DATA SHEET

CA Privileged Access Manager: MMIS Systems Risk Mitigation—MARS-E 2.0

At a Glance

Regulatory compliance and the safety of citizen protected health information (PHI) and personally identifiable information (PII) data are critical to state health modernization efforts. For Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0, Health Insurance Portability and Accountability Act (HIPAA) compliance, and Federal Information Security Management Act (FISMA) compliance, states must ensure that all citizen data is secure in production systems and supporting test environments.

CA Privileged Access Manager prevents security breaches by consistently protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies, and monitoring and recording privileged user activity across virtual, cloud and physical environments.

Key Benefits/Results

- Control privileged access across all IT resources.
- Manage privileged account credentials.
- Monitor, react and record everything.
- Protect hybrid-cloud consoles and management APIs.
- Provide for positive, privileged user authentication.
- Prevent leapfrogging.
- Automatically discover and protect AWS and virtualized resources.

Key Features

- Unify cross-platform support.
- Control access that is role based and fine-grained.
- Get privileged user credential protection.
- Monitor, audit and record sessions.
- Support security and privacy regulations.
- Fully attribute activity to individuals.
- Manage password and keys.
- Get VMware, Amazon Web Services (AWS), Linux®, UNIX®, Microsoft® Windows®, mainframes and network gear protection.
- Take advantage of multifactor authentication, single sign-on and federation support.
- Achieve interoperability with Active Directory, LDAP, Radius, TACACS+ and other identity stores.

Business Challenges

MARS-E 2.0, in conjunction with key supplemental documents (including NIST SP 800-53 Rev4), prioritizes the focus on securing citizens' PHI, PII, and federal tax information. Breaches are on the rise and compromised privileged user credentials have been used to get inside an organization's network and jeopardize systems, data and the enterprise. The high trust that we grant these individuals and the level of risk associated with their accounts make privileged accounts a common attack vector. Misused administrator credentials can have catastrophic consequences on your enterprise.

Organizations need an easy-to-deploy solution that provides comprehensive privileged access management capabilities. The solution needs to offer protection across traditional physical data centers (servers, networking devices, databases, switches and related resources) and extend that protection to the growing hybrid cloud environment, which includes software-defined data centers and networks, as well as infrastructure as a service (IaaS) and software as a service (SaaS)—ultimately protecting the underlying management infrastructure in addition to the resources operating in these environments.

Solution Overview

CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for MARS-E 2.0 security compliance, which states use to achieve privileged access management in physical, virtual and cloud environments. Available as a hardened hardware appliance, an Open Virtual Appliance (OVA), or an Amazon Machine Image (AMI), CA Privileged Access Manager provides:

- Credential management to protect and manage sensitive administrative credentials
- Policy-based access control to provide network-based, highly granular and role-based access control
- Command filtering to provide agentless command filtering based on white- and black-list models
- Session recording to provide full-resolution capture of privileged user sessions with DVR-like playback controls
- Application password management to eliminate hard-coded, hard-to-change passwords from applications and scripts
- Hybrid enterprise protection to deliver for widely deployed hybrid-cloud computing platforms and traditional systems alike

Critical Differentiators

CA Privileged Access Manager enforces security by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity.

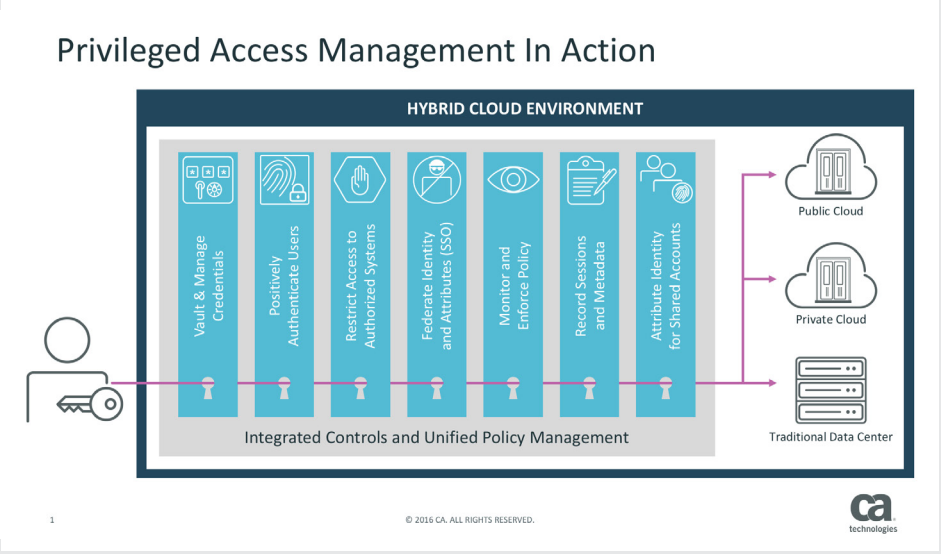
Leverage massive scalability. Support for thousands of concurrent recorded sessions from a single appliance provides a scalable platform, even during heavy load.

Eliminate hidden costs. The appliance-based architecture within CA Privileged Access Manager includes a hardened Linux operating system and provides built-in load-balancing, high availability and storage to eliminate the need for additional servers, OS licenses, databases, load balancers and other hidden infrastructure costs.

Enjoy fast time to protection. Quickly deploy CA Privileged Access Manager as a hardened device or a virtual machine, protecting your enterprise resources with one, scalable, agentless solution.

Monitor, react to and record everything. Log events and generate alerts, warnings, or even terminate sessions. Capture continuous, tamper-evident logging and video recording of administrative sessions.

Get protection for hybrid-cloud consoles. Privileged users gain access only to authorized hybrid-cloud infrastructure, with all activity fully monitored and recorded.



Leverage existing IAM infrastructure. The solution provides integration with Active Directory, LDAP-compliant directories, RADIUS, TACACS+, smartcards, hardware tokens and more.

Related Products/Solutions

CA Privileged Access Manager Server Control: A complementary, market-leading, host-based solution for controlling privileged user actions on servers.

CA Single Sign-On: Create federation to provide a single sign-on experience.

CA Advanced Authentication: Provide users with optional, two-factor authentication.

CA Identity Governance: Offers integration for entitlements certification.

Supported Environments

- Support for traditional data center enterprises including TCP/IP networks, popular commercial databases, operating systems and network devices using standard protocols including SSH, RDP and HTTPS
- Integration with AWS, VMWare esx(i) and NSX, Microsoft Office 365™ and Splunk, as well as other standards-based integrations
- Support for a wide variety of authentication types including Active Directory, LDAP-compliant directories, RADIUS, TACACS+, smartcards and hardware tokens

For more information, please visit **ca.com/publicsector**

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**.

CS200-203816