DATA SHEET

CA Privileged Access Manager for Amazon Web Services (AWS)

At A Glance

Quickly deployable and delivering fast time to protection, CA Privileged Access Manager enhances security capabilities of the AWS Management Console and Management APIs, facilitates compliance and minimizes costs. Available as a virtual appliance, CA Privileged Access Manager is designed to prevent security breaches in EC2 environments by consistently controlling privileged user activities, proactively enforcing security policies, protecting sensitive administrative credentials, and monitoring and recording privileged user activity across virtual, cloud and physical environments.

KEY BENEFITS

- Deploy the solution quickly.
- Protect AWS management console and APIs, as well as EC2 instances.
- Control privileged access across all IT resources.
- Apply unified cross-platform privileged user credentials protection.
- Monitor, react and record everything.
- Ensure security and privacy regulatory compliance.
- Provide for positive privileged user authentication.

KEY FEATURES

- Automatically discover and protect AWS and virtualized resources.
- Get AWS management console integration.
- Full attribution of actions to individuals with separation of duties enforcement.
- Secure credential storage, including password and key management.
- Multifactor authentication, single sign-on and federation support.
- Interoperability with Active Directory, LDAP, RADIUS, TACACS+ and other identity stores.

Business Challenges

Privileged user accounts are your most valuable assets—and the most likely to be exploited by external hackers or insider threats. One compromised privileged account can cause irreparable damage to your infrastructure, intellectual property and brand. And the attack surface is expanding as you move to virtualized and cloud environments. Recognizing these risks, many emerging standards and regulations are requiring mandatory controls and auditing of privileged user access and activity.

In addition, as organizations adopt DevOps, new risks are being introduced. Automation tools like CA's Automation solutions, Chef and Puppet leverage AWS Management APIs and Amazon software development kits (SDKs). Developers create command line scripts and programs to perform AWS administrative and operational tasks and embed these scripts within the automation tools. Unfortunately, a single set of credentials is often used for all cloud management APIs across all automation initiatives, creating a single point for hackers to compromise.

Because of their power and to comply with information security regulations, privileged access for both users and applications must be carefully managed and controlled.

Solution Overview

CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for privileged access management in physical, virtual and cloud environments. Available as an Amazon Machine Instance (AMI) and fully integrated with the AWS Management Console, CA Privileged Access Manager enhances Amazon's security groups and network control lists to better protect the AWS EC2 environment by monitoring and recording privileged user access and activity, proactively enforcing separation of duties, providing full password and credential management, and enabling a single point of privileged identity management for all AWS and other IT resources.

Critical Differentiators

CA Privileged Access Manager enhances AWS's native security capabilities and adds fine-grained access control to AWS Management Console and APIs.

Automatically discover and protect AWS EC2 instances. Automatically establish and enforce policies across dynamic EC2 resources by adding policy protections and access permissions in real time, as virtual instances are created.

Enforce granular separation of duties for AWS. Track or block privileged user activity at the command-level granularity for both manual and programmatic AWS management by assigning users personal credentials and permissions, without rewriting automation scripts that use shared administrative privileges.

Monitor, react and record everything. Log events, generate alerts and warnings, or even terminate sessions. Capture continuous, tamperproof evidence logging and video recording of administrative sessions for all AWM management activity, including calls to/from AWS management APIs.

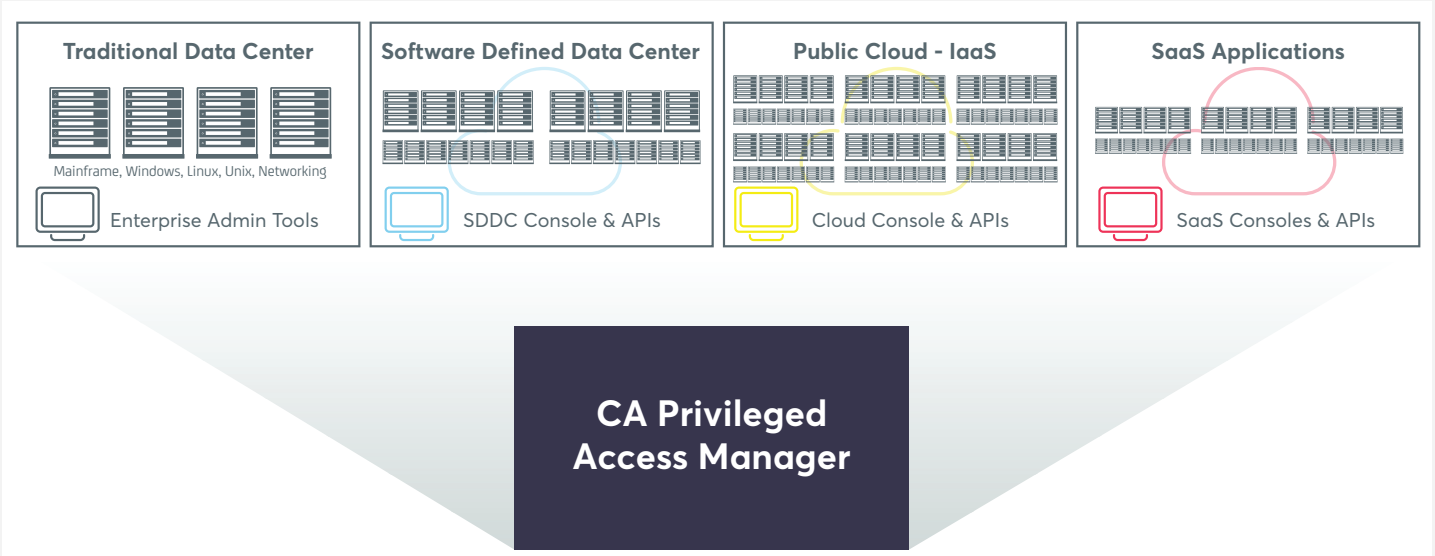
Manage privileged user credentials and simplify with single sign-on. Vault AWS credentials and other sensitive credentials in an encrypted credential safe. Gain faster access and productivity improvements with single sign-on.

Related Products/Solutions

CA Threat Analytics for PAM dynamically analyzes user behavior and compares the same user's past similar behavior to highlight anomalies and other activities that pose a higher-than-normal risk of breach.

CA Privileged Access Manager Server Control provides a comprehensive solution for protecting extremely critical business assets with fine-grained protections over operating system–level access and application-level access.

CA Privileged Access Manager provides comprehensive protection for the entire hybrid enterprise.



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

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**.

200-392383_0918