

# Privileged Access Management: More Necessary Than Ever as Cloud-Shift Intensifies

Initial Publication Date: 23 July 2019

## Abstract

Breaches, breaches, breaches – will they ever end? Not likely as protecting the enterprise is getting harder and harder. With our IT infrastructure becoming more complicated and porous as cloud-based applications and systems are being blended with legacy systems and emerging technologies the attack surface continues to expand.

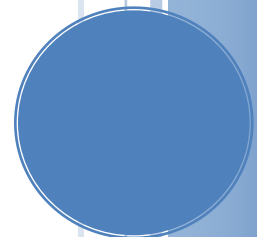
Often, the ultimate targets for most hackers are the administrative accounts used by systems administrators of OS's like Windows and Linux, network and security devices, cloud platforms, databases such as Oracle and SQL Server, and web servers - as well as those embedded within applications to perform various administrative functions in application-to-application communications. To rescue us from administrative account hijacking, solutions residing under the banner of Privileged Access Management (PAM) are available. Such solutions have been on the market for nearly two decades now and have gradually improved to the point where most enterprises will find them compelling. That said, the overall footprint for PAM deployments across many enterprises remains patchy.

This report starts by looking at what PAM is, then evaluates the various types of approaches currently being deployed, the challenges associated with deployment, and provides a review of our short-list of vendors and solutions you should consider. We then conclude with a set of pragmatic recommendations and an enterprise action plan for PAM deployment.

## Authors:

Doug Simmons  
Principal Consulting Analyst  
[dsimmons@techvisionresearch.com](mailto:dsimmons@techvisionresearch.com)

Gary Rowe  
CEO / Principal Consulting Analyst  
[gary@techvisionresearch.com](mailto:gary@techvisionresearch.com)



## Table of Contents

<b>Abstract .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Executive Summary .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>6</b>
<i>Functional Types of PAM .....</i>	<i>7</i>
System Administrator Privileged Management .....	7
Privileged Session Management .....	8
Application-to-Application Privileged Management .....	8
Super User Privileged Management .....	8
<i>PAM from a Historical Perspective .....</i>	<i>8</i>
It's Getting Cloudy .....	9
<i>Future State of PAM .....</i>	<i>10</i>
<b>PAM Deployment Best Practices.....</b>	<b>13</b>
<i>Key Requirements for PAM Deployment .....</i>	<i>13</i>
Discovering Privileged Accounts .....	14
Don't Skimp on Authentication .....	15
<i>Architectural Principles .....</i>	<i>16</i>
<i>TechVision Privileged Access Management Pattern .....</i>	<i>19</i>
<b>Leading PAM Solution Overview .....</b>	<b>23</b>
<i>CyberArk .....</i>	<i>23</i>
<i>Saviynt .....</i>	<i>25</i>
<i>BeyondTrust .....</i>	<i>27</i>
<i>Thycotic .....</i>	<i>29</i>
<i>One Identity .....</i>	<i>30</i>
<i>Micro Focus .....</i>	<i>32</i>
<i>Centrify .....</i>	<i>34</i>
<i>Okta .....</i>	<i>35</i>
<i>Microsoft .....</i>	<i>37</i>
<i>Google .....</i>	<i>38</i>
<i>Amazon .....</i>	<i>38</i>

**Recommendations ..... 39**

**About TechVision ..... 43**

**About the Authors ..... 44**

## Executive Summary

We're all tired of hearing about security breaches and sensitive data theft. But the hackers and thieves are more sophisticated than ever – and it is hard to tell who's the cat and who's the mouse in this never-ending battle. The shifting of our IT infrastructures to Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) commences rapidly, and these cloud-level topologies we deploy create more security risks than many of us can contemplate.

In reviewing most of the high-profile breaches over the past decade or so, it is apparent that the ultimate targets for most hackers are the administrative accounts used by systems administrators and administration-centric applications. Systems 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 those 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.

And the risk associated with privileged access is even greater in that many administrative and service accounts are *shared*. As we gradually move toward Zero Trust principles (described in detail in our Zero Trust Networking report by Sorell Slaymaker) across the enterprise, the fact that privileged access and the resultant actions taken during this access cannot be traced to a specific individual or application service is alarming.

To rescue us from administrative account hijacking, solutions residing under the banner of Privileged Access Management (PAM) are available. Such solutions have been on the market for nearly two decades now and have gradually improved to the point where most enterprises will find them compelling. That said, the overall footprint for PAM deployments across many enterprises remains patchy.

PAM solutions typically address four primary types of privileged access activities:

1. System Administrator Privileged Management (SAPM), which is focused on system administration (SysAdmin), 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 other hosts or environments.
2. Privileged session management (PSM) 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 often not 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 or factory default 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.

Privileged Access Management is sometimes viewed as a subset of the Identity and Access Management (IAM) market but is often deployed as a separate project or program from IAM-centric provisioning, access management, access governance and authentication services. As we discuss in more detail further in this report, the deployment of PAM in typical high-risk IT environments can and should be removed from the critical path of general IAM implementations. In other words, enterprises should not delay PAM deployments while waiting for user provisioning lifecycle processes to be designed/re-designed, codified and implemented. However, the deployment of PAM should *not* be done in a vacuum.

While PAM and IAM deployments may proceed in parallel, there needs to be an intersection at some point in the not-to-distant future in order to establish more comprehensive and auditable capabilities reflecting all identities and access rights – whether end users, system or application administrators or application entities. The key intersection should occur with Identity Governance and Administration (IGA). IGA and PAM are two inter-related technologies because together, they provide one of the most important risk reduction services and enterprise can have. Furthermore, as we begin re-architecting our enterprise environments to incorporate elements of Zero Trust (ZT) security, PAM becomes a critical piece of the ZT puzzle. Within ZT, the endpoint becomes the ‘perimeter’. When an endpoint, such as a systems administrator or application with administrative rights performs high-risk commands, it becomes imperative that these endpoints are managed and audited very carefully. This level of management and audit is what IGA enables, in that IGA policies and processes institute a keen level of awareness and monitoring of ‘who has access to what, for what purposes, for how long and under whose authority?’

So, while we dive deeper into the world of PAM – especially as the unparalleled levels of migration to cloud-based environments continue to escalate (i.e., cloud-shift: SaaS, PaaS, IaaS), we will retain some focus on approaches that engender tighter PAM/IGA integration. At the end of the day, this level of visibility (i.e., monitoring, auditing, etc.) will be necessary to ‘see’ what is happening and react accordingly in the ever-expanding cloud-universe.

## Introduction

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 approaches, and we’ll get to them later.)

Stepping back a bit, 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 he or she is authenticated to.

On the other hand, the ‘standard user’ account type is more restrictive. Users with this type of account can work with applications, but they’re not allowed to install new applications. They can change settings, but only settings that won’t affect other accounts. If an application requires elevation of privileges, they’ll 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. Call it ‘privilege sprawl’, which, much like data sprawl can spiral out of control over the years and becomes increasingly difficult to properly rein in.

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.

A consistent set of well-thought out privileged access management (PAM) controls that are aligned to a comprehensive cybersecurity framework is an imperative, 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 typically deployed in the cloud. Most of these cloud environments (e.g., AWS, Google, Azure) have powerful management consoles and APIs that can expand the available attack surface requiring protection and defense. Therefore, PAM solutions that provide comprehensive automated PAM capabilities are becoming an absolute necessity.

### Functional Types of PAM

PAM isn't one monolithic 'thing'. It is a set of capabilities that are focused on the type of administrative functionality being acted upon. There are typically four functional types of PAM capabilities that constitute complete offerings. They are:

- 1) System Administrator Privileged Management
- 2) Privileged Session Management,
- 3) Application-to-Application Privileged Management
- 4) Super User Privileged Management.

Each functional category is briefly described below.

### System Administrator Privileged Management

System Administrator Privileged Management (SAPM) is centered on managing and rotating passwords and access to them. This is the original PAM formula, which was established nearly two decades ago with CyberArk's vault model. Many products also manage SSL/TLS keys, encryption keys, SSH keys, and/or other confidential data in their vaults. Some products also save password history to handle restoring from backups and continuously monitor the environment for password changes made outside the solution (reconciliation). Access to shared accounts often involves a request and approval workflow. An incontestable audit trail is typically kept of any access to passwords. Sometimes access may be configured to only be possible when there is an outstanding ticket in an IT Service Management (ITSM) system that explicitly requires access. Additional authentication may also be required before access is granted. Some highly critical systems may require an additional person to monitor the session. Break-glass or fire-call functionality may also be supported for emergency access.

*A consistent set of well-thought out privileged access management (PAM) controls that are aligned to a comprehensive cybersecurity framework is an imperative, enabling the automation and enforcement of controls over privileged credentials in any system, platform, or environment*

## Privileged Session Management

Privileged session management (PSM) involves establishing and monitoring sessions for multiple systems. It functions by authenticating users (e.g., using multi-factor authentication) and then providing user access to shared accounts. Shared accounts are potentially very dangerous and PSM attaches an individual user account, such as the user's Active Directory account to a shared administrative account, monitors every action during the subsequent administrative session and removes the association between the user account and the shared account upon completion of the administrative task.

## Application-to-Application Privileged Management

Application-to-Application Privileged management (AAPM) functionality refers to providing applications and scripts access to passwords stored in a password vault. This is basically used to eliminate hard-coded passwords stored in each application. Hard-coded passwords are generally very easy to guess due to minimal password complexity and the fact that they are likely *never* updated.

## Super User Privileged Management

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.

## PAM from a Historical Perspective

Privileged access management tools became de rigueur in the early 2000's, precipitated in large part by the advancement of regulations such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI/DSS), the Health Information Portability and Accountability Act (HIPAA) and similar regulations in light of the 'dawn of the information age'. Regulations such as these armed auditors with specific guidelines for protecting information from theft or misuse. To be sure, the regulatory environment has since exploded over the past several years, most recently with the General Data Protection Regulation (GDPR) and California's Consumer Protection Act (CCPA). These regulations are necessary to protect businesses and consumers from significant cyber threats, and policies and tooling to assist enterprises in marshaling information and network access rights with the level of granularity necessary to succeed is of extreme importance.

A startup company (at the time) named CyberArk Software was one of the first vendors to develop and sell a commercially available PAM solution back in 2003. It may be worth mentioning here that many PAM vendors have come and gone since that time frame, but CyberArk is still in business and going strong. Note that both IBM and Computer Associates (CA) were quick to follow suit in the early 2000s, and they, too remain viable vendors for PAM solutions depending on the enterprise's requirements. In fact, CyberArk's PAM server/Enterprise Password Vault (EPV) ran on IBM WebSphere application servers in the early days.

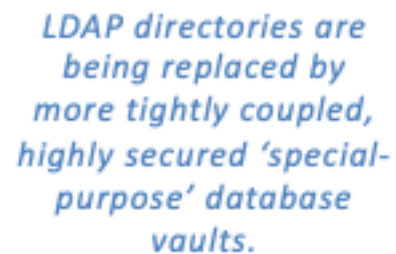


In those ‘early days’, Lightweight Directory Access Protocol (LDAP) directories were seen as the logical place to ‘vault’ credentials. For example, at runtime, the privileged account management system would query the LDAP system to determine the existence of the system administrator, the administrator password and his or her LDAP group membership. The privileged account management system's policy would then bind system administrators to privileged accounts by *LDAP group membership*. This was seen as beneficial because provisioning solutions could (and still can) provision accounts to an LDAP directory without requiring any explicit knowledge about the privileged account management system.

In this way, CyberArk’s EPV PAM solution would make authorization calls to the LDAP server for all system administrator activity. If the system administrator's LDAP group membership changed during his or her employment, his access rights immediately changed. Similarly, if the system administrator's user object is removed from the directory, the system administrator's next attempt to access privileged systems would be denied.

But LDAP directories could only be secured to a point, and other forms of vaulting were desired. This led to the emergence of new technology vendors such as HashiCorp. In 2015, the company released its first version of HashiCorp Vault as a tool for securely accessing ‘secrets’, which it defined as anything that you want to tightly control access to, such as API keys, passwords, or certificates. The HashiCorp Vault provided a unified interface to any secret, while providing tight access control and recording a detailed audit log. In March of 2018, CyberArk acquired Vaultive, in an effort to bring their own vaulting technology into the cloud-first, DevOps mindset.

In essence, LDAP directories are being replaced by more tightly coupled, highly secured ‘special-purpose’ database vaults.



*LDAP directories are being replaced by more tightly coupled, highly secured ‘special-purpose’ database vaults.*

### It’s Getting Cloudy

This advancement of special-purpose, cloud-ready vault technology is better suited to enable automation and continuous integration/continuous development (CI/CD) use cases while enabling policy to codify, protect, and govern access to secrets. The vault can leverage many trusted identity providers, such as cloud IAM platforms, Active Directory, cloud automation platforms such as Kubernetes, and so forth to authenticate into the vault. Identity is abstracted and is scale independent, unlike IP addresses, which require complex firewall rules and frequent updates. Vaulting allows a service to request secrets for any system through a consistent, audited, and secured workflow.

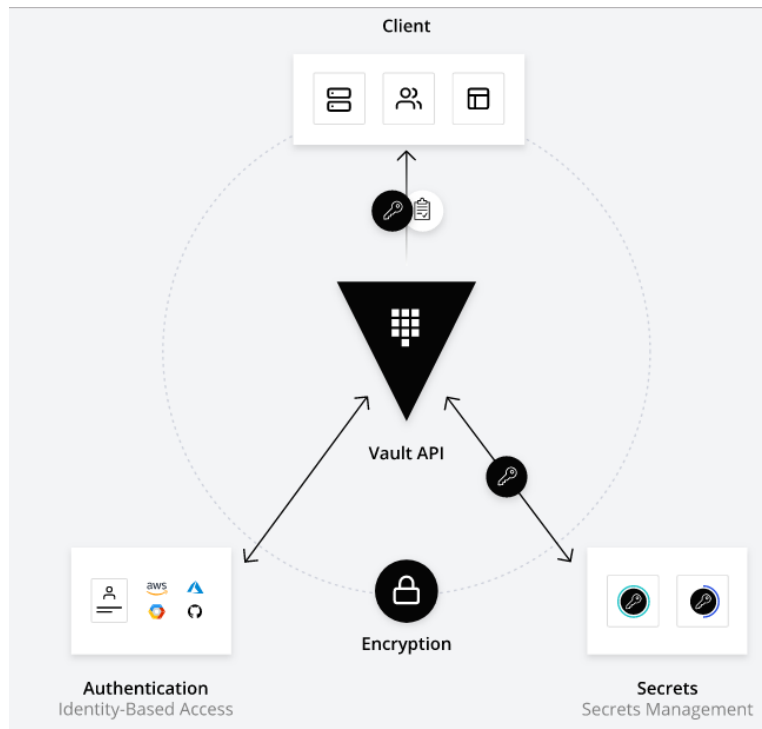


Figure 1: HashiCorp's Vault Solution

With this evolution of the vault model, HashiCorp Vault became the credential vaulting solution behind Amazon's AWS/EC2 IaaS environment, as well as the chosen vaulting solution for emerging PAM vendors such as Saviynt.

Secondly, the early PAM solutions were focusing primarily on human administrators and left a lot of room for further development of application-to-application PAM. This began to change with CyberArk's 2017 acquisition of Conjur, a solution developed to better secure DevOps environments. With Conjur, CyberArk's PAM environment can reach deeper into the DevOps lifecycle to protect secrets and manage machine identities.

For instance, Conjur's Kubernetes integration consists of TLS-connected 'client and server' plugins that adds Kubernetes authentication capabilities. Conjur (with this plugin installed) is on the server-side. The second piece of the integration is a sidecar container that is deployed alongside a user's application. This sidecar container handles the authentication with Conjur on behalf of the application. This sidecar container is the client. Using this type of methodology for cloud service automation extends application-based PAM functionality across enterprise IaaS infrastructures, which is a major step forward to bringing 'service account'-type authentication into the highly monitored world of PAM.

### Future State of PAM

In determining where PAM is going, vendors are increasingly describing their offerings in terms of Just in Time (JIT) PAM. JIT PAM means that system administrators – whether human or application functions, can be assigned privileges in near real time *using their existing, or creating*

*temporary, end-user accounts.* JIT PAM limits the duration for which an account possesses elevated privileges and access rights in that the creation and deletion of an appropriate privileged account is assigned only to meet that specific period's mission objectives. The goal is to eliminate the risk surface of having privileged accounts that are "always on".

In order to make this work, users typically request the access they need via a workflow process – such as ServiceNow or via an existing IAM/IGA workflow process and are quickly granted access or an access privilege level to an application or system. Privileged access may be granted for just a few minutes or several months, depending on the sensitivity level of the application or the organization's governance requirements. In some cases, like developers who compile code, JIT PAM may be

*JIT PAM means that system administrators – whether human or application functions, can be assigned privileges in near real time using their existing, or creating temporary, end-user accounts.*

available all the time but use other methods for privileged elevation in order to avoid the risks of always on accounts. In addition, special approvals and logic checks can be added when access to sensitive applications or systems is requested. When JIT PAM is combined with role-based or attribute-based access control policies (RBAC and ABAC, respectively), organizations can better ensure control and insight over every user's systems access at any point in time. Coupling Multi-factor Authentication (MFA) with JIT PAM processes also adds a significant element of trust that the individuals requesting elevated privileged access are who they say they are, and with added contextual information such as device, geo-location, previous requests/approvals and so forth, an organization can provide better guard against multiple threat vectors.

Here's how JIT PAM can work, as illustrated by BeyondTrust, one of the several vendors that is increasingly focused on this approach:

JIT PAM in Action

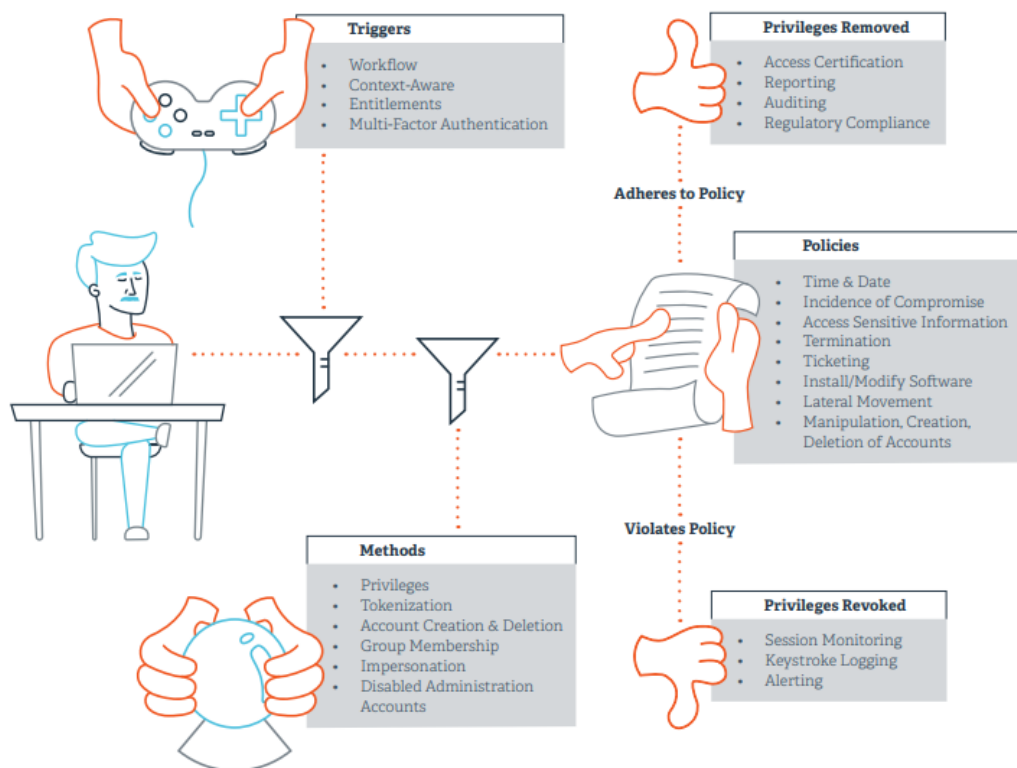


Figure 2: Example JIT PAM Process Diagram

In the JIT PAM process diagram illustrated above (courtesy of BeyondTrust), the journey begins with ‘triggers’ associated with workflow requests taken in context with other information including existing entitlements (e.g., RBAC, ABAC) associated with the user, MFA usage, etc. These triggers act as input to the programmatic ‘methods’ for assigning elevated privileges that include on-the-fly administrator account creation and deletion, assignment to privileged security groups, *impersonation* by means of attaching an existing user account to a privileged account and tokenization of the application to raise privileges on a local system. Policies are applied to the request and the actual session in order to monitor activity and ensure it falls within identified ranges. Once the privileged session is concluded, the entitlements are immediately removed. If administrative actions were attempted that fell outside the associated policies, session recording enables alerting and the escalation of remediation processes.

It bears mentioning that Microsoft is also heavily centered on JIT PAM, referring to it as Just Enough Administration (JEA). In on-premise and Azure-based (cloud) Microsoft environments, PAM is an instance of Privileged Identity Management (PIM) that is implemented using Microsoft Identity Manager (MIM). JEA is a Windows PowerShell toolkit that defines a set of commands for performing privileged activities. In JEA, an administrator decides that users with a certain privilege can perform a certain task. Every time an eligible user needs to perform that task, the administrator enables that permission via MIM workflow. The permissions are ephemeral (expire after a specified time period) so that a malicious user can't steal the access. For example, a MIM

policy can specify that if a specific user requests administrative privileges and is authenticated by MFA, the request is approved and a separate account for the user will be added to the privileged group in a bastion AD forest.

Assuming the request is approved, the MIM workflow communicates directly with the bastion forest Active Directory to put a user in a group. For example, when Joe requests to administer the HR database, the administrative account for Joe is added to the privileged group in the bastion AD forest within seconds. His administrative account's membership in that group will expire after a time limit.

These examples show where vendors and the industry are moving. It is a significant departure from the password vault model in place for the past two decades and affords a more IAM and workflow-integrated approach that may make PAM much easier to deploy at an enterprise-wide level that is increasingly cloud-centric.

## 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



**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.



**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.

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 at Gartner.