A Broadcom Company

technologies

Solution Brief

Privileged Access Governance

Are You Managing and Governing Your Privileged Users?

Description

Privileged accounts hold elevated access to critical IT resources and sensitive data in your organization, the keys to the kingdom. Privileged access management can significantly help to mitigate this risk, but is it enough? Access that is needed today might not be needed tomorrow. Compliance auditors are increasingly looking for organizations to continuously inspect and govern privileged users to prevent unnecessary access. As the number of privileged identities continues to expand exponentially, manually managing this access is not feasible. Learn how privileged access management and identity management can be combined to provide privileged access governance.

Features

Privileged access governance establishes full lifecycle management over privileged users:

- Controlling access to privileged accounts and credentials.
- Enforcing fine-grained controls over what users can do with these accounts.
- Governing these access entitlements on an ongoing basis.

Applications

Layer7® Privileged Access Management
Layer7® Identity Management

Executive Summary

Challenges

Despite the numerous, headline-making incidents in recent years, cybercrime continues to rise while organizations must contend with an ever-increasing attack surface. Many types of attacks depend on stealing and exploiting privileged credentials and accounts. Organizations have recognized these dangers and are focusing their protection efforts in this area. But many are still failing to manage and govern their privileged users on an ongoing basis.

Overview

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 to a small pilot project because organizations lack the automated processes for approving, provisioning, and verifying privileged access on an enterprise scale. Privileged access management and identity management technologies provide significant value independently; but when they are combined, they enable organizations to manage and govern their privileged users more efficiently and in complementary ways. We call this privileged access governance.

Benefits

Implementing privileged acess governance can deliver significant benefits to your organization. First, automated governance processes around privileged users can help prevent breaches due to improper administrator actions or data exposure. Second, 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. Lastly, privileged access governance can also help reduce risk and improve efficiencies associated with existing processes around entitlement management and certification.

Background

Many data breaches and insider attacks exploit privileged accounts or credentials. This is not surprising when you consider that privileged identities have access to the most sensitive resources and data in your environment. Of course, hackers would seek to compromise this type of access. However, you can view the hackers' targeting of privileged users as a positive factor. If privileged accounts and the credentials associated with them are the common thread among innumerable attacks, then that is exactly where you should focus your protection efforts. But tackling this problem is not simple.

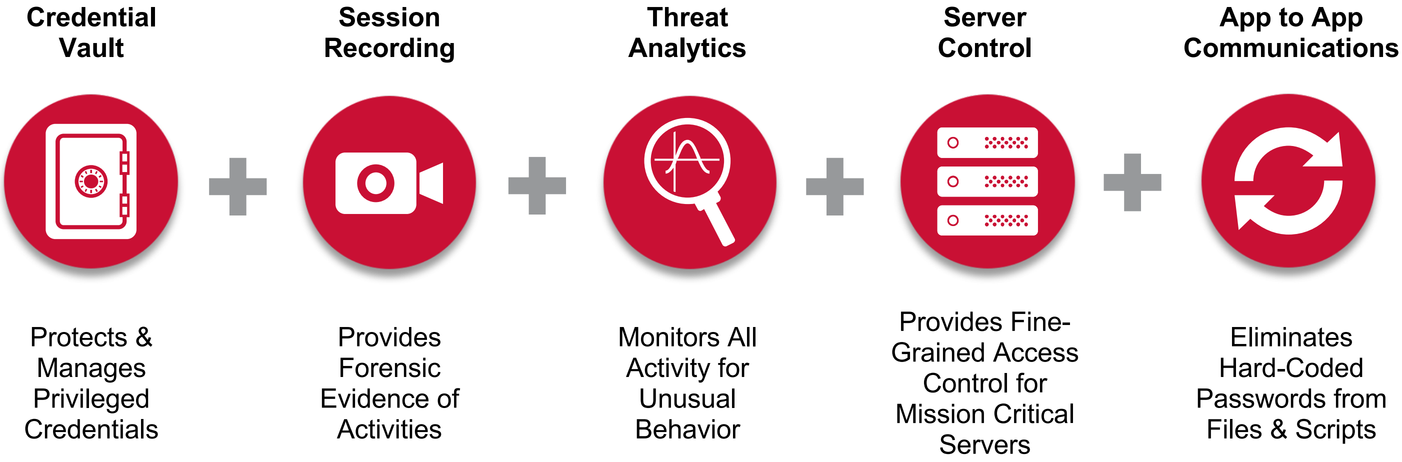
Organizations face four primary challenges with privileged access.

- 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

Layer7 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.

Five Key Capabilities of Layer7 Privileged Access Management



Credential Vault

Protects & Manages Privileged Credentials

Session Recording

Provides Forensic Evidence of Activities

Threat Analytics

Monitors All Activity for Unusual Behavior

Server Control

Provides Fine-Grained Access Control for Mission Critical Servers

App to App Communications

Eliminates Hard-Coded Passwords from Files & Scripts

Layer7 Privileged Access Management provides granular authorization of users to systems and accounts and records attempts to access these systems and account. The solution also vaults and rotates the credentials for privileged accounts, including the passwords.

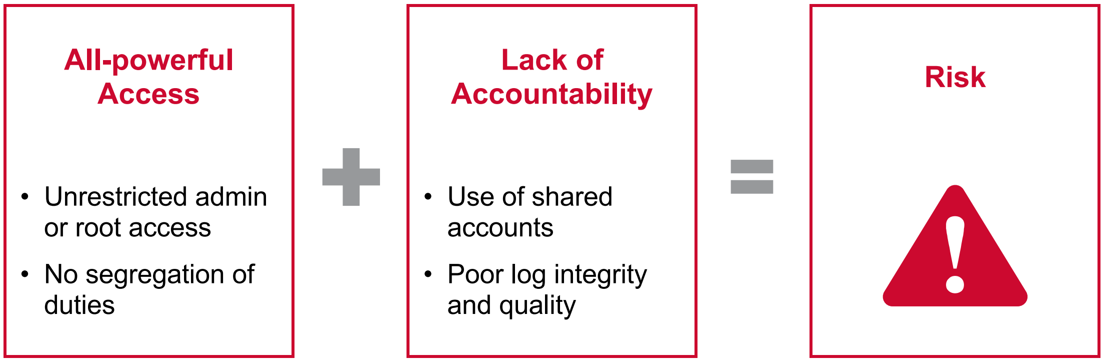
Additionally, when you deploy the threat analytics module to the solution, you can detect unusual, out-of-pattern activities. You can then trigger automatic mitigations of these activities if the behavior is deemed too risky. However, even organizations that have effective privileged access management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

The Emergence of the Compliance Conundrum

Today's breach-infested environments demand more effective ways to control the access and actions of privileged users. We have seen that many of the most damaging breaches originated with the theft of privileged credentials for many reasons, including the reasons below.

- Privileged users almost always have more access than they need for their roles.
- Privileged users tend to accumulate access rights, but often keep the ones they no longer need.
- Privileged users have limited accountability; therefore, it is often not possible to tie privileged accounts and activities back to a named user.

The Risk of Privileged Users



All-powerful Access

- Unrestricted admin or root access
- No segregation of duties

Lack of Accountability

- Use of shared accounts
- Poor log integrity and quality

Risk

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 actions.

- Controlling the access of privileged users to critical resources and the actions that they can perform on those resources.
- Governing their access on an ongoing basis to make sure that they have 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 these, you have privileged access governance.

Introducing Privileged Access Governance

Managing business user access entitlements is a continuous process. Over the years, many organizations have implemented identity management tools to automate and streamline this process to eliminate manual work and to reduce costs. But organizations have struggled to manage their privileged users because the population can be so diverse and difficult to identify.

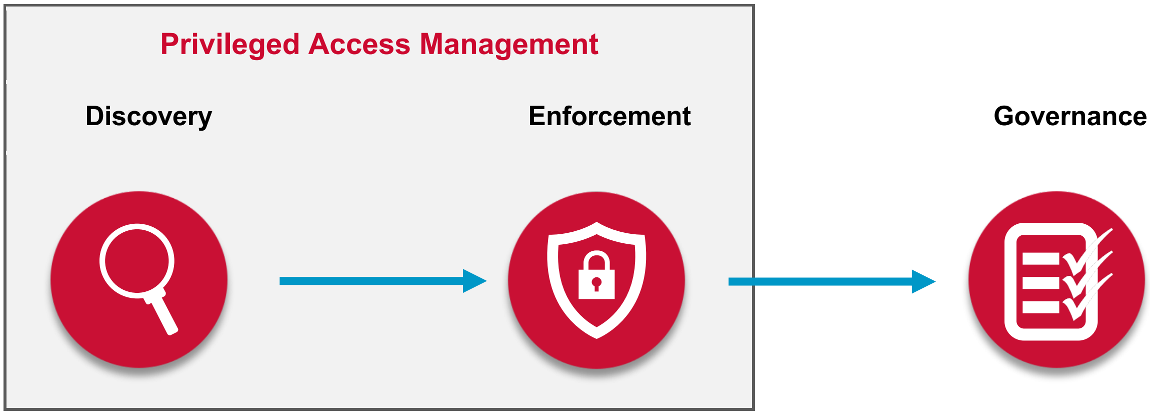
How can you map a user to a shared account when you have no idea who has been given the credentials to that account? In addition, privileged accounts and access are not just granted to employees with direct, hands-on responsibility for system administration but also to contractors and business partners. You may even have privileged unknowns who are securing shadow IT resources without your knowledge.

Introducing Privileged Access Governance (cont.)

Deploying a privileged access management solution can help because it discovers privileged accounts, maps users to these accounts, and then defines the policies that grant access to these accounts. But this solution is more concerned with discovery and enforcement, not ongoing user management. Users are imported through batch jobs in phases, while the solution is rolled out across different endpoints and systems. There is no automated provisioning or de-provisioning as these users change jobs or leave the company.

In addition, the security team is more concerned with access that already exists; they are not trying to determine if this access is appropriate or who authorized it. Governance, a critical component to achieve full privileged user lifecycle management, is missing from the solution.

Governance Gap in Privileged Access Management



Privileged access governance addresses this challenge by ensuring 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.

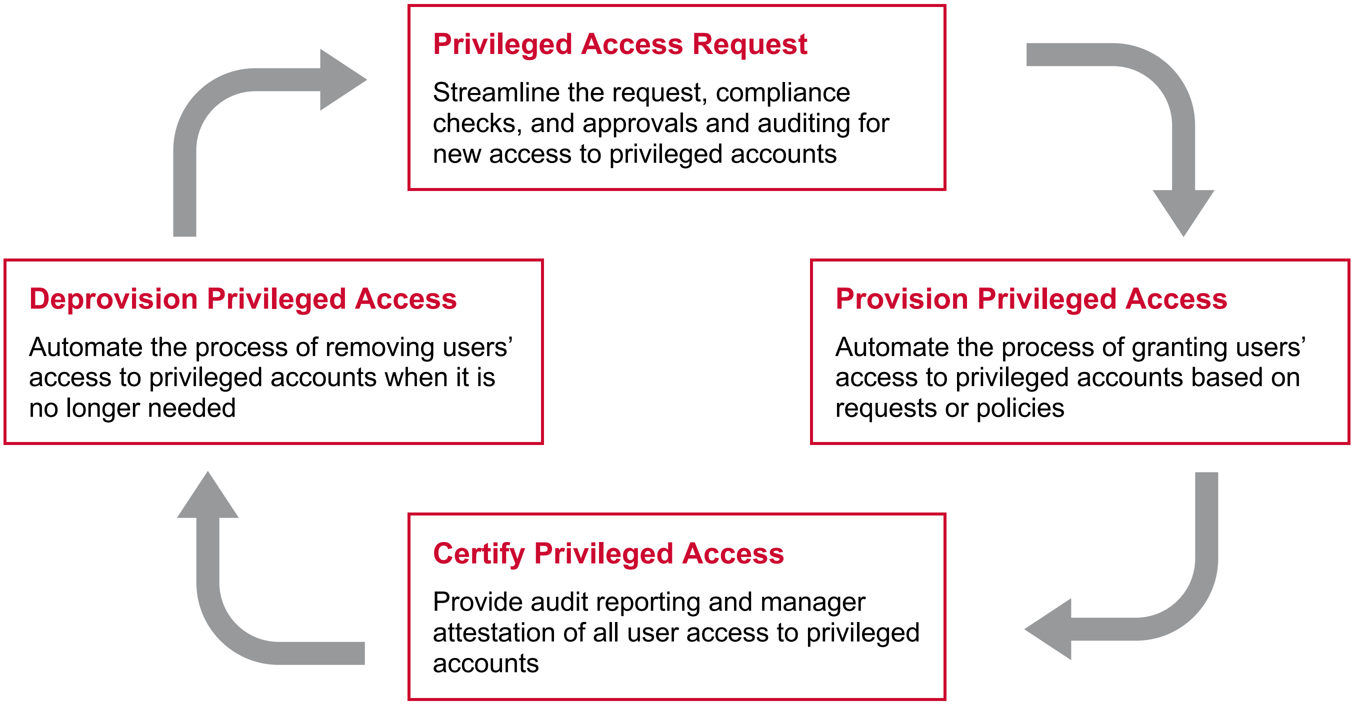
- Automated provisioning for new users based on group members or roles, and automated de-provisioning when users leave the organization or change jobs.
- A streamlined request process that gathers appropriate approvals and checks for security violations before new privileged access is granted.
- Periodic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

You can realize privileged access governance by integrating Layer7 Privileged Access Management with Layer7 Identity Management. Together, these solutions significantly improve your security posture and also 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 Layer7 Solution

The Layer7 solution employs a *zero trust* model, which means that all access is denied, and that access is only allowed by explicitly defining access within a policy, within 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.

Full Privileged User Lifecycle Management



Privileged Access Request

Streamline the request, compliance checks, and approvals and auditing for new access to privileged accounts

Provision Privileged Access

Automate the process of granting users' access to privileged accounts based on requests or policies

Certify Privileged Access

Provide audit reporting and manager attestation of all user access to privileged accounts

Deprovision Privileged Access

Automate the process of removing users' access to privileged accounts when it is no longer needed

- **Automated provisioning and de-provisioning**. The Layer7 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 Layer7 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 Layer7 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 Layer7 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.

CA Technologies, a Broadcom company, is changing the game. With Layer7, 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, 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 Global 1000 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 $3.3 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 Layer7 portfolio offers a comprehensive strategy against ever-evolving threats, regardless of origin.

For more information, please visit ca.com/us/products/security**.**

Revision History

Layer7 SB100; May 30, 2019

Initial document version.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.