Symantec® PAM

Secrets Management

Overview

Organizations are rapidly undergoing IT modernizations to transform and accelerate their software delivery cycles and application development processes. However, these initiatives have expanded the attack surface, amplifying risks and security concerns. Attackers are increasingly (and successfully) leveraging privileged user credentials to gain unauthorized access. One major area of concern is secrets.

A secret is a piece of information that must be protected to avoid discovery. In the digital world, secrets refer to authentication credentials. These authentication credentials are leveraged by and often embedded within DevOps tools and processes to enable automation for faster application delivery to market. Unfortunately, lapses in adequate security controls have allowed malicious actors to compromise secrets, granting them unauthorized access to steal data and significantly disrupt business operations.

Introducing Symantec PAM

Symantec® Privileged Access Management (PAM) is designed to prevent security breaches by offering a comprehensive set of privileged access management capabilities. These privileged access management capabilities include the following features: Privileged Credential Vault, Session Management and Recording, Behavioral Analytics, Fine-Grained Policy Controls, and Secrets Management. Symantec PAM capabilities safeguard sensitive administrative credentials, regulate privileged user access, proactively enforce security policies, and monitor and record privileged user activities across virtual, cloud, and physical environments.

Benefits of Secrets Management

Zero Trust Adoption

Process Automation Enablement

Data Privacy Compliance

Delivering the Benefits of Secrets Management

Zero Trust Adoption

Various security tools and technologies are required to implement a Zero Trust framework to mitigate different attack vectors. A significant area of concern involves users with elevated or privileged access, as they often operate outside the scope of standard application security controls. Secrets management addresses these security gaps by implementing policy controls over non-human users. Applications and DevOps tools must authenticate their identity before gaining access to a secret. Moreover, Symantec PAM enables organizations to maintain multiple secrets vaults to accommodate different types of secrets, their intended usage, and access policies. It can also enforce role-based access controls to ensure that only authorized users are permitted to view and manage the secrets stored within these vaults.

Process Automation Enablement

At its core, DevOps aims to enhance the speed and quality of introducing innovation to applications and delivering them to customers. DevOps tools and processes rely on authentication credentials to facilitate automation, and secrets management ensures the safeguarding and authorization of access to these credentials. One of the key strengths of Symantec PAM is its scalability, a critical aspect for secrets management because of the substantially higher transaction volumes involved in automated processes. Symantec PAM also allows enterprises to automate the creation and provisioning of new devices within the solution through REST APIs. This automation guarantees that each newly established server, container, and environment has its privileged credentials and accounts secured immediately upon creation through the DevOps toolchain.

Data Privacy Compliance

As the significance of compromised privileged accounts and credentials has become evident, regulatory bodies and auditors have directed their attention towards the controls that organizations need to implement to mitigate these risks. Compliance with these regulations and audits primarily revolves around four aspects: enhancing initial access through stronger authentication, bolstering auditing practices for heightened accountability, enforcing separation of duties through least privileged access, and regularly rotating credentials to minimize risk. The most critical aspect in the realm of secrets management is credential rotation. Symantec PAM enables you to rotate passwords and enforce credential expiration and deletion dates.

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 connections compared to alternative solutions. This scalability facilitates large-scale deployments with minimal infrastructure requirements.
- **Total cost of ownership:** Symantec PAM includes encrypted credential 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

PAM-SEC-MAN-OT100 September 11, 2023