Symantec™
A Division of **Broadcom**

Product Brief

Symantec Privileged Access Management

Overview

Organizations are under tremendous pressure to secure their customer, financial, and other proprietary data against a burgeoning pantheon of threats. For those that suffer a breach, the repercussions can be costly: fines, increased public scrutiny, decreased customer loyalty, and reduced revenues. Because the exploitation of privileged accounts has been a critical success factor in many data breaches, organizations are focusing on privileged access management as the foundation to data breach prevention.

Business Challenges

Addressing privileged access is difficult because privileged accounts and access 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. In addition, the adoption of hybrid environments is expanding the threat surface with the introduction of new attack vectors, such as management consoles and APIs, often with little to no security in place. Furthermore, in many cases, privileged accounts are not even people; they might be applications or configuration files empowered by hard-coded administrative credentials. Compounding the problem, DevOps tool chains are introducing automated processes that often use embedded credentials that are ripe for theft and misuse. You need to address these challenges quickly with a proven privileged access management solution that works across all IT resources, can scale to address the entire enterprise, and is not cost-prohibitive.

Solutions Overview

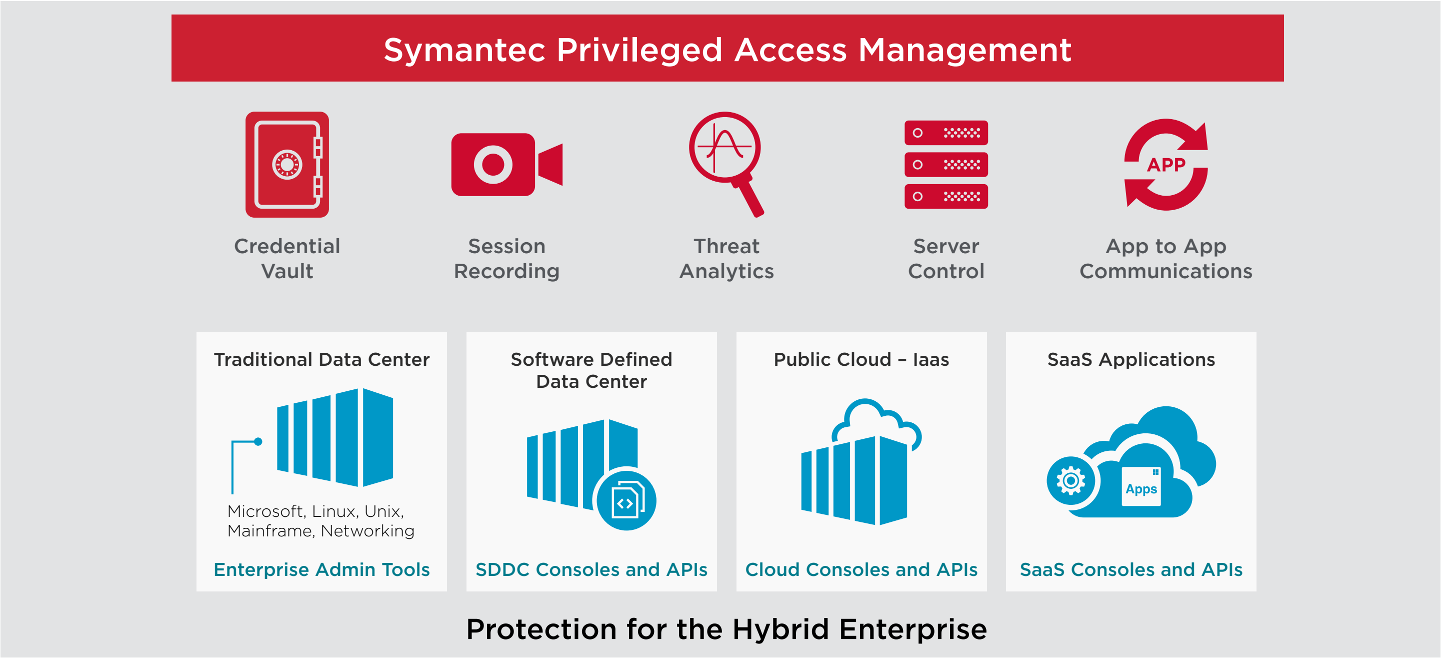
Symantec Privileged Access Management is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies, and monitoring and recording privileged user activity across virtual, cloud, and physical environments. The solution provides a privileged credential vault, session recording, threat analytics, host-based access control for mission-critical servers, and application-to-application password management to address non-human actors, such as applications, configuration files, and scripts.

Key Benefits

- Control privileged access across all IT resources, from cloud to mainframe.
- Apply unified cross-platform protection and management of privileged account credentials.
- Automatically discover and protect virtual and cloud-based resources.
- Provide tamper-proof audit data and forensic evidence for all privileged user activity.
- Segregate duties of superusers through fine-grained access control and secure task delegation.
- Eliminate hard-coded passwords from apps, scripts, and files.
- Support DevOps toolchains.

Key Features

- A privileged credential vault with a zero-trust access model.
- Threat analytics with machine learning and automated mitigations.
- Host-based access control to protect mission-critical servers and containers.
- Application-to-application password management with flexible options.
- Audit data and forensic evidence to support compliance and investigations.



Symantec Privileged Access Management

Credential Vault

Session Recording

Threat Analytics

Server Control

App to App Communications

Traditional Data Center

Microsoft, Linux, Unix, Mainframe, Networking

Enterprise Admin Tools

Software Defined Data Center

SDDC Consoles and APIs

Public Cloud – Iaas

Cloud Consoles and APIs

SaaS Applications

SaaS Consoles and APIs

Protection for the Hybrid Enterprise

Features and Capabilities

Symantec Privileged Access Management delivers a comprehensive solution to prevent data breaches and to combat insider threats through the following features and capabilities:

- **A privileged credential vault** protects and manages sensitive administrative credentials, such as root and administrator passwords and SSH keys. Credentials are stored in a secure vault and automatically rotated to ensure compliance with security policies. A zero-trust, policy-based access model ensures 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.
- **Threat analytics** provides continuous, intelligent monitoring that assesses privileged user behavior and leverages machine learning to compare current actions to historical observations and the behavior of other users. When unusual or risky behavior is detected, mitigating controls can be automatically triggered to stop attacks and limit damages, and to combat insider threats and account takeover attacks.
- **Host-based access control** protects mission-critical servers with powerful, fine-grained security controls over operating system-level access and privileged user actions. Host-based access control protects and monitors files, folders, processes, registries, and connections to the Docker daemon. Host-based access control can also manage who is allowed to run docker commands on a host, and enable UNIX and Linux users to be authenticated using active directory and Kerberos.
- **Application-to-application password management** eliminates hard-coded, hard-to-change passwords from applications, scripts, and configuration files, providing effective protection and management of these privileged credentials. This capability supports application-to-application, application-to-database, and continuous delivery and continuous DevOps use cases. Additionally, the solution offers both agent-based and agentless integration options.
- **Audit data and forensic evidence** is captured to support compliance audits and security investigations. Positively authenticating users before granting access allows the solution to link all privileged access and activity to a named user. This audit data is stored in an encrypted, tamper-proof vault, where you can view it with internal tools or export it. The solution can also capture a video recording of all privileged user activity to improve accountability and provide forensic evidence.

Critical Differentiators

Symantec Privileged Access Management offers the following competitive differentiators:

- **Fast time-to-protection**. Quickly deploy the solution as a hardened device or virtual appliance. Easily 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 privileged access management technologies, the solution can handle and record significantly more simultaneous connections than other solutions can. This scalability supports large-scale deployments with minimal infrastructure.
- **Automated risk mitigation**. The solution monitors all privileged user activity, analyzes it in real-time, and can trigger automatic mitigation actions when unusual behavior is detected. The solution enables an immediate response to potential risks without any human interaction.
- **Flexible deployment architecture**. The solution supports agent-based and agentless deployment options, which can be used individually or jointly to provide a comprehensive strategy to address privileged access management challenges.
- **Meaningful security insights**. Robust reporting tools and dashboards make it easy for security teams to investigate incidents, respond to inquiries for information, and to understand how their privileged accounts are being accessed and used.
- **Protection for hybrid enterprise**. Discover, protect, and provide granular separation of duties for cloud consoles, APIs, and virtual resources, and also secure privileged access on your legacy mainframe environment and mission-critical servers.
- **Total cost of ownership**. The solution offers best-in-class total cost of ownership because the solution is quick to deploy, easy-to-use, and scalability. Additionally, the new portfolio license agreement offers flexibility and lower, predictable costs, for your organization.

Additional Capabilities

Symantec, a Broadcom division, offers a broad portfolio of cybersecurity software designed to protect the largest, most complex, and most demanding IT environments.

You can easily add the following capabilities to further extend the Symantec Privileged Access Management solution:

- **Advanced authentication** provides a variety of multifactor credentials and mechanisms that can be used to positively authenticate users before granting them access to any privileged accounts or credentials.
- **Full privileged user lifecycle management** streamlines and automates the processes associated with managing privileged users, including privileged account and credential access requests, security and SoD (separation of duties) violation checks, approval routing, and privileged access provisioning, certification, and de-provisioning.
- **Secure DevOps automation** implements continuous delivery and continuous testing capabilities that leverage Symantec Privileged Access Management to eliminate hard-coded administrative credentials from automated processes that could otherwise be stolen and misused.

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

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-PAM-PB100 December 5, 2019