DATA SHEET

CA Privileged Access Manager Server Control

At A Glance

CA Privileged Access Manager Server Control provides a comprehensive solution for protecting the most critical business assets—your mission-critical servers—with powerful, fine-grained protections over operating system-level access and privileged user actions. CA Privileged Access Manager Server Control is a system-level, host-based solution that controls, monitors and audits privileged user activity to improve security, reduce administrative costs and simplify audit and compliance processes across physical and virtual environments.

KEY BENEFITS

- Reduce risk of breach for critical UNIX®, Linux® and Microsoft Windows® servers.
- Limit privileged account rights and capabilities.
- Manage privileged user control over files, folders, processes, registries, etc.
- Segregate duties of superusers (root, administrator) by entrusting authority to named users.
- Facilitate compliance with regulatory mandates.

KEY FEATURES

- In-depth protection for critical servers
- Highly-granular access controls, even for users with superuser privileges
- Delegated superuser privileges to named users
- Controlled access to system resources, including files, folders, processes, registries and more.
- Protects Windows services
- Secured task delegation (sudo utility)
- Monitors files and programs and alerts when changes occur; optionally block tampering programs
- Authenticates UNIX and Linux users using active directory and Kerberos credentials
- User activity reporting

Business Challenges

Many data breaches happen because of compromises in privileged user accounts, such as UNIX/Linux superuser account (root) and Windows administrator accounts. Malicious insiders and external hackers specifically target these superuser accounts for exploitation, to give full, unauthorized access to all applications, data and audit logs. Unfortunately, these superuser accounts cannot be disabled because systems administrators need the privileges to perform necessary and legitimate maintenance of critical servers. Extra protections that audit all access, identify and prevent unauthorized activities, while still allowing legitimate actions, are key to defending mission-critical servers. Just one improperly authorized privileged account usage can cause widespread and irreparable damage to an organization's infrastructure, intellectual property and brand equity.

You need a proven privileged access management solution that provides powerful controls over privileged users on your most critical systems.

Solution Overview

CA Privileged Access Manager Server Control is a comprehensive and mature solution specifically designed to protect your most sensitive systems whether they are physical, virtual or cloud. CA Privileged Access Manager Server Control is a scalable solution capable of providing fine-grained access controls, auditing and UNIX authentication bridging across servers from a central management console. And CA Privileged Access Manager Server Control is uniquely capable of enforcing access controls on powerful native superuser accounts, like the UNIX and Linux root and Windows administrator.

Critical Differentiators

CA Privileged Access Manager Server Control provides in-depth protection of critical servers to enforce host-based, fine-grained access controls to resources, segregated duties of superusers, management of system resources and secure task delegation (sudo).

Fine-grained access control to resources: Control and monitor privileged user access to files, folders, processes and registries, enabling accountability and segregation of duties.

Segregated duties of superusers: Restrict superuser privileges with finer level of granularity than what is available in the host operating system.

Secured task delegation (sudo): Manage task delegation and the ability of a user to run commands as another user.

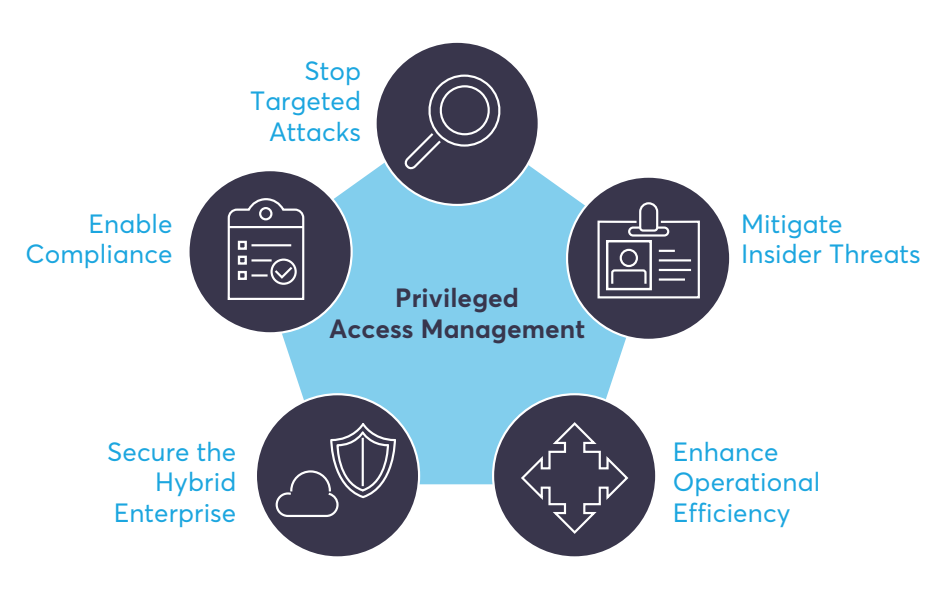
Facilitate compliance with powerful reporting: Generate configurable, highly granular audit events and reports to monitor activities of key users, access to resources and status of compliance policies.

Reduce IT costs through automation: Create policy-based rules to reduce human error and improve security, enabling required changes to happen in real time.

Reduce UNIX/Linux administration costs: Authenticate users to Microsoft Active Directory® and provide single sign-on capabilities.

Docker support: In addition to controlling interprocess communication (IPC) over TCP, the solution can also restrict local IPC which uses UNIX (or LOCAL) named domain sockets. The product intercepts processes which attempt to connect to a socket using the named socket path.

CA Privileged Access Manager Server Control
Fine-grained access controls and host system protections enhance the benefits delivered by the privileged access management solution from CA Technologies.



Related Products/Solutions

- CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for privileged access management in physical, virtual and cloud environments.
- CA Identity Governance protects identity and access governance, including entitlement certification and role management.

Supported Environments

- UNIX
- Linux
- Windows

For more information, please visit **ca.com/privileged-access-management**

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**.

200-389793_0918