PRODUCT BRIEF

AT A GLANCE

Privileged Access Management protects and controls access to privileged accounts, credentials, secrets and sessions to prevent unauthorized access and data breaches.

KEY BENEFITS

- Control privileged access across all IT resources, from cloud to mainframe
- Enable process automation and secure DevOps toolchains
- Automatically discover and protect cloud-based and virtual resources
- Provide tamper-proof audit data and forensic evidence for privileged activity
- Enforce fine-grained access controls to segregate the duties of administrators and superusers

KEY FEATURES

- Privileged credential vault
- Secrets management
- Session management and recording
- Behavioral analytics
- Host-based server controls
- Enterprise scalability

Privileged Access Management

Overview

Organizations are under tremendous pressure to secure their customer, financial, and other proprietary data against a burgeoning pantheon of threats. Research has shown that the exploitation of privileged accounts has been a critical success factor in many data breaches, which has driven many regulations and industry best practice guidelines to require stricter control over users with elevated entitlements.

Addressing privileged access has traditionally been difficult because privileged accounts are not just granted to employees with direct, hands-on responsibility for system and network administration, but also to vendors, contractors, business partners, and others. Furthermore, in many cases, privileged users are not even people; they might be applications or scripts that are empowered by hard-coded administrative credentials that are ripe for theft and misuse. Additionally, the threat surface has expanded exponentially with the adoption of hybrid environments and automated DevOps toolchains, which create new environments, often with little to no security in place.

Symantec® Privileged Access Management (PAM) is designed to prevent security breaches by delivering a set of comprehensive privileged access management capabilities. The following capabilities are included with PAM:

- **Privileged credential vault:** Protect and manage access to sensitive administrative credentials by storing them in an encrypted database.
- **Secrets management:** Eliminate hard-coded passwords from applications, configuration files, and scripts to enable secure communications and automation within DevOps toolchains.
- **Session recording:** Capture privileged account activities that are linked to individual users for accountability and forensic evidence.
- **Behavioral analytics:** Combat the insider threat and compromised accounts by detecting changes in normal user behavior.
- **Fine-grained access controls:** Restrict the entitlements for specific accounts, such as admin or root, to ensure least privileged access.
- **Enterprise scalability:** Implement a solution that can scale, address a wide range of use cases, and deliver superior performance.

For those that suffer a breach, the repercussions can be costly fines, increased public scrutiny, decreased customer loyalty, and reduced revenues. PAM enables organizations to implement comprehensive privileged access controls across all IT resources, can scale to address large enterprise environments, and is cost effective.

Privileged Credential Vault

Protecting privileged accounts is often difficult because the credentials to access them are often shared by multiple individuals. PAM protects and manages access to these credentials by safely storing them in a vault, applying best practices and limiting risk of theft or disclosure by encrypting them at rest, in transit, and in use. The solution adheres to a zero-trust, policy-based access model to ensure that only authorized users are granted access to privileged credentials and accounts, and that users are positively authenticated with two-factor credentials before this access is granted. The solution supports a range of authentication mechanisms, including passwords (stored in Active Directory, Azure Active Directory, or any LDAP compliant directory), identity federation, multifactor credentials (Symantec VIP, Symantec Advanced Authentication, PKI/X.509 certificates, HSPID-12 PIV and CAC cards, and RSA SecurID), and external authentication services (RADIUS, TACACS+, and HSM). The vault can store passwords and other sensitive credentials, including SSH keys, Amazon Web Services credentials, and PEM-encoded keys. It can also automatically rotate and expire credentials to ensure compliance with security policies.

Secrets Management

A secret is a piece of information that must be protected to avoid discovery. In the digital world, secrets are often leveraged by and embedded within DevOps tools and processes to enable automation to deliver applications faster. Lapses in adequate security controls allow malicious actors to compromise secrets, giving them unrestricted access and elevated permissions, enabling them to steal data and significantly disrupt business operations. Secrets management protects and authorizes access to this sensitive information. PAM has supported secrets management for years through a feature called App-to-App Password Management. This feature allows the removal of embedded passwords from applications, configuration files, and scripts. The passwords were instead stored in the encrypted vault, and were only retrieved when needed. In addition, the solution enabled organizations to rotate and change these passwords to comply with internal security policies, something that was very difficult and time consuming to do when they were embedded through the environment. These capabilities have been significantly enhanced. The solution now allows you to create vaults to securely store many different types of secrets, including the ability to define your own secret types through the user interface, command line, or REST API. Additionally, PAM can apply role-based access controls over vault management and secrets ownership, so that only authorized individuals can access, view, and use these secrets. The solution also supports the enforcement and notification of expiration and deletion dates.

Session Recording

Privileged accounts are often used for administration, operation, and maintenance of shared resources, and are often shared across multiple users. But shared accounts (such as root and admin) do not provide accountability. Shared accounts lack the ability to trace activities back to the user who performed the actions, resulting in increased security risk as well as compliance challenges. PAM enables full attribution for shared account activities to individual privileged users. The solution separates user authentication from shared account access, enabling the ability to link session-based clicks, commands, and entries to the individual user who *checked out* the credential. This audit data is stored in an encrypted, tamper-proof vault, where you can view it with internal tools or export it. PAM can also capture a video recording of all privileged user activity to improve accountability and provide forensic evidence of malicious activity. In addition, the solution architecture enables PAM to record significantly more concurrent sessions per appliance than most competitive products. This capability allows you to capture more forensic evidence at a lower cost. Combined, the audit data and the forensic data are critical to support compliance audits and security investigations.

Behavioral Analytics

Privileged accounts generally provide elevated access that, if compromised, would enable a malicious user to access and steal sensitive data. Certainly preventing external users from gaining access to these accounts should be a critical focus, and implementing strong authentication can help to combat this type of attack. However, Zero Trust states that we must assume breach, and therefore plan for this occurrence. PAM provides an optional module called Threat Analytics, which delivers behavioral analytics to the solution. Threat Analytics takes, as input a stream of data about how a given privileged user or group of privileged users interacts with services or applications. Machine learning and advanced algorithms continuously assess these user activities. The activities are compared to their own historical actions, as well as to the behavior of other users, to accurately identify out-of-pattern activities. Once a predefined threshold has been reached, Threat Analytics can trigger automated mitigation actions, including triggering session recording, forcing session re-authentication, and real-time alerting to mitigate the issue and protect the enterprise.

Fine-Grained Access Controls

Privileged accounts generally provide unrestricted access and permissions, which is why they are often targeted by external hackers. These accounts are required to perform key activities, so removing or blocking access to them is not a feasible option; however, there are ways to minimize the damages by enforcing granular controls over these accounts. PAM provides the following types of controls over privileged users and accounts: command filtering, socket filtering, separation of duties, server OS hardening, registry protection, sudo controls, and more. These capabilities enable organizations to restrict specific users from performing specific actions that would ordinarily be granted by the privileged account. Furthermore, the PAM architecture also enables the enforcement of zones of containment and zones of trust which logically and systematically restricts which systems can communicate with each other. This systematic restriction can be useful for attack mitigation when a malicious user has compromised a privileged account in one segment and is seeking to leapfrog into another.

Enterprise Scalability

The privileged access management journey for most organizations began with implementing an encrypted vault, and often times, only for protecting access to a specific set of resources for a specific set of users. Organizations soon realize that this approach is not sufficient, and then look to expand their deployments to cover significantly more resources, more users, and more use cases. This expansion can present two challenges. First, the solution they have does not support all of the new use cases they want to address. Second, the solution cannot easily scale to address the expanded environment.

PAM addresses these challenges with the following key attributes:

- **Fast time-to-protection:** PAM can be quickly deployed as a hardened device or virtual appliance, and you can quickly configure the solution through an easy-to-use console to achieve faster-time-to-protection and reduced implementation costs.
- **Enterprise performance and scalability:** As one of the most efficient and scalable technologies, PAM can handle and record significantly more simultaneous connections than other solutions. This scalability supports large-scale deployments with minimal infrastructure.
- **Total cost of ownership:** PAM provides the encrypted credential vault, session recording, threat analytics, and secrets management features as part of its base software license, which combined with its scalability offers best-in-class total cost of ownership.

Summary

PAM provides a comprehensive approach for detecting and preventing unauthorized access and usage of privileged credentials and accounts (the most common threat vector for targeted breaches and insider attacks). Our appliance-based solution installs quickly, and it is easy to use and maintain. It also offers the scalability and unparalleled performance needed for customers seeking an enterprise-wide solution. Combined, both these benefits yield the lowest total cost of ownership in the industry.

For more information, please visit: www.broadcom.com/symantec-pam

Symantec™
by Broadcom Software

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

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