Solution Brief

Symantec
A Division of Broadcom

Are You Managing and Governing Your Privileged Users?

Challenge

Stealing and exploiting privileged credentials and accounts is a critical success factor for many types of cyberattacks. Thankfully, organizations have recognized these dangers and are focusing their protection efforts in this area, but still many are failing to manage and govern their privileged users on an ongoing basis.

Opportunity

Organizations have deployed privileged access management solutions to better protect and control access to privileged accounts and their credentials. However, these deployments are often limited in scope because organizations lack the automated processes for managing privileged access on an enterprise scale. Identity management technologies provide significant value on their own, but when combined with a privileged access management solution, they enable privileged access governance.

Benefits

Privileged access governance automates processes associated with requesting, approving, provisioning, and certifying access to privileged accounts and credentials. In addition, using identity governance with privileged access management also provides visibility into administrator access and actual usage, which can greatly assist with ongoing audit and compliance efforts.

Numerous, headline-making incidents in recent years show that cybercrime continues to rise and that organizations continue to struggle with an ever-increasing attack surface. Privileged access governance enables organizations to manage and govern their privileged users more efficiently and to fight back against cybercrime more effectively.

Background

Many data breaches and insider attacks exploit privileged accounts or credentials. This is not surprising when you consider that privileged identities have elevated access to the most sensitive resources and data in your environment; they literally hold the keys to the kingdom. Of course, hackers would seek to compromise this type of access.

Thankfully, there is a positive angle you can take. If privileged accounts are the common thread amongst innumerable attack types and vulnerability points, then these accounts, and the credentials associated with them, are exactly where you should focus your protection efforts. However, tackling this problem is not simple. Organizations face four primary challenges with privileged access:

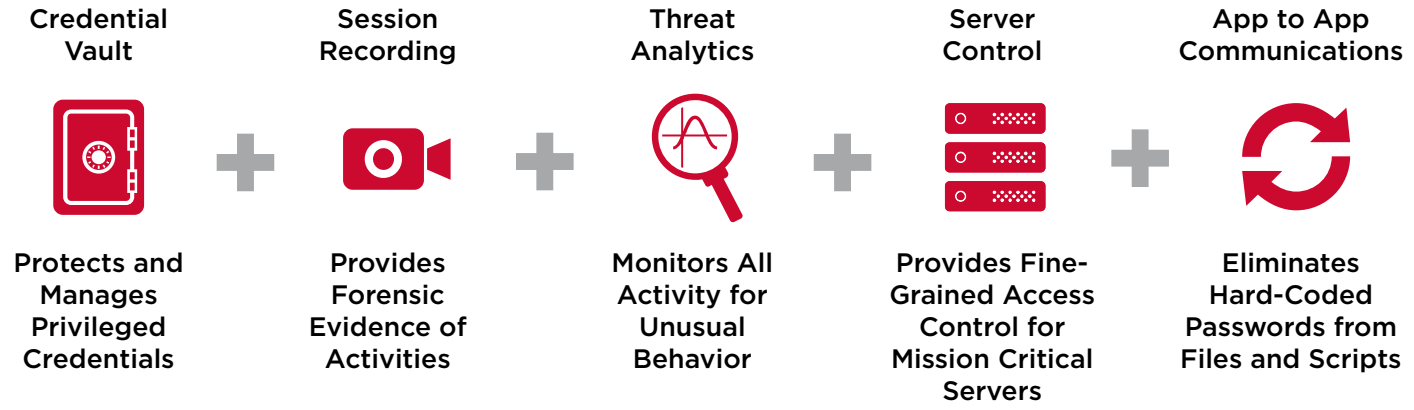
- Privileged accounts are required to perform key activities; so, removing or blocking access to them is not a feasible option.
- Privileged accounts generally provide unrestricted access; but there is no mechanism to provide fine-grained entitlements or support separation of duties.
- Privileged accounts passwords are often shared by multiple internal and sometimes external individuals; and they are rarely changed in accordance with security best practice policies.
- The number and types of privileged accounts are expanding exponentially with the emergence of cloud and virtualized environments, and the adoption of continuous delivery.

The Role of Privileged Access Management

Symantec Privileged Access Management is the strategic solution to address these challenges. The solution allows organizations to create and enforce controls over users, accounts, and systems that have elevated or privileged entitlements. Symantec Privileged Access Management also provides granular authorization of users to systems and accounts and records attempts to access these systems and accounts.

The solution also vaults and rotates the credentials for privileged accounts, including the passwords. Additionally, when you deploy the threat analytics module to the solution, you can detect unusual, out-of-pattern activities. You can then trigger automatic mitigations of these activities if the behavior is deemed too risky. However, even organizations that have effective privileged access management solutions in place often face challenges in governing privileged user access on a continuous basis.

Figure 1: Five Key Capabilities of Symantec Privileged Access Management



Introducing Privileged Access Governance

As the role of compromised privileged accounts and credentials has become clear, regulatory bodies and auditors have focused their attention on the controls that organizations must implement to mitigate these risks. Thus, organizations are subject to an ever-expanding list of data security regulations and standards that mandate increased auditing and controls over users with privileged access. Compliance with these regulations and audits generally focus on two points:

- Control the access of privileged users to critical resources and the actions that they can perform on those resources.
- Govern the access of privileged users on an ongoing basis to make sure that they have only the level of access that they absolutely need.

Privileged access management addresses the first point; and identity management addresses the second point. When you combine the two, this yields privileged access governance.

Privileged access governance ensures that all user access to privileged accounts and credentials is required and appropriate. Privileged access governance applies the basic identity governance and administration processes to privileged users, including the following processes:

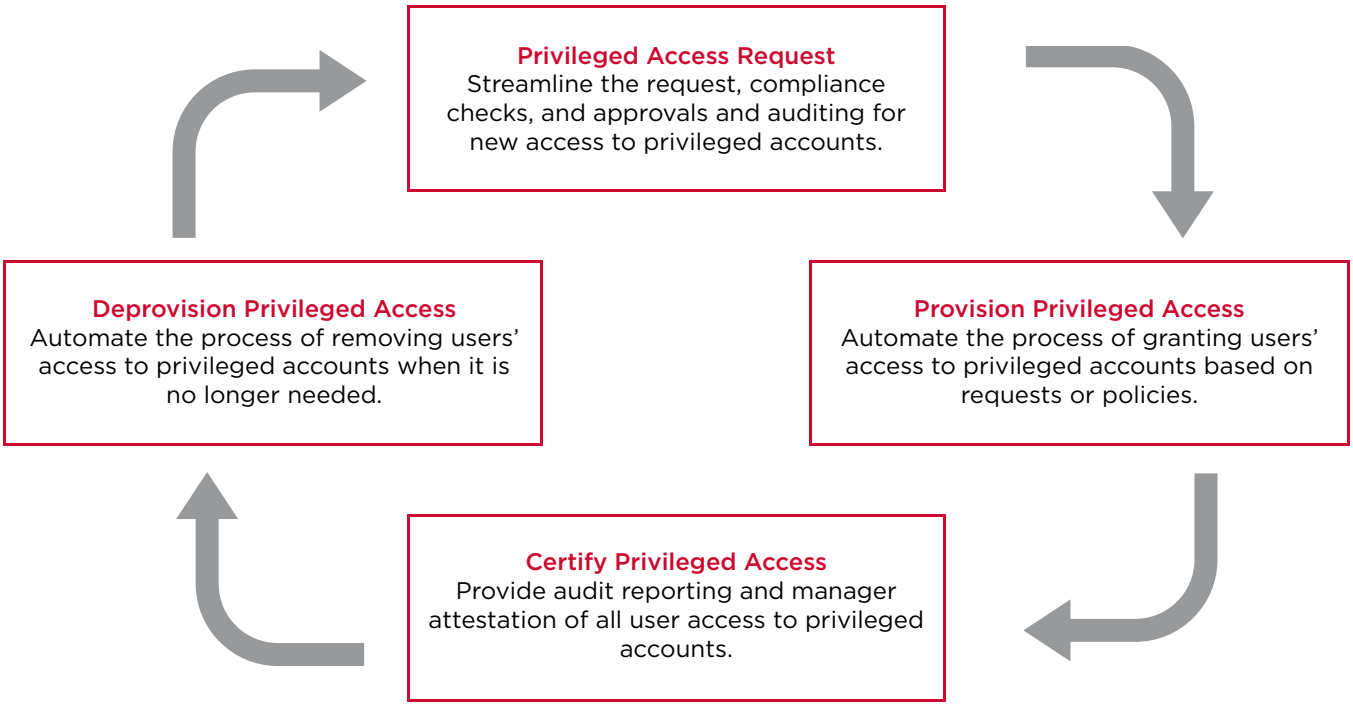
- Automated provisioning for new users based on group members or roles, and automated deprovisioning when users leave the organization or change jobs.
- A streamlined request process that gathers appropriate approvals and checks for security violations before new privileged access is granted.
- Periodic reviews and attestations to ensure that access to privileged accounts is still necessary.

You can realize privileged access governance by integrating Symantec Privileged Access Management with Symantec Identity Management. Together, these solutions significantly improve your security posture and help address compliance. When auditors ask you for proof that access to all privileged accounts has been properly reviewed and authorized, you can provide it.

The Symantec Solution

The Symantec solution employs a zero-trust model, which means that all access is denied by default, and that access is only allowed by explicitly defining it within a policy in the privileged access management component. To further reduce risk, privileged users are only granted the minimal access that they need to perform their jobs. The least privileged posture is maintained on an ongoing basis through full lifecycle management of the privileged user.

Figure 2: Full Privileged User Lifecycle Management



The Symantec privileged access governance solution provides the following four key capabilities:

- Automated provisioning and deprovisioning. The Symantec solution automates the provisioning and deprovisioning of access to privileged accounts, along with role and group management of all privileged users. The solution enables more granular control over privileged roles, groups, start and stop dates, and other attributes of privileged users. Privileged access can also be provisioned on a time-limited basis.
- Access requests. The Symantec solution provides a familiar shopping cart experience and a business-friendly entitlements catalog that allows privileged entitlements to be mapped from IT-centric names to business terms that are easily recognized. More importantly, requests are automatically checked for compliance or policy violations and evaluated to determine if the additional access poses more-than-normal risk.
- Delegated administration. The Symantec solution supports fine-grained delegated administration, which allows you to securely offload management activities, including basic CRUD activities, workflow approvals, and access certifications, for large communities of internal users or external users with privileged access (such as development teams or third-party service providers).
- Attestation and certification. The Symantec solution automatically gathers privileged user access entitlement data and presents this data to reviewers in an easy-to-use and customizable interface. Risk-level contextual information is provided to help reviewers focus their attention riskier users first. All rejected access can be immediately removed and all decisions are logged to support compliance audits.

The Broadcom Advantage

In today's world, consumer and regulatory expectations around security, consent, and privacy continue to increase steadily. Meanwhile, the legal, financial, and reputation costs of failure are exploding as data sets become bigger, more complex, and even more personal. With their silos and point solutions, current security models will soon be too slow, error-prone, and reliant on human scaling to address this challenge.

Symantec, A Division of Broadcom, is changing the game. With Symantec, we are bringing security and connectivity together with powerful AI and automation. The result is a unified platform that monitors data for risk across the entire enterprise, responds instantly to threats, and safeguards trust from mainframe to IoT, all at the speed and scale of the next era.

Critical Differentiators

Broadcom offers a broad portfolio of enterprise and mainframe software solutions aimed at addressing the business needs of the world's largest organizations. The following qualities are what set us apart.

- Best-in-class technology with a heritage of innovation and analyst leadership across multiple categories.
- Reliability that is trusted by 98% of the Fortune 50 companies, 19 out of 20 of the biggest global banks, and all ten of the world's largest telecoms.
- Simple business models offering more flexibility, and lower, more predictable costs to all software platforms.
- A unified vision of infrastructure software to meet and exceed the needs of the world's largest enterprise businesses.
- Investment in AI and automation that is designed to drive efficiencies through scale, security, and agility.
- A long-term, strategic partnership that is backed by over $4.7 billion in R&D spending.

Next Steps

The rise in data theft is alarming. Organizations need to consider their options and select a vendor that offers a layered, in-depth defense to combat insider threats and targeted data breaches. The Symantec portfolio offers a comprehensive strategy against ever-evolving threats, regardless of origin.

For more information, 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-PAG-SB103 February 4, 2020