CYBER MANAGEMENT ALLIANCE

A SPECIAL REPORT FROM THE CYBER MANAGEMENT ALLIANCE

Securing Your Organization with Cloud-based Privileged Access Management (PAM)

Why read this report?

In 2018, 80% of enterprises were already engaged with one or more cloud vendors. Thus, it's no surprise that in 2019 and beyond businesses will increasingly mandate a cloud-first, digital, growth-ready strategy. By 2022 it's predicted that 28% of spending on Information Technology will shift to the cloud, up from 18% in 2018 .

This relentless drive to the cloud means the organization's default attack surface now includes systems and services outside of the traditional network perimeter with multiple shared owners and ecosystems. The exponential growth of Software-as-a-Service, Microsoft Azure, AWS, hybrid on-premise systems, random micro-cloud service providers have all abetted and magnified the exposure and risk to enterprises.

Compromising a privileged account is a key ingredient of today's successful cyber-attacks and breaches. Our "always on", cloud-interconnectivity only adds to the complexity that produces unnecessary and avoidable risks such as system misconfigurations and granting unnecessary elevated privileges to accounts and users.

The challenge for the security leader is straightforward yet highly challenging. You must allow the business to embrace and expand into the cloud and at the same time manage access to privileged credentials that does not hinder productivity.

The Increasingly Urgent Case for PAM

Cybersecurity can no longer be relegated to a purely IT technology problem. The respected World Economic Forum has consistently placed cybersecurity among their top 10 risks, with cybersecurity ranked number five in terms of likelihood and seven when it comes to impact.

Consequently, business leaders are elevating cybersecurity efforts in their organizations and are prioritizing budgets and other resources to improve their overall cyber-resilience. The rush to reduce cyber-risk, however, can leave organizations vulnerable to both overspend and misspend which can increase their overall risk exposure.

To Manage Risk, You Must Manage Privileged Users and Accounts

There is a common theme that appears when analyzing cyber-attacks and data breaches. When our penetration testers analyzed the step-by-step processes that attacker(s) followed, it became clear that at a very early stage of the assault, the attacker seeks to acquire elevated privileges to persist within the network. Without such privileges, attacks are limited in the damage they can inflict and are more readily contained.

> At a very early stage of a cyber assault, the attacker seeks to acquire elevated privileges to persist within the network. Without such privileges, attacks are limited in the damage they can inflict and are more readily contained.

Two key ingredients required for the success of most cyber-attacks include:

CREDENTIALS	Often referred to as username and password. All things equal, a criminal cannot gain access to systems unless they have the right credentials.
PRIVILEGES	Once criminals gain access, they need sufficiently elevated privileges to take actions such as copying a sensitive file, changing confidential data, or taking down a critical business application or cyber defense system.

The potential damage from a compromised privileged user or account includes, but is not limited to:

Copying, moving, destroying all back-ups of critical files, servers and file-shares.

Creating, deleting, editing users (including privileged) and non-human accounts.

Destroying evidence of all actions by wiping log data.

Destroying or creating backdoors at the core of an enterprise, its Active Directory.

Compromised privileged accounts and users strike at the core of the Confidentiality-Integrity-and Availability (CIA) triad. Below is a sample of data breaches and cyber-attacks that required privileged credentials to succeed, including the attack on the Ukrainian power grid that is recognized as one of the most sophisticated ever.

UK SUPERMARKET CHAIN	One of the top supermarket chains in the UK has had its brand and reputation repeatedly damaged as a result of a disgruntled employee using privileged access to leak the personal information records of 100,000 employees on the Internet. The malicious employee exploited his privileges to copy data without being detected.
ATTACK ON UKRAINE'S ENERGY GRID	Classified as one of the most sophisticated cyber-attacks in recent times, the Ukraine's energy grid physical hardware was targeted, leaving the equipment inoperable and unrecoverable . After using spear phishing emails and maliciously poisoned Microsoft documents to gain access to sensitive infrastructure, the attackers only succeeded when they were able to steal user credentials and then compromise privileged accounts.
EQUIFAX	In the Equifax hack, that exposed personal details of over 170 million users in the US and UK, one of the first things the attacker did, after exploiting an unpatched web server, was to elevate privileges and permissions from the compromised account.

Is there a Silver Bullet for PAM?

Organizations today increasingly recognize that in order to reduce the likelihood of a successful cyber-attack you must deny the criminal access to user-credentials and more importantly, privileged accounts. Denying attackers privileged access into the network provides a critical safeguard against several common threats, including malware and advanced persistent attacks. It is no surprise that managing privileged access and safeguarding credentials are often at the top of the "Major Gaps" in security assessments performed by CM Alliance for clients. Faced with limited budgets and trying to reduce their risk exposure, organizations inevitably ask which one area most deserves their spend and effort. Increasingly, we encourage them to form a Privileged Access Management program and begin partnering with PAM vendors to apply the latest automated technology---including PAM in the Cloud.

Key Takeaways

Transform or Tweak a Cloud PAM Approach: You Decide.

Over the past several years CM-Alliance has observed the evolution of PAM vendors offering a Cloud PAM solution. We categorize these vendors into two approaches distinguished by their architectures: Cloud-Native PAM solutions and Cloud-Ready solutions. The following description of these approaches has been somewhat simplified in an attempt to help a wider audience of both business and IT professionals understand the differences involved.

Cloud-Ready PAM Solutions

are typically hosted in virtual images at cloud platforms, like Microsoft Azure or AWS. These solutions are predominantly deployed in an on-premise data center, but the vendor also offers a "hosted" solution atop a cloud platform, leveraging mechanisms such as the AWS Marketplace. Some vendors may also offer PAM managed services based on a similar architecture.

The drawbacks associated with these options may include, but are not limited to, challenges associated with product maintenance amid upgrade cycles. While this deployment mechanism, including the managed service offerings, may initially sound appealing, we emphasize that these should not be regarded as identical to cloud-native solutions. Relying on a Cloud-Ready PAM solution can be considered more tweaking than transforming your PAM security.

Cloud-Native PAM Solutions

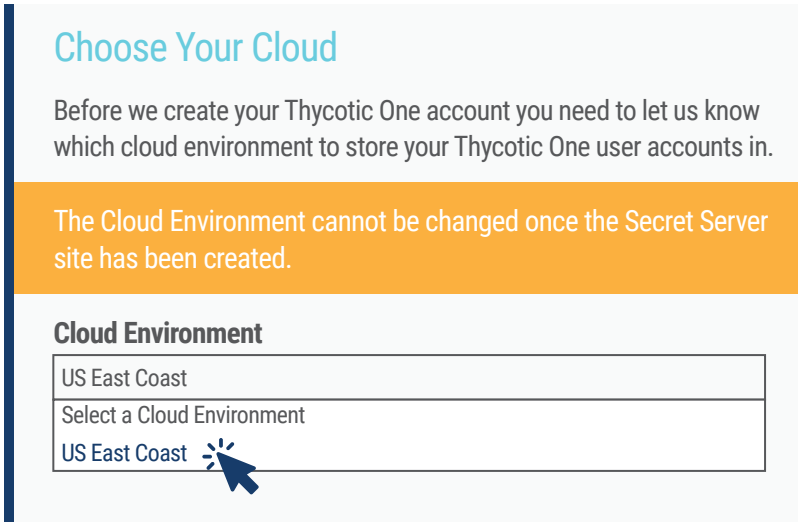
are applications that have been developed for SaaS (Software-as-a-Service) delivery in public or private cloud environments such as Microsoft Azure or AWS. These solutions leverage the scalability and micro-services architectures offered by such public cloud infrastructure vendors. More importantly, they do not require the operational overhead introduced by managed services for administration.

For CM-Alliance, the Cloud-Native approach signals a vendor's commitment towards innovation that truly transforms the protection and management of privileged credentials by fully leveraging the benefits of cloud computing.

Cloud-Native Example:

You have a Microsoft Azure Active Directory running in the cloud and you want to install a PAM solution to manage your privileged users and passwords. Instead of taking a convoluted route as described in the cloud-ready section, all you do is login to a web page, signup, provide a few details of your AD instance and you have a PAM solution that is available to your organization in a matter of minutes or hours.

If an organization wants to genuinely entrench itself in the Cloud and promote Cloud-first as the norm, it must seek out Cloud-Native solution providers where possible. Anything else is a patchwork or a tweak of the current PAM modus-operandi; that of buying a solution, installing hardware and software and devoting resources to maintaining them.



Key Considerations
for a Cloud-Native PAM Approach

Cloud-Native solutions are ideal for those organizations that have a clear Cloud-first strategy. Shown in the table here are several considerations to help you decide if Cloud-Native PAM is the right approach for your business.

CONSIDER CLOUD-NATIVE PAM	ONSITE PAM SHOULD SUFFICE
75% or more of your infrastructure is on IaaS platforms such as Google, Amazon or Azure.	You have some IaaS presence but have no concrete plans to move your current infrastructure to the major Cloud Infrastructure providers.
The majority of your business applications are in the Cloud, such as CRM, HR, Staff Management and Accounting.	Most of your applications are hosted onsite or in a traditional data center.
You plan on moving all or the majority of your Active Directory into Azure Active Directory.	Software as a Service platforms are implemented on an ad hoc basis rather than part of an overall strategy.
You have a hybrid cloud strategy but are concerned about the lack of security and control over access and authentication in the cloud.	You have not established a clear Azure Active Directory strategy

KEY CONSIDERATIONS FOR A CLOUD-NATIVE PAM APPROACH

CONSIDER CLOUD-NATIVE PAM	ONSITE PAM SHOULD SUFFICE
You are using a spreadsheet or other work-arounds to manage general access control to your cloud-based applications and services.	You have a working and integrated access and authorization work-flow with your current onsite PAM solution and your cloud-based applications and services.
You are using a spreadsheet or other work-arounds to manage privileged access control to your cloud-based applications and services.	You have a working and integrated privileged access and authorization work-flow with your current onsite PAM solution and cloud-based applications and services.
You have only limited funding and resources to manage the infrastructure of your existing PAM solution.	You have the funding and bandwidth for the skilled resources and the infrastructure to maintain and run your current PAM solution.

Evaluating a Cloud-Native PAM solution

For this report, we were invited to review Thycotic's PAM approach, their strategy for developing cloud-native technologies and their readiness in delivering Cloud-Native PAM solutions for organizations of varying sizes. We were given open access to their senior executives, their roadmap and access to their product management team. We carried out a bounded analysis of similar vendors offering PAM in the Cloud services, including CyberArk and Beyond Trust.

Many existing vendors deliver Cloud-Native PAM applications, including a host of recent market entrants pitching their solutions to smaller businesses. However, there are only a select few whose Cloud-Native solutions scale and operate at effectiveness levels demanded by Fortune 100 organizations. Based on our review, we recognize several advantages that Thycotic's Cloud-Native PAM offers:

Thycotic's intense commitment from the senior executives to its developers, firmly establishes the company as a Cloud-First organization deploying Cloud-Native technologies that organizations of all sizes can deploy.

Free from the fear of takeovers and unburdened by recent market volatility that resulted in consolidation of some leading PAM vendors, Thycotic appears to be distraction-free and able to deliver on a Cloud-First roadmap designed to penetrate markets that have been underserved by most PAM vendors.

Thycotic continues to focus on ensuring their PAM solutions are user friendly and easy to manage yet deliver powerful capabilities to solve PAM-related and cloud-specific challenges associated with cloud infrastructures and SaaS applications. Destroying or creating backdoors at the core of an enterprise, its Active Directory.

As part of the Thycotic evaluation, CM-Alliance's researchers tapped into our global network of cyber executives and experts.

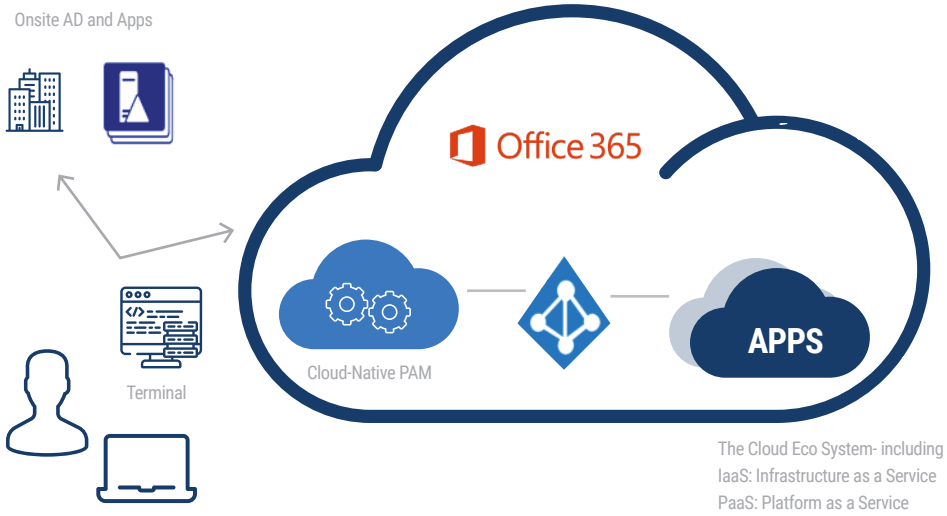
PAM in the Cloud Recommendations

The CM Alliance 2018 Leaderboard report, titled "Privilege Access Management Vendor Evaluation" focused on the established on-premise PAM vendor landscape. It offered insights into key requirements for an effective and secure PAM solution while gauging the capabilities of several leading PAM vendors.

In our report we defined Privileged Access Management (PAM) broadly as a set of controls that allow organizations to manage risks associated with privileged accounts. A privileged account is an account that has administrative or full-system permissions on a system. Traditional on-premise PAM delivers on a broad range of requirements.

NOTE: A word of caution to buyers: When it comes to session-management in the cloud, there is dependency on the application or service provider to step-up and collaborate fully, for example, by providing suitable APIs.

FIG. 1
The diagram below provides a simplistic, light-touch view of what a PAM in the cloud solution would look like.



The Cloud Eco System- including
IaaS: Infrastructure as a Service
PaaS: Platform as a Service
Software asa Service

When considering Cloud-Native PAM, we recommend our clients evaluate PAM solutions that, demonstrate strong capabilities in the following areas, asking critical questions:

CLOUD-NATIVE	Is the PAM product from a leading public cloud infrastructure? What is the vendor's mid-to-long-term roadmap for delivering access controls to secure privileged entry points to cloud platforms and applications?
AUTHENTICATION IN THE CLOUD	Can an organization easily connect their Azure AD in the Cloud to the PAM solution, and can the they manage their on-premise AD with the same solution?
PASSWORD VAULTING	Is the Cloud-Native PAM capable of managing passwords or secrets (password vault) and can you manage the secrets to your PaaS & IaaS using the Cloud-Native PAM (AWS, GCP, Azure)?
ANALYTICS	Does the vendor provide advanced analytics, preferably with a focus on machine learning and not simply static "if-then" rules, to monitor, understand, and alert on suspicious user activity?
SESSION MANAGEMENT	Can the solution carry out the basics of the credential brokering (also called PASM or Privileged Account Session Management) that allows users to securely connect to remote servers[4]?

This list is not a comprehensive list of PAM in the Cloud requirements nor does it mean that the reader should ignore traditional onsite-PAM features. However, we advise our clients to steer away from the feature-list approach encouraged by most sales and marketing departments and instead focus on these core PAM in the Cloud capabilities. For this report, our focus has been to assess the current and future roadmap and the existing Cloud features of the PAM vendor, Thycotic.

PAM in the Cloud Vendor Selection Guidelines

As with any selection process, customers have a wide array of choices when selecting a PAM vendor. It is also tempting to allow vendors to shape buying requirements with PAM by requiring the supposed-necessity of hundreds of features, few of which are actually deployed or utilized in production. When considering a PAM vendor, ask yourself and seek evidence that a particular feature can address a large portion of your estate rather than obsessing about a feature that would be an ideal-to-have but does not impact the majority of your digital estate.

Here are some examples:

Discovering Privileged Accounts

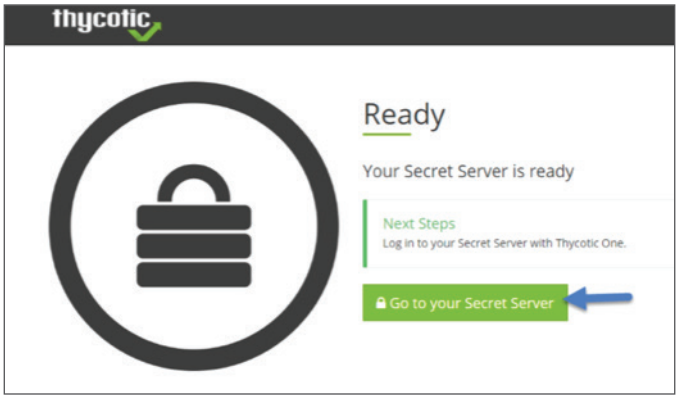
In our opinion, Thycotic's approach to discovery suits a large majority of organizations and scenarios. Thycotic solutions are able to discover new assets on a continuous basis through network and AD scanning. Furthermore, it can detect accounts on UNIX/Linux and Windows systems, Microsoft SQL Server, Oracle, and Sybase, VMware and ESXi.

Finally, where applicable and required, you can create custom-scripts for further discovery. This discovery feature is available in Thycotic's Secret Server Cloud offering. Thycotic also offers a free privileged account discovery tool for Windows and Unix.

Note: Discovery is a critical, foundational requirement. You cannot protect what you cannot see. The same logic applies with privileged accounts. In our experience there are anywhere between 3 – 6 hidden or undiscovered accounts for every known account on servers and this figure is larger if you consider the number of unmanaged privileged accounts on endpoint devices. Continuous discovery of privileged and service accounts must be a foundational requirement in any PAM project.

Ease of Administration must be a priority

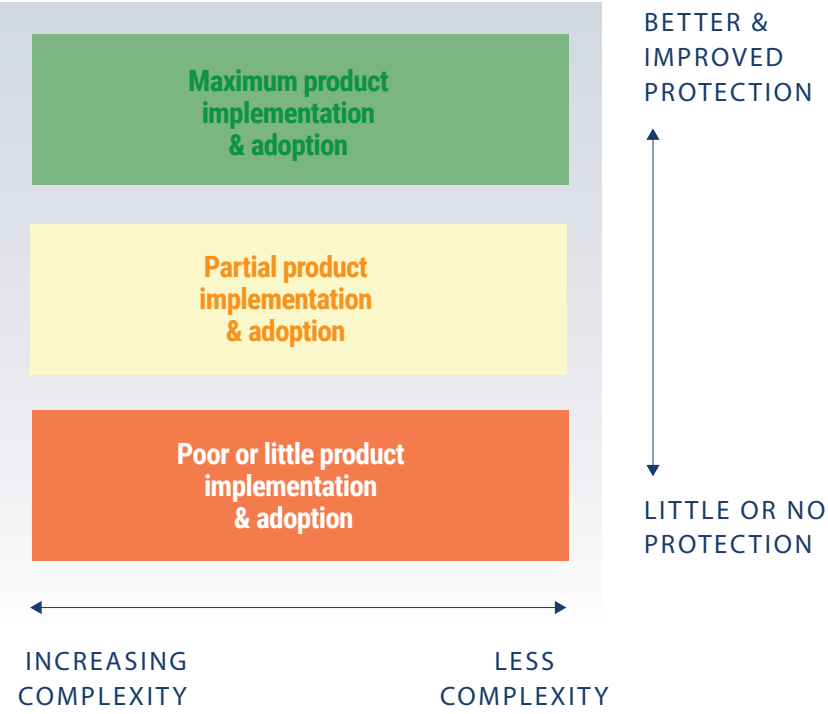
In our 2018 PAM vendor evaluation, we focused on ease-of-use as a key ingredient and we still stand by this as one of key requirements when selecting any product, let alone PAM. A solution may have hundreds of features and solve all types of problems but if the operations teams---the folks that run the day-to-day operations--- are unable to quickly learn and use all its features without extensive training or professional services, the solution is DOA or dead-on-arrival and will sooner or later be delegated as shelfware.



For an organization to be cyber-resilient it cannot rely solely on the traditional "we have policies" and tick-box governance for compliance. A robust and secure business must strive to achieve maximum product implementation and adoption of a solution within its operations.

FIG. 2

The relationship between little, partial and maximum product implementation and adoption and how this relates to an organization's overall security protection.



Consider a scenario where Security Admins typically mandate that users "check out" a password stored in a vault---especially if it's a shared password. If the password is not rotated upon "check in" (which can easily happen), the password is still vulnerable since the user may have written it on a sticky note to avoid having to get the password when logging back into the vault later. With an automated PAM solution, a launcher can "mask" the password, and the user has only to click a launcher icon with authentication occurring in the background.

Time-to-value is a critical factor here. Consequently, organizations should look to solutions where the operator does not have to attend a five-day training course to use the product. Rather you should opt for products that provide an intuitive user experience that makes the process of leveraging privileged secrets and managing privileged users easy and readily adopted. As noted in our 2018 PAM report:

> "Over-complicated solutions often become so cumbersome that operational teams are unable to configure, optimize and run the tools effectively. This circle of confusion leads to a downward spiral of lower product-utilization and as a result, teams are unable to deliver on the overall organizational task of keeping the business secure and resilient".

Thycotic shares our ethos and appears to maintain their focus on the user friendliness and easy-to-operate aspect in their Cloud-Native products such as Secret Server Cloud and Privilege Manager Cloud.

Thycotic the CM Alliance Leader for PAM in the Cloud

In summarizing our research, CM-Alliance has produced the PAM in the Cloud Leaderboard shown below.

Thycotic is the clear leader with a Cloud-Native PAM solution that can be implemented today and that features discovery, vaulting, monitoring and control capabilities on par with its flagship on-premise offerings. This includes Cloud-Native SaaS with Secret Server Cloud privileged access management and Privilege Manager Cloud to enforce least privilege with application control.

With the acquisition of Lieberman, Avecto and BeyondTrust in 2018 by Bomgar, and going forward under the BeyondTrust brand, CM-Alliance believes that the combined entity is on a path to a Cloud-Native strategy. But it's unclear at this point how managing so many mergers might impact its progress, or possibly impede it in developing a Cloud-Native PAM solution.

Given its market presence and typical reliance on professional services for PAM implementations, CyberArk is certainly a contender but today it's PAM Cloud strategy focuses primarily on offering managed services. That approach, although a viable solution for some, may not be a practical or affordable option for many enterprises.

THE LEADER: THYCOTIC	Uncomplicated Cloud-first strategy with a viable Cloud-Native PAM offering. Less internal upheaval means it can focus on product development and customer requirements. Being agile, gives it flexibility compared with more established vendors.
THE RUNNER-UP: BEYONDTRUST	Actively considering Cloud-native strategy and appears to have a steady pace. Comprehensive onsite offering coupled with recent mergers and buyouts could slow product integration and development.
THE CONTENDER: CYBER ARK	Offers a managed service in the Cloud compared to a SaaS instance. Albeit feature-rich but clunky and less operationally friendly compared to the leader and runner-up.

At Cyber Management Alliance Ltd we believe that honesty and integrity are key pillars on which to build a business. We did not include many vendors in this assessment simply because they do not stack up in their PAM in the Cloud capabilities around SaaS offerings.

About CM Alliance

Experienced thought leaders and GCHQ-accredited cyber security training providers, Cyber Management Alliance are the creators of the internationally-acclaimed GCHQ Certified Cyber Security and Privacy Essentials and the GCHQ Certified Cyber Incident Planning and Response training courses. In addition, we provide informative and well-rounded courses in CISSP, Information Security Awareness, the Anatomy of a Network Attack and SAP Compliance, Security and Audit Essentials.

Specialist event practitioners and consultants. We deliver the highest level of specialized operational and strategic cyber security training courses, educational webinars, and an informative series of executive interviews with highly regarded industry professionals, innovative live and virtual events, bringing about the collaboration and sharing of information worldwide.

Our new Insights with Cyber Leaders video interview series together with our educational webinars are highly popular and have provided a wealth of knowledge and information sharing among security professionals.

Cyber Management Alliance truly unites the global community of CISOs and security professionals to achieve joint strategic goals of reducing organizational exposure to cyber threats.