TechVision RESEARCH

Privileged Access Management: Developing a Reference Architecture for PAM

Published 13 November 2020

Abstract

A consistent set of well thought out Privileged Access Management (PAM) controls that are aligned with a comprehensive cybersecurity framework is an imperative for most organizations. This enables the automation and enforcement of controls over privileged credentials in any system, platform, or environment. As we've worked with our clients in developing IAM/Security strategies and reference architectures, PAM continues to be a top priority, and this will continue for the foreseeable future.

While most organizations at least claim to have a "least privileged access" strategy, the challenges associated with executing on this strategy are not insignificant. No matter how far along you are (or aren't) in PAM deployment, don't delay developing a Reference Architecture for PAM, which includes documented business and technical requirements, a comprehensive, defensible set of patterns mapped to existing and required capabilities and, ultimately, vendor solutions. By developing this foundation your organization will be able to select the appropriate vendor(s) and deploy the solution that best fits into your IAM environment and with the appropriate security controls. This process is intended to put your organization in the best position to make vendor choices, to determine your deployment priorities and strategy based on a solid requirements and business; not simply responding to vendor marketing programs and promises.

This report provides a solid framework for developing a PAM Reference Architecture. We review common enterprise requirements for PAM, then describe how to build a Reference Architecture for PAM that can fit well within the context of leading vendor offerings/directions in an effort to help you understand how to match vendor solutions to your needs and how to deploy those solutions thoughtfully and effectively.

Authors:

Doug Simmons
Principal Consulting Analyst
dsimmons@techvisionresearch.com

Gary Rowe
CEO/ Principal Consulting Analyst
gary@techvisionresearch.com

Table of Contents

Executive Summary

In reviewing most of the high-profile breaches over the past decade, it is apparent that the ultimate targets for most hackers are the administrative accounts used by systems administrators and administration-centric applications. System administration accounts for Operating Systems like Windows and Linux, network and security devices, cloud platforms, databases such as Oracle and SQL Server, and web servers - as well as privileges embedded within applications to perform administrative functions in application-to-application communications are the top prize for hackers and thieves. These administrative accounts are *privileged accounts*, in that they enable the human or system to configure environments and access the data contained therein. Once a hacker has administrative access to a single server or device, the path often opens to move laterally within the infrastructure to hack deeper and deeper within the enterprise – or beyond.

TechVision Research feels that PAM is one of the more critical elements of an enterprise security posture. Hackers and thieves want your privileged account access rights because that is the way to your data – whether in your data center or in the cloud. No matter how far along you are (or aren't) in PAM deployment, don't delay developing a Reference Architecture for PAM, which includes documented business and technical requirements, a comprehensive, defensible set of patterns mapped to existing and required capabilities and vendor solution capabilities. With these elements all addressed, you will be able to select the appropriate vendor and deploy the solution to fit your IAM environment and address specific information security risks.

A Reference Architecture for PAM is crucial to help identify the areas that require more stringent protection mechanisms for administrative access management.

As we state in this report, Reference Architectures are standardized frameworks that provide a model for a domain, sector, or field of interest. Reference models or architectures provide a common vocabulary, reusable designs and industry best practices. They are not solution designs and as such are not meant to be implemented directly. Rather, they are used to guide more concrete efforts. Typically, a Reference Architecture includes common architecture principles, patterns, building blocks and standards. A Reference Architecture for PAM is crucial to help identify the areas that require more stringent protection mechanisms for administrative access management. Once a Reference Architecture that defines common architecture principles, patterns, building blocks and standards is developed, your organization can better evaluate vendor solutions and their ability to address the critical needs of your organization.

Introduction

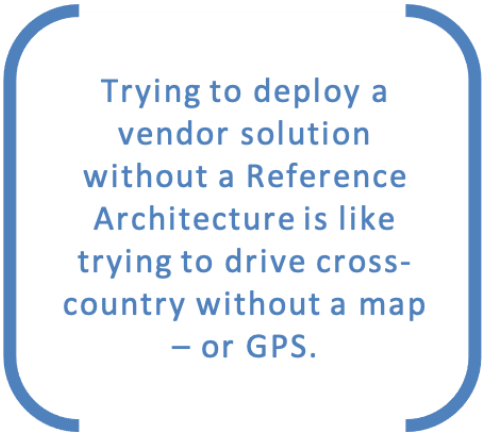
As we described in our report titled "*Privileged Access Management: More Necessary Than Ever as Cloud-Shift Intensifies*", published in July 2019, a consistent set of well thought out Privileged Access Management (PAM) controls that are aligned to a comprehensive cybersecurity framework is an imperative for nearly every organization, enabling the automation and enforcement of controls over privileged credentials in any system, platform, or environment. PAM also identifies all known exceptions that require special control implementation. This is particularly important considering the large number and dynamic nature of resources many organizations are deploying in the cloud, coinciding with requirements to provide on-going support for multi-cloud environments. Most of these cloud environments (e.g., Azure, AWS, Google) have powerful management consoles and APIs that can expand the available attack surface requiring protection and defense.

While most organizations recognize the importance of getting PAM right, the challenges we have seen revolve around where, how and what PAM services to deploy are not insignificant. Most PAM solution vendors have numerous modules that provide privileged management capabilities for specific types of environments, whether in the form of privileged password vaults, various user and administrative interfaces for requesting, approving and monitoring privileged access, session management, policy management, privileged threat analytics and so forth. Often, end user organizations begin deploying PAM solutions and their various modules in a reactive fashion, striving to address what they perceive to be their IT assets that pose the highest risk. This is, of course, valiant and necessary. However, like most IT initiatives, it is extremely advantageous to have a strong Reference Architecture for identity and access management (IAM) in general, as well as for PAM in particular.

That is the objective of this report – to help you develop a viable Reference Architecture for your PAM Program. As we describe in the TechVision report titled "*IAM Reference Architecture*", published in September 2020, we provide guidance for how to develop and use a Reference Architecture to:

- Organize business requirements
- Tie the requirements to capabilities

- Identify strengths and gaps
- Measure progress



As we state in this report, Reference Architectures are standardized frameworks that provide a model for a domain, sector, or field of interest. Reference models or architectures provide a common vocabulary, reusable designs and industry best practices. They are not solution designs and as such are not meant to be implemented directly. Rather, they are used to guide more concrete efforts. Typically, a Reference Architecture includes common architecture principles, patterns, building blocks and standards. A Reference Architecture for PAM is crucial to help identify the areas that require more stringent protection mechanisms for administrative access management. Once a Reference Architecture that defines common architecture principles, patterns, building blocks and standards is developed, your organization can better evaluate vendor solutions and their ability to address the critical needs of your organization. In retrospect, trying to deploy a vendor solution without a Reference Architecture acting as a functional map specific to your organization is like trying to drive cross-country without a map – or GPS.

Before we dig into the specifics of developing a Reference Architecture for PAM, let's quickly review 'what PAM is'.

A Review of the PAM Technology Landscape

Simply put, most current-day PAM solutions take privileged account credentials, such as systems administrator and application service accounts, and put them inside a secure repository typically called a 'vault'. Once inside the vault, system administrators and application service accounts need to go through the PAM system to access the credentials in the vault, at which point they may authenticate to the target system and their access is monitored and logged. When the credential is checked back into the vault, it is reset to ensure administrators must go through the PAM system next time they want to use a credential from the vault. This method of vaulting credentials (or 'secrets') and checking credentials in and out on a real-time, as-needed basis accounts for the majority of PAM approaches today. (There are more capabilities and new approaches, and we'll get to them later.)

Stepping back a bit, we recognize that the first word in the term Privileged Access Management is the word 'privileged'. A privileged account is one that has the ability to perform various types of configuration and operational activities – and these activities can vary quite a bit and can yield devastating consequences to enterprise systems, applications and networks if not tightly controlled. For instance, some privileged accounts, such as Windows Administrator, have more system rights than a 'standard user', as defined by Microsoft Windows. The Administrator type allows complete control, which means that the administrator can change settings globally, install applications, run elevated tasks, and do pretty much anything else on the server or workstation on which he or she

is authenticated.

On the other hand, the 'standard user' account type is more restrictive. Users with this type of account can work with applications, but they are not allowed to install new applications. They can change settings, but only settings that will not affect other accounts. If an application requires elevation of privileges, they will need administrative credentials to complete the task. This simple scenario highlights the 'principle of least privilege', which means "give the administrator or user only the capabilities needed to perform their job". In the case of an end (standard) user as just described, the principle can be somewhat easy to apply – give them next to nothing in terms of admin privileges.

However, when looking at the multiple types of systems administrators – or, SysAdmins, that an enterprise typically has, the granularity required to appropriately affect the principle of least privilege can be quite daunting. What typically occurs, unfortunately, is that sysadmins of all types are granted or acquire over time much more administrative capabilities than they need to perform their day-to-day administrative duties. As a result, when it comes to effectively managing access to important resources and infrastructure, it is critically important to pay special attention to the accounts that have the most privileges, what can be done with those privileges, and who has access to those accounts.

SysAdmins of all types are granted or acquire over time much more administrative capabilities than they need to perform their day-to-day administrative duties.

PAM isn't one monolithic 'thing'. It is a set of capabilities that are focused on the type of administrative functionality being acted upon. Therefore, PAM solutions typically address four primary types of privileged access activities:

1. **System Administrator Privileged Management (SAPM)**, which is focused on SysAdmin system administration, such as Windows Server or Azure Service administration, database administration, etc. The privileges associated with SAPM are usually restricted to administration and configuration services related only to the server, application, database, network device or platform to which the administrative account is associated. In other words, a Windows SysAdmin should only be able to run with administrative privileges on the associated Windows environment – he or she should not be able to use Windows SysAdmin credentials to configure
2. **Privileged Session Management (PSM)**, which involves establishing and monitoring sessions to multiple systems. Authenticating users (e.g., using two-factor authentication) and then providing the users access to shared accounts from which all actions will be monitored.
3. **Application-to-Application Privileged Management (AAPM)** is focused on what are often referred to as 'service accounts' associated with application identities and credentials used for system-to-system communications, such as a web application that interacts

directly with a backend database. Service accounts typically have a username and password that is programmatically sent on the network when connecting to the target system (e.g., the backend database). The passwords associated with service accounts are not often managed in accordance with the Enterprise Password Policy that is focused on end users (i.e., people, including SysAdmins) and are all too often simple passwords, such as "password" that are not even rotated periodically in line with the Policy.

4. **Super User Privileged Management (SUPM)** is focused on "root" accounts (e.g., root is the ***superuser*** on Linux systems). Root / superuser accounts are most often used to make system configuration changes and can override user file protection. These are very powerful, often-human-associated privileged accounts that provide the basis for configuring almost everything deployed in the enterprise IT infrastructure, including in the cloud.
5. With this PAM level-set in mind, we'll now start delving into what it takes to build a Reference Architecture to help your organization make more consistent and better future state architecture, product, service and deployment decisions.

Building a Reference Architecture for PAM

There are some logical steps to follow in order to develop an appropriate Reference Architecture for your organization, namely:

1. Identify and organize your key business requirements
2. Tie the requirements to specific capabilities that are necessary
3. Develop Reference Architecture patterns
4. Socialize the PAM Reference Architecture across your organization
5. Map the PAM Reference Architecture to specific vendors' functional capabilities
6. Begin deployment
7. Measure progress

In subsequent sections of this document, we'll dig into each of these steps in more detail.

About TechVision

World-class research requires world-class consulting analysts, and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skillsets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include:

Identity and Access Management, blockchain, Internet of Things, cloud computing, security/risk management, privacy, innovation, AI, new IT/business models and organizational strategies.

Prior to starting TechVision Research he was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President (now Gartner for Technical Professionals) at Gartner.

Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for 10 years and security, and identity management consulting at Gartner for 5 years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.