Symantech PAM (Privileged Access Management) features enablement security audit compliance regulations

Seema Kalwani

Independent contributor
IL, USA.

Abstract:
The article provides Symantec PAM features that can address and that stand in the way of the audit regulatory compliance queries for financial institutions. The article explores the varied features of the Symantec PAM and the floor of audit queries that can be posed by regulatory bodies. It delves into the features that go above and beyond in meeting the audit compliance requirement, also detailing the drawbacks and challenges to be aware of while making a decision to implement the product.

Keywords: CA PAM, Symantec PAM, Audit regulatory compliance, Identity and Access Management.

I. INTRODUCTION TO SYMANTEC PAM

Protecting privileged access has moved beyond the vault and enterprises require a platform that can scale to secure an exponential number of accounts and credentials with elevated access and is flexible enough to cover a wide variety of use cases. A brief of the features that Symantec PAM provided
(1) Credential vault: Store privileged credentials in an encrypted vault and only grant access after users have been positively identified.
(2) Zero Trust Access: Implement zero trust approach that denies all access by default and only grants access through explicit policies.
(3) Threat Analytics: Monitor privileged user activities to assess risk and trigger automatic mitigation actions when unusual behavior is detected.
(4) Session Recording: Capture a video of all privileged user actions to improve accountability and provide forensic evidence of malicious activity.
(5) Fine-Grained Access: Enforce fine-grained access controls over super user accounts to support secure task delegation and compromised accounts.
(6) Secrets Management: Enable applications and scripts to retrieve secrets from an encrypted vault rather than have these credentials hard-coded.

II. SYMANTEC PAM ARCHITECTURE

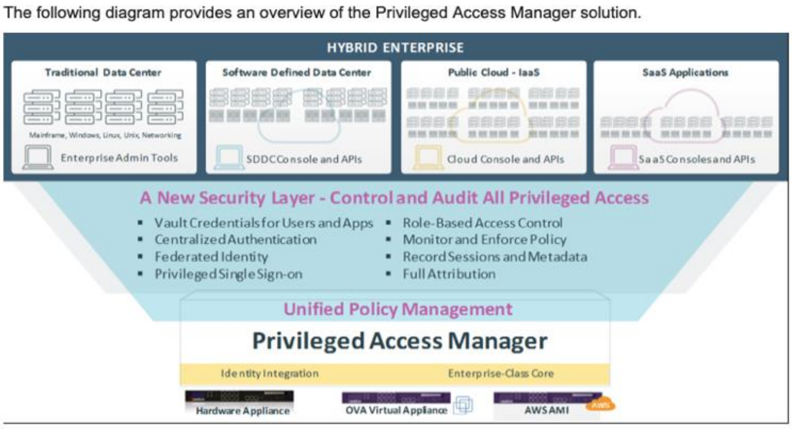

The following diagram provides an overview of the Privileged Access Manager solution.
HYBRID ENTERPRISE
Traditional Data Center
Mainframe, Windows, Linux, Unix, Networking
Enterprise Admin Tools
Software Defined Data Center
SDDC Console and APIs
Public Cloud - IaaS
Cloud Console and APIs
SaaS Applications
SaaS Consoles and APIs
A New Security Layer - Control and Audit All Privileged Access
Vault Credentials for Users and Apps
Centralized Authentication
Federated Identity
Privileged Single Sign-on
Role-Based Access Control
Monitor and Enforce Policy
Record Sessions and Metadata
Full Attribution
Unified Policy Management
Privileged Access Manager
Identity Integration
Enterprise-Class Core
Hardware Appliance
OVA Virtual Appliance
AWS AMI
AWS

Fig. 1. Privileged Access Manager Solution taken from Broadcom training docs

A. *Policy Enforcement*

Policy enforcement compartmentalizes high-risk users using integrated Java applets with a reverse port-tunneling access technology that provides segregation of critical IT infrastructure components and separation of duties that easily meets compliance requirements. Users are contained within these compartments through the CA Technologies Leap Frog Prevention™ technology, which employs a whitelist/blacklist approach, blocking users from leaving authorized areas at the socket level.

B. *User Activity Monitoring*

User activity monitoring watches user activity with real-time alerts for attempted policy violations. Administrators are notified immediately when an access violation has been attempted, detected, and prevented. Access might be terminated when a user attempts to access an unauthorized system or device.

C. *User Event Recording*

User event recording provides centralized tracking of all activities and events using session recording and playback capabilities. An administrator can have complete visibility into user activities in CLI sessions. You can configure event recording that is based on individual user profiles or individual back-end devices. All command line activity is monitored, recorded, and archived for audit and compliance purposes.

D. Centralized Reporting

Centralized reporting provides comprehensive, customized audit and compliance reports for any user-initiated events. The reports can include usage data and attempted security violations. You can also run automated reports that are focused on the compliance of individual users. You can configure the automated reports to run at predetermined intervals and then distribute the reports using email.

E. Privileged Access Management Server Control (PAM SC)

The Server Control module makes the PAM Server the central management server for all Server Control functions. The Server Control module replaces the Enterprise Management Server in the standalone PIM and PAM SC products. The Server Control module includes components and tools that allow you to:

1. Deploy policies to endpoints.
2. Define resources
3. Define accessors
4. Define access levels

III. AUDIT REQUIREMENTS

Please note the below audit criteria being used for this article.

A. *Multi-factor Authentication (MFA)*

Ensure that people and systems are authenticated prior to accessing information systems and data according to the criticality and sensitivity of information systems and data. 1) Multi-factor authentication must be utilized for all the user access to privileged accounts 2) Multi factor authentication mechanisms must be utilized for all remote access to the organization’s networks and information systems.

B. *Restricted Access*

Ensure that privileged access to information systems and data is restricted, monitored and controlled to prevent unauthorized use and misuse. 1) New or modified access must be granted only on an as-needed and/or need-to-know basis to support the principle of least privilege after approval by the user’s manager and application owner. 2) Privileged access must be reviewed and recertified at a minimum twice a year 3) The use of privileged access must be independently reviewed and validated to detect misuse.

C. *Security Authentication*

- Only authentication mechanisms approved by the information security group may be used.
- Authentication data such as passwords, cookies, tokens must be protected during storage and transmission using approved encryption mechanism.
- Identification and/or knowledge-based authentication mechanism must be used to verify accounts

IV. SYMANTEC PAM ADDRESSING THE AUDIT REGULATION

A. Multi-factor Authentication

PAM access control facilitates stronger or multi-factor authentication for privileged users. In addition, the product fully supports enabling technologies like PKI/X.509 certificates and security tokens. Its support for Personal Identity Verification/Common Access Cards (PIV/CAC) ensures compliance with U.S. Federal Government HSPD-12 and OMB M-11-11 mandates.

B. Restricted Access

PAM access control employs a unique "Deny All, Permit by Exception" (DAPE) security model to control access for high-risk users with zero footprint on the network. Users are granted visibility only to authorized areas. This security model also offers a centralized, secure access channel for administrators. Administrators gain a single point of entry and view to critical IT infrastructure.

C. Monitoring

In terms of getting session recordings of users that do connect to servers using the feature of Symantec PAM called auto-login the monitoring is effective. Yet to locate a particular breach that may have happened would need the exact date/time to be able to pin point. At times can be a struggle to locate the exact item although it is recorded.

D. Encryption

The cryptography portion of the configuration of Symantec PAM version 4.1.3 and above does allow the capability to disable the ciphers that might be old and not supported by the organization's information security.

V. SYMANTEC PAM DRAWBACK TO MEET AUDIT REGULATION

A. Multi-factor Authentication (MFA)

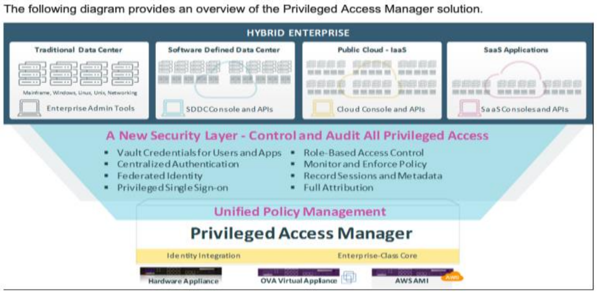
The Privileged Access Management Server Control (PAM SC) side of the component which integrates with Symantec PAM does have the capabilities to do granular monitoring at the endpoint level. Yet the implementation of PAM SC might cost expensive and the client need to be installed on every single system in the enterprise to provide the monitoring ability.

B. Event Recording

There is a provision to send all the events of activities happening at the Symantec PAM end by the users and admin to Splunk. Which does take care of the most of the audit concerns. Yet in transmission the events were noticed to be lost when the configuration was UDP versus TCP

C. Recertification

Different recertification product which has capabilities to integrate with Symantec PAM field need to be used. The RESTAPI capabilities are still developing and integrations have seen to be a trouble.



The following diagram provides an overview of the Privileged Access Manager solution.

HYBRID ENTERPRISE
Traditional Data Center
Mainframe, Windows, Linux, Unix, Networking
Enterprise Admin Tools
Software Defined Data Center
SDDC Console and APIs
Public Cloud - IaaS
Cloud Console and APIs
SaaS Applications
SaaS Consoles and APIs
A New Security Layer - Control and Audit All Privileged Access
Vault Credentials for Users and Apps
Centralized Authentication
Federated Identity
Privileged Single Sign-on
Role-Based Access Control
Monitor and Enforce Policy
Record Sessions and Metadata
Full Attribution
Unified Policy Management
Privileged Access Manager
Identity Integration
Enterprise-Class Core
Hardware Appliance
OVA Virtual Appliance
AWS AMI
AWS

Fig. 1. Privileged Access Manager Solution taken from Broadcom training docs

CONCLUSION:

Symantec PAM has great features from a user and admin perspective, it is easy to learn and administer. User experience from a usability stand point mostly depends upon the way architecture and configuration is done in each environment. To extract data from Symantec PAM has been restrictive and may need programming expertise to build additional customized modules. To address audit and compliance requirements for financial institutions may need more work as the REST API integration component is still undergoing enhancements.

REFERENCES:

1. Broadcom, “Symantic Security Software”, https://techdocs.broadcom.com (accessed Nov 21 2024)
2. Broadcom, “Mordernize the credential vault – Extend priviledged access controls to protect secrets, enable DevSecOps, and enforce zero trust architecture”, https://www.broadcom.com/products/identity/pam (accessed Nov 21 2024)
3. Broadcom, “Symantec Enterprise Blogs/Product Insights”, https://www.security.com/product-insights/role-symantec-privileged-access-management (March 2021)
4. Broadcom, “Symantec PAM Overview”, https://www.youtube.com/watch?v=i7l6tqYb0KA, (December 2023)
5. Rob Marti, “Beyond the vault – where to take your PAM Implementation next with Symantec”, https://www.security.com/product-insights/beyond-vault-where-take-your-pam-implementation-next-symantec. (September 2021)