Symantec® PAM

Securing VMware® Cloud Foundation™

Overview

As organizations work to modernize application portfolios to remain competitive, it becomes clear that legacy data center infrastructure lacks the resiliency and scalability needed. As a result, cloud adoption and migration strategies are inextricably linked to application modernization. To run applications across multiple cloud boundaries, organizations need a platform that provides consistent infrastructure and operations across clouds. VMware® Cloud Foundation™ addresses this challenge by combining the scale and agility of public cloud with the security and performance of private cloud.

Many data breaches trace back to an exploited privileged account. One improperly authorized or compromised privileged account can cause widespread and irreparable damage to an organization's infrastructure and reputation. This risk is significantly amplified by the growing, dynamically distributed virtualized and cloud environments that are commonly found across today's modern enterprise IT. Symantec® Privileged Access Management (PAM) boosts the native VMware Cloud Foundation security capabilities to prevent security breaches in VMware environments.

Introducing Symantec PAM

Symantec PAM is designed to protect sensitive administrative credentials and secrets, and can control privileged access across cloud, physical, and virtual environments at both the IaaS provider and IaaS layers. The solution delivers five core services: privileged credential vault, session recording and management, behavioral analytics, fine-grained access controls, and secrets management from a single platform. This document highlights how Symantec PAM can be used to enhance and safeguard both VMware guest systems as well as the underlying VMware vCenter® server environment.

Benefits of Symantec PAM for VMware Cloud Foundation



Zero Trust Access



Process Automation Enablement



Data Privacy Compliance

Delivering the Benefits of VMware Cloud Foundation

Zero Trust Adoption

Zero Trust adoption starts with verifying the identities of every user and device requesting access to resources. Symantec PAM protects access to VMware vCenter by removing administrative passwords from the hands of multiple users and placing them into an encrypted data store. Access to these credentials is only granted after the user's identity has been verified through strong authentication. Similarly, secrets management eliminates hard-coded credentials to enable secure communications and automation within DevOps toolchains. Furthermore, Symantec PAM implements fine-grained access control to the VMware vSphere® server management console and guest systems to enforce least-privileged access (the second tenet of a Zero Trust architecture).

Process Automation Enablement

The primary goal of application modernization and cloud migration is to improve the speed and quality of innovations to online services, and to deliver those innovations to customers. Symantec PAM supports this dynamic environment through the automatic discovery of, and policy provisioning for, virtual hosts. Symantec PAM eliminates manual identification and the delay caused by manually defining, applying, and enforcing privileged access control policies for virtual resources. Additionally, one of the core strengths of Symantec PAM is its scalability, a critical aspect for virtual environments that may witness unexpected and significant growth. Finally, the solution is offered as an Open Virtualization Format (OVF) compliant VMware virtual appliance, so deployment and administration is greatly simplified.

Data Privacy Compliance

Standards and regulatory bodies, as well as auditors, have recognized the risks associated with privileged users and now incorporate changes to mitigate these risks. Symantec PAM enables organizations to demonstrate compliance through four primary aspects. First, it implements strong authentication before granting users access to the VMware infrastructure. Second, it enforces fine-grained policy controls to enable least privileged access, which supports Zero Trust principles and separation of duties requirements. Third, the solution provides tamper-proof audit data and forensic evidence for privileged activity, which is attributed back to the user who performed those activities. Finally, it can proactively rotate privileged credentials on a per use or periodic basis, or both.

Why Symantec PAM?

- **Fast time-to-protection:** Symantec PAM can be rapidly deployed either as a hardened physical device or a virtual appliance. You can swiftly configure the solution through an easy-to-use console, leading to quicker time-to-protection and reduced implementation costs.
- **Enterprise performance and scalability:** Renowned for its efficiency and scalability, Symantec PAM can manage and record a notably higher number of simultaneous recorded connections compared to alternative solutions. This scalability facilitates large-scale deployments with minimal infrastructure requirements.
- **Total cost of ownership:** Symantec PAM includes an encrypted vault, session recording, threat analytics, and secrets management features within its base software license. When combined with its scalability, this offering ensures a best-in-class total cost of ownership.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops, and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage, and industrial. Our solutions include data center networking and storage, enterprise, mainframe, and cybersecurity software focused on automation, monitoring and security, smartphone components, telecoms, and factory automation.

For more information, visit our website at: www.broadcom.com

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

PAM-VCF-OT100 July 18, 2024