Symantec by Broadcom

WHITE PAPER

A PAM Maturity Model for IT Modernization

WHITE PAPER

A PAM Maturity Model for IT Modernization

Symantec by Broadcom

TABLE OF CONTENTS

Introduction

Technology has long played a pivotal role in business strategy and growth, but software is now at the core of how enterprises compete and operate effectively in the 21st century. Organizations are rapidly undergoing IT modernizations to transform and accelerate their software delivery cycle and application development processes. These initiatives change, accelerate, and automate how code, machines, and human identities interact. IT modernizations have expanded the attack surface, amplifying risk and security concerns. Attackers are increasingly, and successfully, leveraging privileged user credentials to gain unauthorized access. A maturity model is needed to enforce policies, monitor blind spots, and enable a proactive detection model through machine-learning-driven analytics. This maturity model can reinforce the value of existing investments and improve accuracy.

IT Modernization Raises Privileged Access Risk

By necessity, organizations must continue to evolve their IT environment. As enterprises advance in their digital transformation journey, the associated risks become more pronounced, unless they have a plan for access security and governance to move in lockstep with the following initiatives:

- Enable automation with accountability and visibility
- Foster speed in delivery in tandem with protection of enterprise assets
- Ensure scale with integrated access governance and threat detection

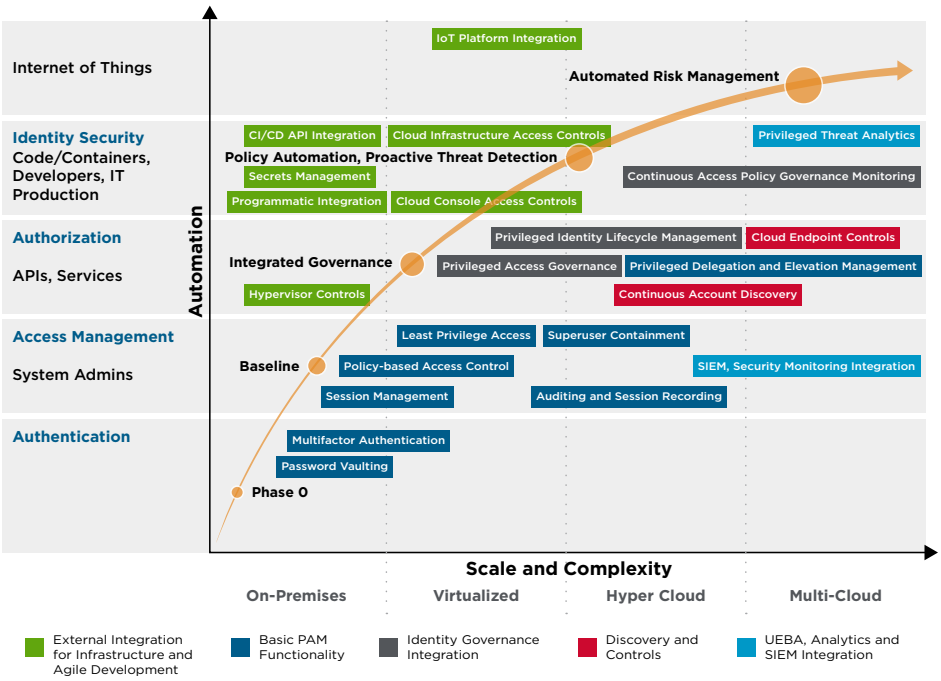
In the same way that enterprise architects are now engaged in defining a practical map for their modernization journeys, security teams need the correct tools and integration capabilities to progressively automate, accelerate, and scale access management and risk mitigation according to business needs—without the need for significant new investments.

Determining which identities should have access to specific services and resources, managing their credentials to the resources, and ensuring that the access is appropriate with minimal manual intervention and based on policy is a central challenge to enabling automation, scale, and speed. This access is especially critical for users, both human and non-human, who hold elevated access entitlements.

ENFORCING POLICY CONTROLS OVER USERS, HUMAN OR NON-HUMAN, ADDRESSES SECURITY GAPS AND YIELDS SIGNIFICANT BENEFITS

Knowing your privileged users is understanding your risk. Privileged access management (PAM) tools must support automation in the authorization process and enable scalability through the provision of both dynamic operations and ephemeral infrastructure—such as Amazon Web Services (AWS) administrative accounts for human identities or secrets management in a DevOps environment. For PAM to serve as a crucial facilitator for IT modernization instead of a bottleneck, the technology and tools need to deliver a consolidated and extensible solution to the risks created by the transformation journey. However, as shown in the following figure, most organizations follow an organic path when implementing their PAM use cases.

PAM Maturity



Establishing the Baseline

The privileged credential vault is commonly one of the first capabilities that most organizations implement. Removing administrative passwords from the hands of multiple users and putting them into an encrypted data store yields significant benefits, including the following capabilities:

- Implementing two-factor authentication before granting access to a privileged credential ensures that users are who they claim to be.
- Enforcing policy-based controls over which credentials a privileged individual can use to ensure least privileged access.
- Providing visibility to not only audit all privileged activity and link these activities back to an individual user to improve accountability, but to also record those activities as forensic evidence.

While organizations rush to implement their privileged credential vaults to protect and monitor access to the system administrator accounts, many organizations have realized that protection alone is not sufficient.

DATA PRIVACY LAWS AND INDUSTRY REGULATIONS MANDATE TIGHTER CONTROLS AND AUDITING OF PRIVILEGED USER ACTIVITIES

Integrated Governance

Organizations are subject to an ever-expanding list of data security regulations and standards that mandate increased controls and auditing of privileged access. Compliance with these regulations generally focuses on two requirements:

- Controlling the access of privileged users to critical resources and the actions that they can perform on those resources.
- Governing the access of privileged users on an ongoing basis to ensure that they have only the level of access they absolutely need.

PAM technologies address the first requirement, but integration with identity management technology is required to address the second requirement. Combining both requirements results in integrated governance. Integrated governance enables privileged access governance, ensuring that all user access to privileged accounts and credentials is required and appropriate.

Policy Automation

Modern application development and deployments run on architectures that span on-premise resources, virtualized data centers, and public cloud environments. This hybrid architecture can result in a fragmented, siloed approach to privileged identities. Additionally, privileged access is often associated with people, but elevated access to sensitive data is increasingly being given to applications. In many cases, these non-human identities leverage hard-coded administrative credentials that can be stolen or misused—often with little to no security protecting them.

To ensure consistency, access controls and governance must be centrally managed, dynamically applied, and contextually enforced for environment-specific privileged accounts (such as AWS superadmin accounts). It is necessary for the PAM platform to provide comprehensive coverage by managing both human and non-human privileged access, being scalable, and capable of supporting programmatic access and secrets management to facilitate policy automation.

Proactive Threat Detection

The third tenet of Zero Trust is to assume breach. This assumption means that organizations must evaluate how their security technologies can be compromised and what could be done to detect and mitigate the damages of that breach. Proactive threat detection focuses on two core capabilities: privileged identity analytics and privileged elevation and delegation management. Privileged identity analytics takes a context-driven approach that leverages machine learning and user and entity behavioral analytics to drive real-time detection and trigger risk mitigation steps, even in dynamic, ephemeral environments. Privileged elevation and delegation management leverages agents to protect privileged accounts by enforcing fine-grained policy controls over users who access protected devices. While proxy-based vaults are easy to deploy and manage, under specific circumstances they can be bypassed—agents cannot.

APPLYING AUTOMATED CHECKS TO THE ROLES AND ACCESS AUTHORIZATIONS ASSIGNED TO PRIVILEGED IDENTITIES CAN HELP PROACTIVELY FLAG VIOLATIONS

Automated Risk Management

The adoption of IoT not only introduces a new type of machine privileged identity in the form of IoT device controllers, but the use of the technology contributes to a potentially exponentially larger number of transactions that must be explicitly authorized and monitored for potential attacks. Dealing with the scale of identities and the volume of transactions by privileged identities requires an automated model that is effective at threat detection and supports mechanisms to evaluate risk and implement mitigation, without significantly disrupting business processes.

Additionally, Zero Trust adoption is pushing for the migration to just-in-time provisioning. Users are only given elevated access to systems at the moment they need it and have these access entitlements removed the moment they are done needing them. This policy prevents external hackers or malicious insiders from compromising a legitimate account and exploiting their privileges.

Achieve Integrated Governance and Policy Automation: One Step at a Time

Managing and securing privileged access in the context of IT modernization is a pressing challenge, but not an insurmountable one. Manual approaches that rely on a human certification process cannot scale when digital transformation expands both the number of users needing privileged access beyond traditional system administrator roles and entities that can act as privileged identities. Authorization and role requests must be managed through an integrated governance process to balance agility and security for new access scenarios. Some examples of these scenarios include developers with access to privileged credentials in production, virtualized containers and hosts with authorization to data sources, or administrators with super-user access to cloud services.

Privileged access governance applies the basic identity governance and administration processes to privileged users, encompassing the following processes:

- Automated provisioning for new users based on group memberships 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 a new privileged access authorization is granted.
- Periodic reviews and attestations to ensure that access to privileged accounts remains necessary.

The more tightly integrated PAM and identity lifecycle management processes are, the greater the scope for security teams to enable automation at scale. Applying automated checks to the roles and access authorizations assigned to privileged identities can help proactively flag violations, such as providing a developer access to credentials for production code.

ENTERPRISES MUST UNDERSTAND WHAT CAPABILITIES ARE NEEDED TO ADDRESS ALL PAM USE CASES, NOT JUST THE FIRST STEP IN THEIR JOURNEY

The key point here is that the PAM tools themselves must support automation in the authorization process, and enable scalability through support for both dynamic operations and ephemeral infrastructure, such as AWS administrative accounts for human identities.

Many existing approaches to PAM are based on the coverage of a subset of users and were not designed with modern IT infrastructure in mind. To advance through the phases of a maturity model, enterprises must consider how PAM approaches address privileged identity proliferation, distribution, and transformation. PAM progression is based on the following abilities:

- Extend governance and visibility of privileged identities from on-premises to virtualized data centers and cloud services.
- Automate the authorization of privileged access based on operational requirements through integration with identity management role-based policies, rather than manual approval processes.
- Scale and integrate controls and monitoring into dynamic and ephemeral infrastructure.
- Facilitate centralized continuous monitoring and governance to identify when excessive privileges are initially granted and trigger a remediation workflow.
- Incorporate the ability to detect and remediate new threats as they evolve through machine learning and data-driven models.

Put Risk into the Correct Context

IT modernization programs result in distributed networks, high rates of change, transactional volume, and an increase in privileged identities. This evolution presents a challenge to traditional, rules-based approaches for detecting the misuse or theft of privileged credentials. These traditional approaches have already been proven to be inadequate, even for existing threats.

Adopting a generalized approach to privileged analytics and funneling more data into security information and event management (SIEM) systems overlooks important context. This context enables security analysts and IT operations to distinguish between an inconsistency and a significant anomaly or high-risk activity that requires remediation. Instead, what is needed is a domain-specific approach that leverages context and knowledge about privileged user roles and behavior. The objective is to narrow down and respond to hard to find information about actions that constitute tangible evidence of an attack or compromise.

Privileged identity analytics operate on the same principles of defining behavioral baselines: what actions are privileged users taking, what have they done in the past, and what is the level of risk associated with the actions (including the sensitivity of the target resource and how they are accessing systems). This approach can make risk determinations in real-time, and more importantly, can automatically trigger mitigation actions that might thwart an attack.

AN AGENT-BASED APPROACH COMPLEMENTS A VAULT BY ENFORCING FINE-GRAINED CONTROLS ON CRITICAL HOST SERVERS

No one wants to contemplate a breach, but Zero Trust adoption demands that we do just this; imagine the unthinkable. For organizations that have only deployed a proxy-based privileged credential vault, they must evaluate the various ways in which this PAM solution can be compromised. There are three possible scenarios:

- Compromised user account – The assumption is that a legitimate user, who has access to privileged accounts and credentials, has their account compromised. Privileged identity analytics are used to address this attack.
- Compromised vault – The assumption is that a hacker has gained access to the encrypted vault. The likelihood of this event occurring is minimal; however, some PAM tools leverage an external database to store privileged credentials. This approach introduces a backdoor administrative account that bypasses all PAM policies and controls to directly retrieve and access the privileged credentials stored within the database. This approach violates Zero Trust principles. Privileged elevation and delegation management tools leverage agents that enforce fine-grained policy controls on protected devices, even if hackers gain access to root or superuser accounts.
- Direct access to servers – Most attacks are performed online, so the proxy-based approach can ensure that hackers must be authenticated and authorized before gaining access to a privileged account or credential. But what happens if the attacker gains direct access to the server? They can access the privileged accounts on that server and completely bypass the vault. In this case, host-based agents serve as the secondary line of defense because they are installed on the servers. They can operate and protect the resources on those servers even if they are isolated from the network.

Proxy-based PAM tools have the ability to limit which commands a user can run while using a privileged account; however, these filters typically only work in certain scenarios while accessing a system through the PAM solution. An agent-based approach can enforce much higher controls across multiple operating systems. The controls are integrated with the kernel, and they can intercept system calls and enforce policies on whether or not to allow those commands to proceed to the kernel for processing. For organizations adopting Zero Trust, they cannot fully enforce least privileged access to system resources without an agent.

Know Your Privileged Users, Know Your Risk

Privileged accounts and access are not only granted to employees with direct, hands-on responsibility for system and network administration. In many cases, privileged accounts are utilized by other applications that access these accounts through secrets.

A secret is simply a piece of data that requires protection and should not be easily discoverable. In the digital world, secrets are authentication credentials that are often embedded within DevOps or IT automation tools. These credentials empower DevOps tools to execute administrative actions, essentially designating the tools as privileged identities. Unfortunately, these credentials often lack sufficient security controls. If compromised, they can grant unrestricted access and permissions to a malicious user, enabling data theft or causing significant damage (as observed in the SolarWinds attack).

SECRETS MANAGEMENT ENABLES SECURE AUTOMATION WITHOUT IMPACTING SPEED

Secrets management safeguards and oversees access to these sensitive credentials. Securely stored within a vault, these secrets are encrypted both at rest and in transit, and remain encrypted during use. Properly implemented policies and best practices help mitigate the risk of theft or unauthorized disclosure. Secrets management is a natural extension of the privileged credential vault and is designed to support automated processes, which involve considerably higher transaction volumes. Moreover, it is not uncommon for organizations to maintain multiple secrets vaults to accommodate various types of secrets, their intended usage, and access policies. The PAM platform needs to be highly scalable to effectively handle this workload.

Conclusion

IT modernization is not an overnight process, yet it will inevitably rely on the ability to automate security policy enforcement for the riskiest identities and detect potential threats stemming from the misuse of privileged identities. Implementing a risk-based approach means ensuring that security controls and analytics can operate in tandem with the modernization journey, effectively enabling automation, scalability, and speed without compromise. This journey necessitates careful planning of a clear roadmap spanning multiple years, anticipating both short-term and long-term requirements from a PAM solution, and ensuring that scope and scale needs are met at a reasonable cost of ownership throughout the entire lifecycle.

Security is paramount, but its scope, scale, and cost should not hinder your digital evolution.

BROADCOM®
connecting everything®

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

PAM-MMITM-WP100 August 28, 2023