CA Privileged Access Manager for the VMware NSX Solutions Platform

At A Glance

The Software Defined Data Center is inherently more secure than its physical counterpart, and makes an ideal platform for deploying the applications giving rise to the application economy. Tightly integrated with native NSX security, CA Privileged Access Manager for VMware NSX delivers essential privileged access management capabilities, limiting privileged user activities, dynamically controlling access, proactively enforcing security policies and automatically modifying them as circumstances change, protecting sensitive administrative credentials, and monitoring and recording privileged user activity across all IT infrastructure. Quickly deployable and delivering fast time-to-protection, CA Privileged Access Manager enhances security, facilitates compliance, and minimizes costs.

Key Benefits/Results

- Control privileged access across all resources.
- Deploy solution quickly.
- Automatically discover and protect virtual assets.
- Dynamically modify access controls in response to security posture changes.
- Protect VMware NSX Manager and Controllers.
- Manage privileged account credentials and single sign-on.
- Monitor, react, and record activities.

Key Features

- Automatic discovery of VMware NSX resources.
- Protection of VMware NSX Manager and Controllers, and all other IT resources.
- Dynamically linked security groups.
- Service Composer Integration.
- Distributed Firewall Access Restrictor.
- Unified cross-platform privileged user credentials protection.
- Monitoring, audit trail, session recording and reporting.
- Security and privacy regulatory support.
- Full attribution of actions to individuals and separation of duties.
- Multifactor authentication, single sign-on, and federation support.
- Interoperability with active directory, LDAP, Radius, TACACS+ and other identity stores.

Business Challenge

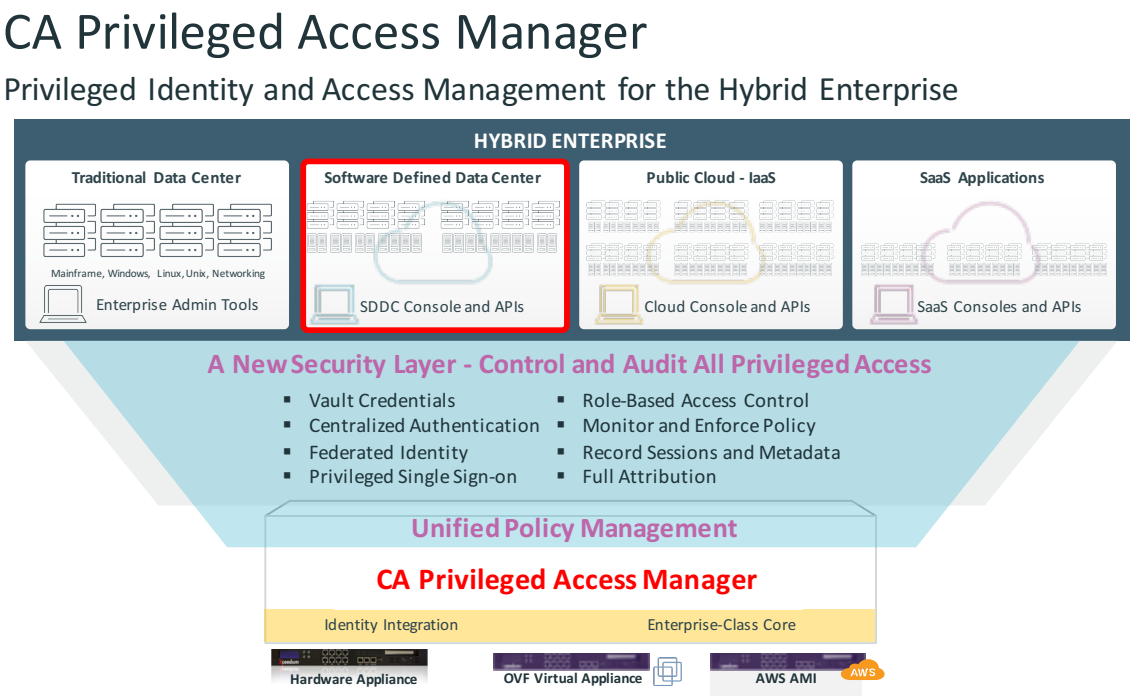
Software defined data centers (SDDC) are being widely adopted as a way to make data centers more agile, operationally scalable, and secure. SDDC is defined by compute, storage and network virtualization and VMware NSX provides the network virtualization component. Virtual networks enable network isolation by default and NSX native security capabilities provide in-

kernel, scale-out firewalling with line-rate performance distributed to every hypervisor, automated provisioning of security services automated workload moves/adds/deletes, and granular policy enforcement at the virtual level. Managing privileged user access is an essential task to ensure security, compliance, and efficient operations.

Solution Overview

CA Privileged Access Manager offers the industry's first privileged access management integration with VMware NSX, VMware's network virtualization platform for the software-defined data center. CA Privileged Access Manager's NSX solution is seamlessly integrated with VMware's NSX. By leveraging NSX's distributed firewall and dynamic tagging and grouping capabilities, CA Privileged Access Manager allows for automated access and monitoring of all privileged user connections. That helps secure system access for NSX administrators, while improving operational efficiencies.

Available as an Open Virtualization Format (OVF) virtual appliance and fully integrated with the VMware management environment, CA Privileged Access Manager for VMware NSX enhances NSX native security by controlling privileged access and limiting sensitive administrative activities in VMware NSX Manager by monitoring and recording privileged user activity, proactively enforcing separation of duties, providing full password and credential management, and enabling a single point of privileged identity management for all of VMware and other IT resources.



Critical Differentiators

CA Privileged Access Manager is a simple-to-deploy, automated, proven solution for privileged access management in physical, virtual and cloud environments. CA Privileged Access Manager for VMware NSX enhances VMware NSX's native security capabilities and adds fine-grained access control.

- **Automatically discover and protect ESX/ ESXi hosts and guest systems.** Automatically establish and enforce policies across dynamic virtual resources by adding policy protections and access permissions in real-time, as virtual instances are created.
- **Automatically define highly restrictive, micro-segmented, secure network access to NSX-based resources.** Using synchronized security settings within NSX Security Groups, automatically provide short-term administrative access to select systems—or deny access and terminate sessions in response to security incidents.
- **Monitor, react and record everything, including NSX REST APIs interactions**. Deliver full audit and response logs of all user events, including interactions with the powerful NSX Manager APIs. Capture continuous, tamper-evident logging and recording of administrative sessions. Generate alerts, warnings or even terminate sessions. Analyze logs using VMware vRealize Log Insight or other log managers.
- **Manage privileged user credentials and simplify with single sign-on.** Vault credentials in an encrypted credential safe. Gain faster access and productivity improvements with single sign-on.

CA Privileged Access Manager is designed to protect the physical data center assets, virtual infrastructure, private cloud, public cloud and hybrid environments with one scalable, agentless solution, providing centralized access across tools and resources.

Related Products/Solution

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.

Supported Environments

CA Privileged Access Manager delivers privileged access capabilities across a range of IT infrastructure, including Linux®, Microsoft Windows®, UNIX®, networking devices, multiple databases and business applications, and more. Optional extensions provide enhanced integration with VMware vSphere vCenter Server and guest systems, NSX software-defined networks, IBM® mainframes, Microsoft Office® 365 Admin Center and Amazon Web Services (AWS), including the AWS Management Console and APIs.

The CA Technologies Advantage

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success. For more information about CA Technologies go to ca.com.

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