SOLUTION BRIEF

CHALLENGE

A hacker can cause widespread and irreparable damage to an organization with just one compromised privileged account. With the emergence of cloud-based and virtualized environments, the number and types of privileged credentials and accounts that must be protected are expanding exponentially. To mitigate this risk, all privileged credentials and access must be effectively managed across the enterprise.

OPPORTUNITY

Symantec® PAM is designed to protect sensitive administrative credentials and control privileged access across cloud, physical, and virtual environments. 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.

BENEFITS

Organizations can retain significant financial and reputational benefits by effectively managing risk, preventing improper use of privileged accounts, and safeguarding high-value assets. Symantec PAM provides multiple layers of defense around privileged identities and credentials at all layers of the technology stack to prevent breaches, facilitate audits, and ensure compliance.

Symantec by Broadcom

Enforcing Policy Controls over Privileged Access

Introduction

As evident from recent hacks on the U.S. government, software vendors, and many corporate enterprises, attacks are becoming more sophisticated. Privileged identities and credentials are frequently used in successful breaches, which is why regulators have been mandating more comprehensive requirements and controls for privileged access.

Privileged access management (PAM) technologies address these challenges as they allow organizations to create and enforce controls over users, accounts, and systems with elevated or privileged entitlements. Traditionally, this was accomplished by deploying one of two following architectural frameworks:

- **Password Account and Session Management (PASM):** These technologies protect privileged accounts by vaulting their credentials and forcing privileged users to authenticate themselves to the tool before granting them access.
- **Privileged Elevation and Delegation Management (PEDM):** These technologies leverage agents to protect privileged accounts by enforcing fine-grained access controls over the users who access the protected devices.

For many years, the two frameworks were considered to be mutually exclusive; that is, most organizations would adopt one or the other to address their requirements. However, many organizations are now realizing that they need to implement both models within their enterprise.

The concept of a comprehensive “One PAM” approach is a critical success factor for effective PAM, as organizations can no longer rely on one framework to provide the level of security the business requires. A combined approach is required.

Securing Privileged Access with Symantec® PAM

Symantec PAM enhances security by protecting privileged credentials and controlling privileged access across all IT resources through the following primary critical capabilities.

Privileged Credential Vault

Historically, the privileged credential vault is the first capability that most organizations implement. Removing administrative passwords from the hands of multiple users and placing them into an encrypted data store yields significant benefits:

- Requiring two-factor authentication to ensure that users are whom they claim to be before granting access to privileged credentials.
- Enforcing policy-based access control over which credentials a privileged user may access to ensure the least privileged access and superuser containment.

- Monitoring all privileged activity and linking that activity back to an individual user to improve accountability and address regulatory compliance.
- Rotating privileged passwords automatically on a configured basis to comply with internal policies and security mandates.

One of the advantages of Symantec PAM is that the credential vault is embedded within the appliance, making it inherently more secure while simplifying deployment. Every user must authenticate themselves to PAM before gaining access to any credential; there are no backdoors that bypass this security. Additionally, because the credentials are within the appliance, they are always available.

Session Management and Recording

Privileged users often have access to multiple administrative accounts, which means that they need access to multiple privileged credentials. While the vault can protect access to these credentials, auditing the actions taken with the credential is impossible if you provide the credential to a user so they can write it down. Instead, Symantec PAM provides session management by automatically logging the user into the resource without revealing the credentials to the user.

Furthermore, when malicious or accidental actions are taken, it can be incredibly difficult to review all of the activities taken by the user. Symantec PAM addresses this challenge by capturing forensic evidence of malicious activity through providing a digital playback of all privileged user activity. Symantec PAM offers a competitive advantage in that session recording capabilities are embedded within the virtual appliance, eliminating the need for external infrastructure and providing industry-leading scale.

Behavioral Analytics

The insider threat is the most difficult to detect because users are often leveraging entitlements that they were legitimately given. Additionally, we must remember the third tenet of Zero Trust: assume breach. This means that we must assume that a privileged user will have their account compromised, thereby granting privileged access to an external hacker. Symantec PAM combats this attack vector through threat analytics. Threat analysts, a User & Entity Behavior Analytics tool, monitor and analyze privileged user activity in real-time to quickly identify abnormal behavior. It assesses the risk associated with this activity and can trigger automated mitigation actions to proactively prevent a potential attack.

Fine-Grained Access Controls

The exploitation of privileged credentials has been a critical success factor in many data breaches, so organizations have focused on implementing vaults to protect these credentials. However, as we learned in the recent SolarWinds breach, threat actors may still find ways around a vault and gain direct access to privileged credentials. If an external hacker manages to gain administrative privileges, they may then install backdoor rootkits and begin to export sensitive data.

Symantec PAM addresses this type of attack through the use of server control agents. With these agents deployed, proper controls can be enforced, even if an attacker has gained root-level access. The agents, running at the kernel level, limit what a threat actor can do, such as preventing access to sensitive files, executing malicious commands, installing programs, starting or stopping services, changing log files, or initiating new inbound or outbound communications.

Secrets Management

Privileged access is often associated with people, but numerous applications are also given privileged access to sensitive resources, and in many cases, they are accessing these privileged accounts via hard-coded administrative credentials that may be stolen or misused—often with little to no security protecting them. This is especially true in more mature environments where DevOps practices are introducing automated processes that see no human intervention at all.

Symantec PAM addresses this challenge with two complementary features: Secrets Management and application-to-application password management. Both provide an automated process for apps to call out and retrieve privileged credentials on demand, thus eliminating embedded credentials from scripts and configuration files. Additionally, both support rotating privileged credentials on a periodic basis to comply with security policies. This provides effective protection and management of these privileged credentials that are being utilized by non-human devices by integrating security within the DevOps toolchain—allowing privileged account passwords, keys, tokens, and other secrets to be stored in an encrypted vault.

Hybrid Environment

Modern application development and deployments run on architectures that span on-premises resources, virtualized data centers, and public cloud environments, and this hybrid nature can result in a fragmented, siloed approach to privileged identities. To ensure consistency, access controls, and governance need to be centrally managed, dynamically applied, and contextually enforced for environment-specific privileged accounts (such as AWS superadmin accounts). This necessitates that the PAM platform must be comprehensive in coverage to span the hybrid environment and manage both human and non-human privileged access.

Enforcing Policy Controls over Privileged Access

SYMANTEC PAM

Enhance security by protecting privileged credentials and controlling privileged access across all IT resources through the following primary critical capabilities:

- Privileged Credential Vault
- Session Management and Recording
- Behavioral Analytics
- Fine-Grained Access Controls
- Secrets Management
- Hybrid Environment

Summary

Symantec PAM provides holistic privileged access security for the entire enterprise, covering a wide range of use cases through its critical capabilities. It also offers the following competitive differentiators:

- **Scalability:** One of the major strengths of Symantec PAM is scalability. Through internal testing, we have routinely found that our appliance can support far more concurrent sessions than our major competitors. This means that in larger environments, our competitors require significantly more hardware to provide the same levels of service that PAM can deliver.
- **Comprehensive Protection:** Historically, PAM solutions delivered either PASM or PEDM capabilities, and to get both, an organization would need to buy two separate solutions. Symantec PAM can deliver both sets of capabilities and manage them from a single user interface.
- **Total Cost of Ownership:** Due to its scalability, Symantec PAM requires fewer infrastructure components to purchase, deploy, configure, and maintain. Additionally, our appliance-based architecture also requires less maintenance to support. Combined with the single user interface to manage both PASM and PEDM capabilities, this yields the lowest total cost of ownership.

BROADCOM®
connecting everything®

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

SYM-PAM-PolicyControls-SB100 December 18, 2023