentials by vaulting them centrally, automate application-to-application credential management and policy enforcement, and simplify related audit and compliance activities.

Application-to-application passwords, keys, tokens and other credentials need to be stored in an encrypted vault, protecting them from prying eyes. Requesting applications are authenticated before passwords are released from the vault. To meet today's performance requirements where enterprises manage hundreds of thousands of passwords, application-to-application password management must provide high scalability, availability and disaster recovery.

As hybrid cloud environments introduce management consoles with extraordinary power, effective password management tools provide depth of controls and scope of coverage that this expanded attack surface now requires. Robust discovery features, secure password vaulting and retrieval, automated password policy enforcement, broad platform coverage (including your traditional data center infrastructure and virtualized and cloud environments), support for machine-to-machine authentication, and coverage for key management systems are all important. These capabilities deliver the next-generation, privileged credential management solution that can help your organization reduce IT risks and improve overall operational efficiency.

Credential Management	CA	Others
Automates the creation, use and change of passwords, SSH session keys and other credentials	✓	
Centralizes the administration, storage, release and audit of credentials	✓	
Store credentials in an encrypted safe, protecting them using managed keys generated, stored, and used via software or FIPS-140-2 validated HSM	✓	
Scales by managing high volume credentials (across multi-site, hybrid enterprise environments)	✓	
Provides built-in replication of the credential safe/password vault, aiding disaster recovery	✓	
Manages and modify credentials based on flexible password change policies including rotating passwords at scheduled intervals	✓	
Provides automated login to managed endpoints using privileged credentials without revealing the credentials to users	✓	
Provides transparent login for secondary credentials such as SUDO, databases, and other targets that require secondary authentications	✓	
Provides learn mode for RDP applications and web applications, simplifying credentials acquisition when using RDP published applications and web-based applications	✓	
Offers support for dual credential approval, requiring approvals by designated users prior to allowing access to credentials for managed accounts	✓	
Provides detailed application-to-application password audits and activity reporting	✓	
Allows specific security controls around requesting applications or scripts, including support for: — Specific UIDs executing the script or application — The calling path — The file path — Checksum validation And denies the requesting application's access to the credential if any or all of the above return a false or untrue value	✓	
Allows for the use of an encrypted cache to speed up transaction times and support outage situations	✓	

Limit Privilege Escalations, Reconnaissance and Lateral Movement

Privileged user access control capabilities provide granular, role-based access control not only to network and systems administrators and trusted insiders but to third-party partners, contractors, customers and other privileged users who may be non-employees. You can implement least-privilege access controls where users only see expressly allowed systems and access methods. Once users are logged into a system, access control policies provide an additional level of protection by selectively filtering issued commands. Unauthorized commands are blocked and logged, users may be warned and the security team alerted about policy violations. Inappropriate sessions can be terminated and violating accounts can be deactivated. You can contain privileged users to authorized systems through leapfrog prevention by limiting a user's ability to use one system as a launch point for additional attacks.

Privileged User Access Control/Containment	CA	Others
Provides a zero-trust model where all access is denied, unless it is specifically permitted	✓	
Provides command and socket filtering capabilities including:	✓	
— Blocking unauthorized commands	✓	
— Generating policy violation alerts/warnings and logging	✓	
— Terminating session of users attempting to violate policies	✓	
— Deactivating account of users violating policies	✓	
— Limiting users to authorized systems	✓	
— Supporting (customer-definable) black and white lists	✓	
— Intercepting blacklisted commands and issuing policy violation alerts	✓	
— Providing user-process socket-level filtering such as detection, alerting, blocking, terminating, tracking and monitoring capabilities to prevent leapfrogging to another device, or blocking unauthorized outbound TCP/IP connections	✓	
— Confining users to published RDP applications only instead of allowing RDP access to the entire desktop	✓	
— Providing full attribution for user activities using shared passwords	✓	
Supports a broad set of end-point types like UNIX®/Linux® via SSH or Telnet, Microsoft Windows® and published apps via RDP, databases, mainframe systems via TN3270 or TN5250, and network devices via SSH or Telnet	✓	
Supports local application execution, invoking local/desktop application connections to managed devices	✓	

The "sudo" command on many Unix and Linux systems or the "runas" command for Microsoft Windows allow users to run commands under the administrator's privileges. Sudo and runas commands can and should be restricted using a centralized policy service that filters commands at the protocol, a gateway level, a shell level or a kernel level. Filtering at the gateway is easiest to implement and maintain; kernel-level filtering provides the highest granularity of control yet typically requires more implementation and administration. The ability to do both provides deep and broad protection for your sensitive assets from unrestricted and highly dangerous execution of commands by a privileged account.

The use of shared accounts (such as root and administrator) typically results in privileged users having unnecessary access to critical servers, systems and data. Operating systems don't have the ability to restrict actions and access for multiple people using a shared account. Privileged access management systems that provide fine-grained server access controls ensure that administrators have only the

privileges they need. Fine-grained controls over access to sensitive server-based resources, programs files and processes deliver greater protection of high-value servers. Further, capabilities that enable you to enforce segregation of duties based on the user's job role, generate granular audit trails of all user actions, trace actions made using superuser account privileges back to the original user identity, and prevent unauthorized access to registry keys, and more—provide greater protection for your critical servers that are hosting sensitive, valuable data.

It's not uncommon for privileged users to end up having unnecessary access to critical systems and data, which violates the security principles of least privilege. Operating systems aren't adequately able to restrict access to high-value services and control the actions of privileged users once those users have privileged access to the system. Fine-grained access controls go beyond OS security to examine a user's identity and determine whether an action should be allowed or denied.

High-Value Server Protection	CA	Others
Original user ID tracking for SoD and accountability	✓	
File and directory resource protection	✓	
System process resource protection	✓	
User ID protection	✓	
Login enforcement protection	✓	
Kernel module load/unload	✓	
Windows registry protection	✓	
Incoming and outgoing TCP/IP protection	✓	
Task delegation (sudo)	✓	
Hide root password capability	✓	
Integrity monitoring	✓	
Application jailing	✓	
UNIX authentication bridging	✓	
Granular auditing and syslog forwarding	✓	
User ID management (including UNIX files and NIS)	✓	
APIs (for authentication, authorization and administration)	✓	
Advanced capabilities including scalable enterprise management, policy delivery and versioning, enterprise reporting, application jailing, MFA integration, and granular user containment/restriction	✓	

Monitor, Record and Track Activity

Privileged user session management and recording establishes and controls a remote session, while recording, analyzing and monitoring privileged user activity. When a privileged user session is initiated using common protocols like SSH, Telnet, RDP, ICA, VNC, HTTPS, and X11, a high-resolution capture is available along with full recording, logging and tracking for analysis and/or real-time monitoring. DVR-like playback capabilities for session replay simplify and accelerate session reviews. Support for a wide variety of environments, including cloud management consoles and web-based systems offer comprehensive tracking for security breach monitoring and prevention, as well as audit and compliance purposes.

Real-time alerts when policy violations occur help prevent breaches from happening and contain damage in the event of an incident. Terminating access when a user attempts to access an unauthorized system or device stops cyber criminals in their tracks. Centralized monitoring of all privileged user activities and events, recording and playback of privileged sessions provides complete visibility into all privileged user activity, as well as an archive of necessary information for audit and compliance purposes.

Privileged User Session Management and Recording	CA	Others
Provides session recording and playback for privileged user sessions across RDP/VNC, SSH and cloud management consoles or web-based systems	✓	
Generates comprehensive logs of all requests and responses by the system, including a complete, detailed account of what happened on sensitive systems and who performed a specific activity	✓	
Provides full-resolution capture of privileged user sessions	✓	
Provides DVR-like playback controls for session replay, allowing session review from beginning to end, back up and replay portions of a session, or fast-forwarding to specific points of interest, like jumping to specific points in the timeline to evaluate violations	✓	
Provides comprehensive support for web application session recording, including high-fidelity session tracking for web-based applications and management interfaces (for example, AWS Management Console, VMware interfaces and the Microsoft Office 365 administrative portal)	✓	
Supports always-on session recording and auto-start session recording when a policy violation is detected	✓	
Provides extensive logging capabilities of the critical interactions that take place between hybrid clouds and individual users, supporting configuration management solutions like Puppet or Chef, and a broad range of application programs employing AWS software development kits	✓	
Records and forwards session activity to SIEM tools for further examination and automation	✓	

Protect the Hybrid Enterprise

Scanning your infrastructure regularly provides visibility into your privileged account landscape. In today's dynamic IT environment, the capability to discover unmanaged systems, services and accounts is extremely important. Regular review of all privileged accounts and credentials, including passwords and especially of new accounts with excessive privileges is a must. Discovered, new privileged accounts need to be on-boarded, and off-boarded without delay when they are no longer needed. Integration with an identity and access governance system helps maintain extended access governance controls over privileged users and accounts, which is critical to satisfy security and compliance requirements, including access certification and auditing users' access to shared accounts.

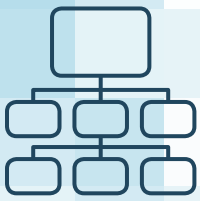
Privileged access management capabilities must be extended to cover the dynamic, rapidly changing cloud and virtual environments, and adequately protect an expanded attack surface. Because volumes of new resources can be added in the cloud in a matter of minutes, you need to automatically discover target resources. Other important elements include flexible deployment options (physical appliance, virtual appliance or AMI), clustering that provides scalability and high availability to keep pace with complex hybrid-cloud computing architectures.

Hybrid Enterprise Protection	CA	Others
Defines and enforces privileged access management controls across enterprise data centers, virtualized infrastructure and public or private clouds	✓	
Provides a single, centralized source for policy definitions, along with comprehensive activity records	✓	
Supports integration with virtualization and public/private cloud platforms like:	✓	
— Amazon: Amazon Web Services Consoles (including tight integration with AWS's IAM system), AWS API Proxy	✓	
— VMware: VMware vSphere, including both the vCenter Server and guest operating systems running on VMware vSphere and NSX	✓	
— Office 365 and Microsoft Online Services (including support for ADFS and SAML)	✓	
Supports widely used enterprise platforms such as:	✓	
— Windows Domain, Local Administrator and Service Accounts	✓	
— Popular Linux and Unix distributions	✓	
— Legacy systems like AS/400	✓	
— Popular networking devices like Cisco and Juniper	✓	
— Telnet/SSH-based systems	✓	
— Popular applications like SAP and Remedy	✓	
— Popular databases	✓	
— Systems and applications servers	✓	
— Out-of-band serial devices supporting RS-232 and 422, etc. (commonly used by Industrial Control Systems)	✓	
— ADFS and SAML 2.0 (support for both service provider and identity provider models)	✓	

Key integrations with enterprise management solutions further extend the business value of a privileged access management solution. Integrating with an identity management and governance system is not only a natural extension of privileged access control measures but is critical to your broader identity and access management strategy. You can automate administrative users' requests for access and grant authorized access by approvers. Service Management integration facilitates automated handling of change-control authorizations and associated service-ticket tracking and management. Integration with SIEM tools enable advanced analysis of privileged activity, triggering real-time alerts when illicit behavior occurs.

Enterprise Management Integrations	CA	Others
Provides IAM integrations:	✓	
— User provisioning and de-provisioning	✓	
— Orphaned account discovery	✓	
— Account certifications and accreditations	✓	
Provides SIEM integrations:	✓	
— Privileged user activity logging and forwarding onto SIEM tools	✓	
— Real-time monitoring, correlation, alerting, response and remediation	✓	
— Historical reporting and forensics investigation	✓	
Provides IT Service Management (ITSM) integrations:	✓	
— Validation of administrative access requests using ITSM tools	✓	
— Provide control authorizations or incident reports using ITSM tools	✓	

As larger enterprises continue to advance IT architectures and implement more complex hybrid environments, knitting together point solutions that are designed for traditional datacenters is a costly and risky proposition. Privileged access management tools must not only scale to address enterprise-class requirements, they must provide a single point of control for resources across the hybrid cloud. This includes providing a comprehensive set of security and compliance controls such as protection and vaulting of credentials, robust authentication, access control, privileged user monitoring and session recording, control over command execution, user attribution for shared administrative accounts, and proactive enforcement of policies—all in a single system over resources in the datacenter, on virtualized infrastructure and in the public cloud.



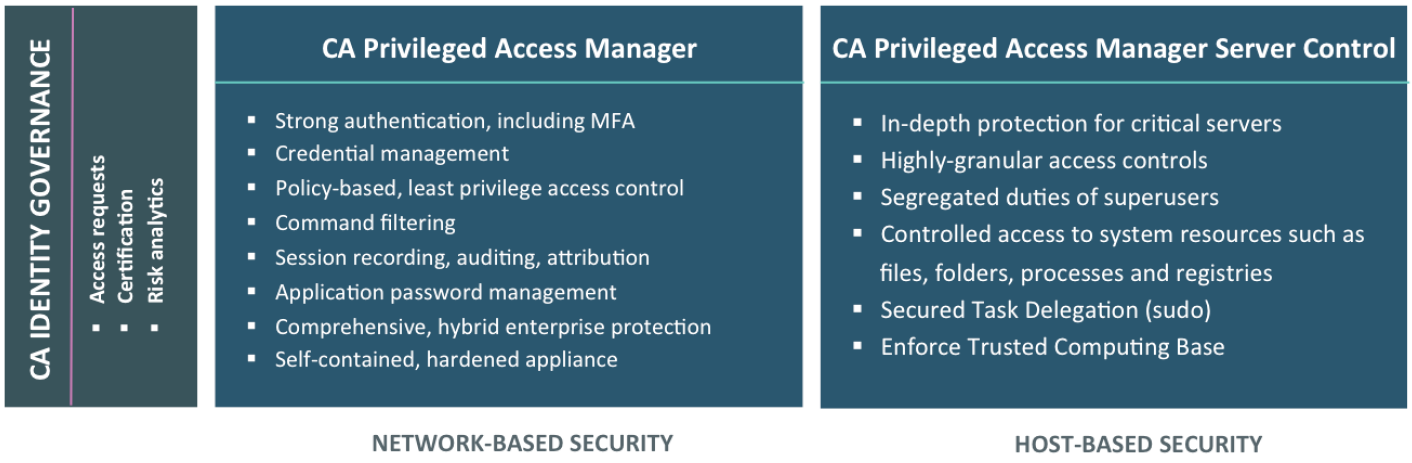
Defense In-depth Privileged Access Management with CA Technologies

CA Privileged Access Management Solution

CA Technologies provides easy-to-deploy and comprehensive privileged access management solutions with integrated credential management, strong authentication, zero-trust access control, proactive command filtering, session monitoring and recording, and fine-grained controls over high-value servers.

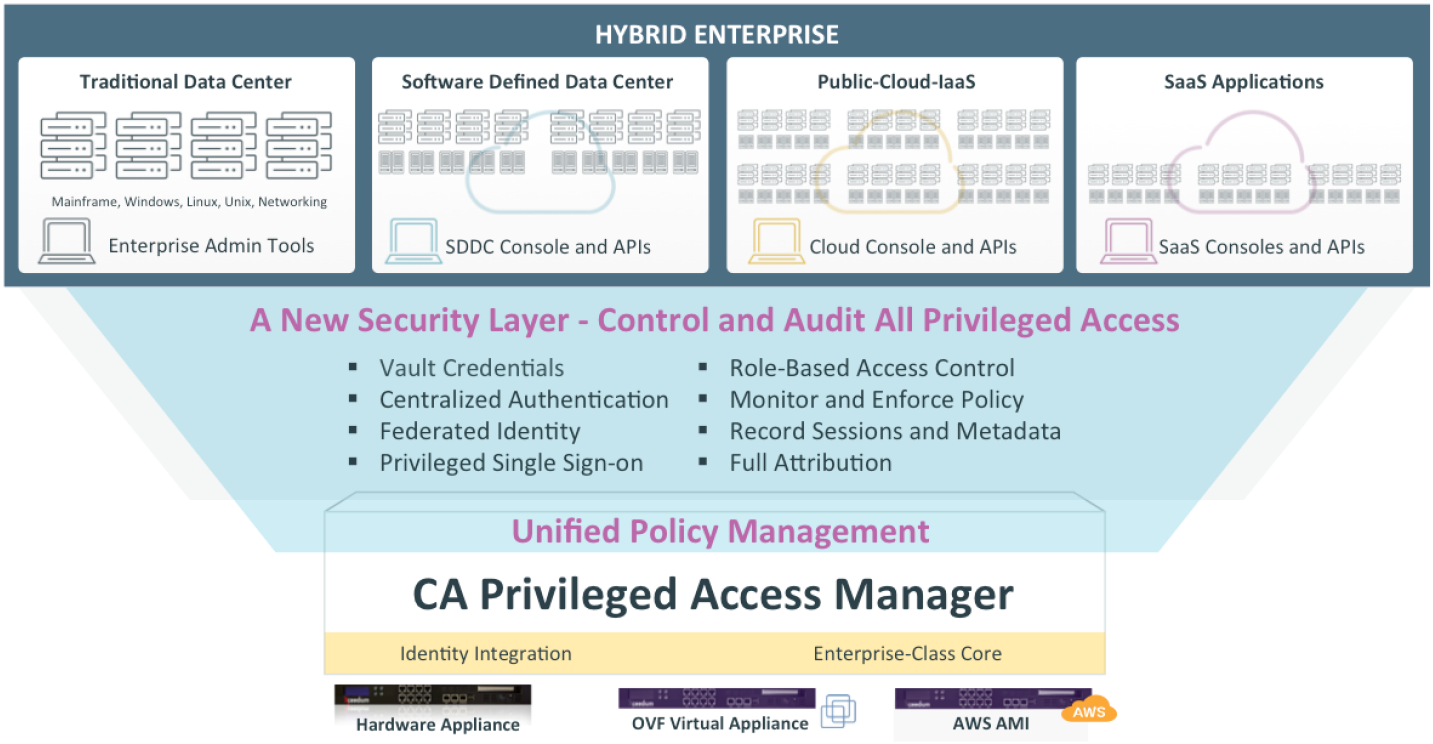
The solution has two deployment options, providing the appropriate level of defense for different security needs and enabling in-depth defense of privileged accounts to minimize security and compliance risks, including:

- Centralized, easy-to-deploy privileged access management delivered through a network architecture and 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



CA Privileged Access Manager

CA Privileged Access Manager is designed as an automated, proven solution for privileged access management that's easy to deploy 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 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, and provides integration to Active Directory and LDAP-compliant directories, as well as authentication systems like Radius. Integrated with advanced authentication tools like CA Advanced Authentication, the solution facilitates stronger or MFA 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) helps ensure 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.

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; CA Privileged Access Manager implements a deny-all, permit-by-exception approach to least-privilege access controls. Users are able to see only expressly permitted systems and access methods.

Socket filtering. CA Privileged Access Manager tracks individual users who are accessing a wide variety of Linux, Unix, and Windows-based servers. When a user attempts to open a socket to another device or server on the network, using interactive protocols such as Telnet, SSH, re-login, Remote Desktop Client, CA Privileged Access Manager immediately detects the attempt to create an outbound socket and blocks it. The solution can issue warnings to the user and generate alerts. With socket-level monitoring capabilities, the solution can detect any leapfrog attempt, regardless of what command the user employs. Which means CA Privileged Access Manager can effectively detect and terminate a program establishing an unauthorized connection to another device on the network, regardless of the overall approach.

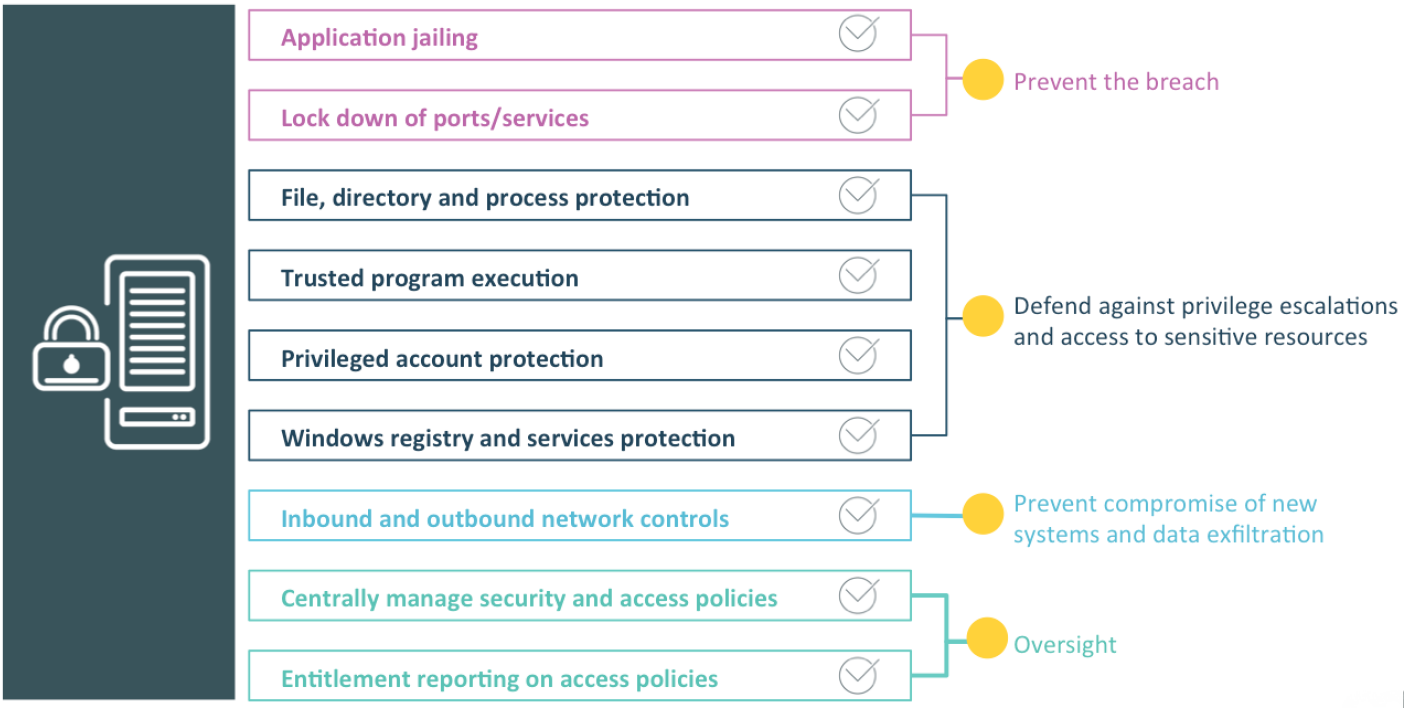
Session recording. CA Privileged Access Manager provides full-resolution capture of privileged user sessions. DVR-like playback controls allow auditors and investigators to review everything that happened during a session, with the ability to jump directly to attempted policy violations. Recording and 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-to-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. Automated 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 reports are available.

Hybrid enterprise protection. CA Privileged Access Manager delivers tightly integrated privileged access management capabilities for widely deployed hybrid-cloud computing platforms and traditional systems including native, API-level integration with various IaaS providers such as Amazon Web Services (AWS), VMware vSphere and NSX, Microsoft Online Services;. The solution also offers broad and deep integration with 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. Agent-based, kernel-level protection is available for individual files, folders and specific commands based on policy and/or fined-grained controls on specific hosts.



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

Host-based access control. OSes 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. These features help ensure accountability and facilitate 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 ineffective.

Solution Benefits

CA Privileged Access Management provides capabilities and controls that actively prevent attackers from carrying out key components of their attacks, while reducing risks and improving operational efficiency. More specifically, CA Privileged Access Management enables organizations to:

- **Reduce risk.** Prevent unauthorized access and limit access to pre-approved 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. Prevent the execution of unauthorized commands and lateral movement within the network.
- **Increase accountability.** Observe full attribution of user activity, even when using shared accounts. Using 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 limits risk but boosts productivity of individual administrators by making it easier and faster to access the systems and resources they need to manage. Centralized policy definition and enforcement simplify the creation and enforcement of security controls.

This solution can protect the broad hybrid IT infrastructure, covering the traditional physical data center (servers, networking devices, databases, switches and related resources), and growing virtual and cloud platforms. This helps protecting the underlying management infrastructure and resources deployed in software-defined data centers and networks, IaaS environments and SaaS offerings.

To learn more about CA Privileged Access Manager and CA Privileged Access Manager Server Control, visit **ca.com/privileged-access**

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.

1 www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779/op-1

2 www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html

3 www.bostonglobe.com/metro/2016/03/25/hackers-target-mass-colleges-with-anti-semitic-fliers/zO8h2xh5YC0GM8jzK7Nv3H/story.html

4 www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

CS200-194909_0516