CYBER MANAGEMENT ALLIANCE

THE CM-ALLIANCE LEADERBOARD:

Privilege Access Management Vendor Evaluation

INTRODUCING THE PAM VENDOR LEADERBOARD
IN THE PRIVILEGED ACCESS MANAGEMENT (PAM) MARKET

Why read this report?

The myriad offerings in the privileged identity management marketplace may easily confuse those looking for an effective solution. To further confound the selection process, most vendors, with a dedicated perseverance, focus solely on features and buzz words to attract attention. This report has researched and analyzed prominent providers of Privileged Access Management (PAM) solutions based on select criteria and discussions with customers and product distributors.

> We have classified the top PAM vendors as The Leader, The Runner-Up and The Contender.

Our goal is to help cybersecurity and risk professionals cut through the clutter in order to make more informed decisions about what is best for their organizations.

The PAM Solution Leaderboard

THE LEADER:
THYCOTIC

Thycotic is our overall favorite solution, earning the top spot on our Leaderboard.

Thycotic is our overall favorite solution and earns CM-Alliance's Leader honor. Despite its rapid growth, the company operates in an agile almost start-up like mindset when it comes to product strategy, development and execution.

> Our researchers were impressed with the enterprise class capabilities of scalability, flexibility and adaptability in one of the industry's easiest to use and deploy products.

The ability for existing staff resources to tweak and optimize the product offers significant cost benefits since Thycotic PAM solutions require little to no professional services for light-weight installations.

Additionally, we find their product management team deeply passionate and importantly, open to constructive criticism.

CyberArk Results

THE RUNNER-UP:
CYBERARK

CyberArk, the granddaddy of the PAM market, continues to push on advanced enterprise-focused features and is still considered a strong contender. In the past, CyberArk was the benchmark against which other vendor assess themselves.

> Typically a product only very large organizations use, CyberArk does tend to lose out to competitors on price.

Arcon Results

THE CONTENDER:
ARCON

The lesser known Arcon captures the Contender category on our Leaderboard. It has been around for several years and continues to gain a strong customer base in Asia and the Middle East.

The Leaderboard

WHAT WE LIKED

THE LEADER: THYCOTIC	• Outstandingly operationally friendly • Comprehensive enterprise-class features • Deeply passionate product team and executive leadership • Innovation packed roadmap
THE RUNNER-UP: CYBERARK	• Large user base and early market leader • Extensive feature set to meet complex requirements • Remains less user friendly and more costly
THE CONTENDER: ARCON	• Feature rich and value for money • Remains low profile in the west • Little assurance on development security

> 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 features, their user-centric approach and their overall direction.

Key Takeaways

ENTERPRISE-CLASS CAPABILITIES

What we liked most about Thycotic–despite being one of the easiest solutions to use and deploy–it delivers meaningful enterprise-class capabilities.

Simplicity & Ease-of-Use Take Priority

Ease-of-use is a key ingredient to operational adoption of a PAM solution. 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 task of "keeping the business secure and resilient."

During our analysis of vendors including CyberArk, Thycotic, Arcon, and BeyondTrust, CM-Alliance's researchers spoke to PAM experts about why they chose one product over another. The common theme among Thycotic's customers was the overall simplicity with which they could implement and maintain the product. What we liked most about Thycotic—despite being one of the easiest solutions to use and deploy—it delivers meaningful enterprise-class capabilities.

> While CyberArk is enterprise-established, with multiple features in many areas, it remains the most complex solution of those researched.

Operationally Friendly is Critical to a Secure Organisation

GDPR requirements and compliance with other industry regulations could be a primary driver of the continued growth in the PAM marketplace.

Unfortunately, continued growth in a sector does not directly correlate with a decrease in cyber-attacks. To the contrary, CM-Alliance's experience suggest that tier-1 business-impacting products are only truly effective when the operational teams—the people that have to use the product on a daily basis:

1. A very short or zero learning curve
2. Easy-to-use features and functionalities
3. Solutions can be configured, optimized and fine-tuned by the customer with little or no professional services input

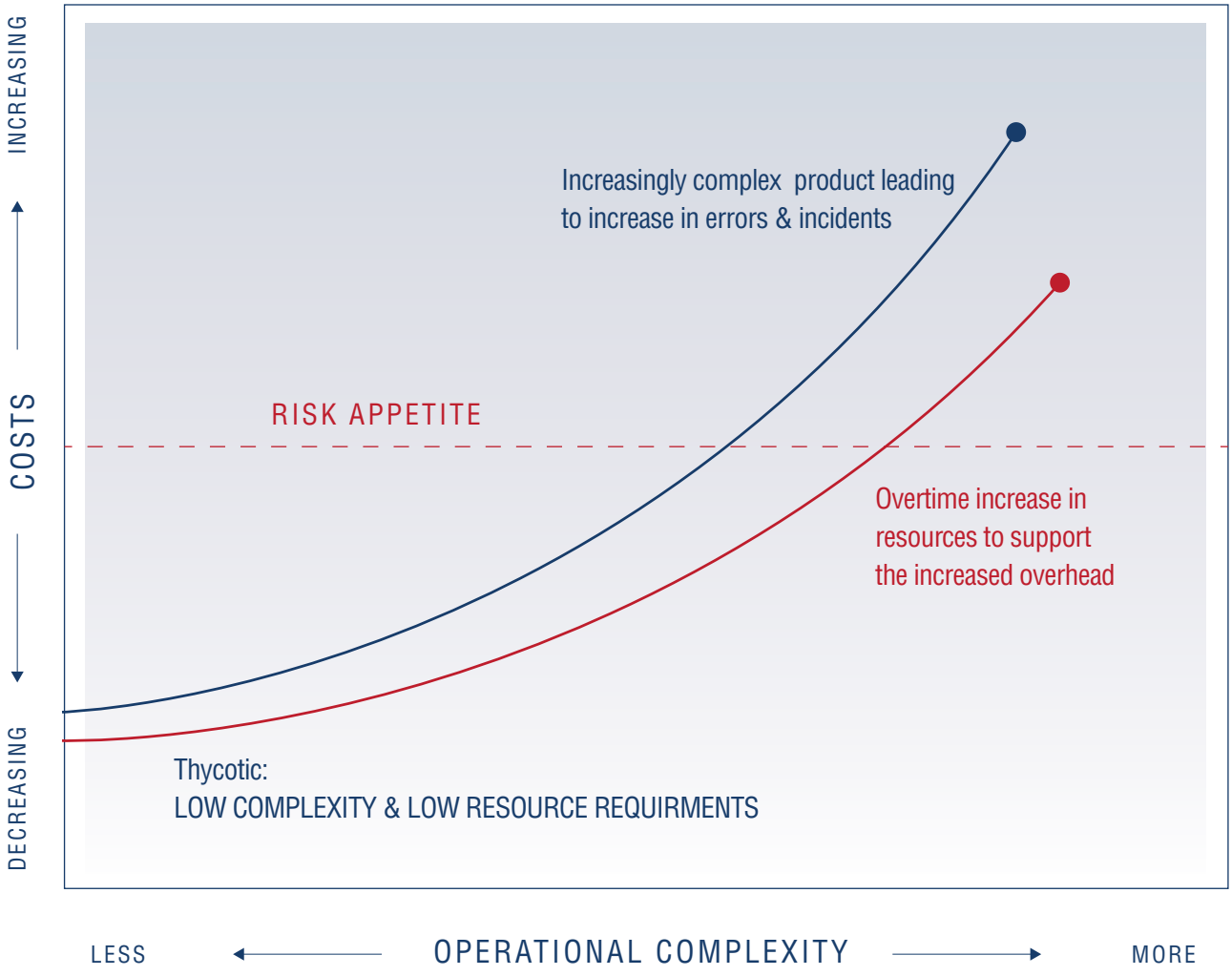
An effective PAM solution, despite a growing set of complex features, must above all, be easy to operate, configure, optimize and tune by the team that is charged with its daily interaction.

ESSENTIAL
EASE OF USE

An effective PAM solution, despite a growing set of complex features, must above all be easy to operate, configure, optimize and tune by the team that is charged with its daily interaction.

FIG. 1

Minimizing complexity in PAM products can help avoid increased incidents and errors as well keeping overhead costs under control.

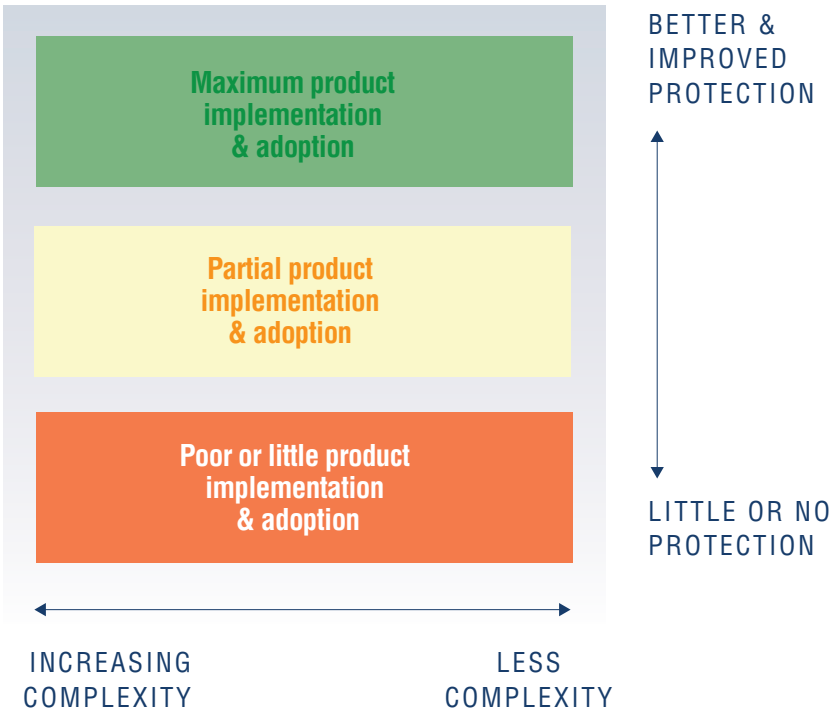


It's More About Implementation Than Features

For an organization to have true and effective cyber resilience it cannot rely solely on the traditional "we have policies" and tick-box governance and compliance. For a business to be robust and secure it 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.



Timely Detection of Unauthorized Privilege Escalation and Contextual Behavior Analytics is a Must

Scalability in a PAM solution, though important, takes second place to PAM simplicity and ease-of-use. In most breaches, an attacker needs elevated access to carry out specific actions on a system. This is achieved by exploiting known or unknown weaknesses and is known as privilege escalation. A worthy PAM solution must provide a robust privilege escalation product able to swiftly detect the early signs of a major cyber attack.

Another key, early-warning compromise indicator comes from detecting abnormal user behavior in privileged account access. Solutions designed to deliver these insights are commonly referred to as User Behavior Analytics (UBA) or User and Entity Behavior Analytics (UEBA). A PAM solution must be able to offer robust, easy to use and contextual analytics of a range of user actions to provide meaningful early warning alerts.

MACHINE LEARNING (ML) & ARTIFICIAL INTELLIGENCE (AI) HYPERBOLE NOTED

Rather than focus on the over-hyped labels of machine learning (ML) or artificial intelligence (AI), we appreciate those vendors who employ data scientists to build a strong foundation in these algorithmic technologies.

SWIFT DETECTION AND ESCALATION

A worthy PAM solution must provide a robust privilege escalation product able to swiftly detect the early signs of a major cyber attack.

90% of Cyber-Attacks Require Enhanced Privilege to Succeed

Without doubt, the privileged account user in today's IT environment needs an enhanced breadth and depth of access and a considerable amount of freedom in making both planned and unplanned changes. However, with this liberty comes the peril of accidental or malicious actions that can have significant business impacts.

> A privileged user's potential for damage 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.

Studying the anatomy of successful cyber-attacks, including the recent, publicly acknowledged, advanced attack on Ukraine's Energy Grid, reveals that this highly complicated breach, carried out by deeply sophisticated attackers, was only successful after they were able to compromise, use and escalate user privileges.

Who Has Access to What?

This may appear to be a simple question, but most organizations are not able to contemplate the urgency and importance of this ask. Given that access is the key requirement for a successful persistent attack, an organization's must focus not just on the typical feature-set of a PAM solution but also how efficiently and continuously it can discover new assets and new accounts.

PAM is Not Only for Servers

The traditional notion that privileged management products apply only to the server infrastructure was often reinforced when PAM products only focused on servers. This meant two things:

First, the business had to procure another system to manage privileged abuse at the desktop/laptop device.

Second, and equally importantly, operational teams had to learn another interface and understand another dashboard in order to manage and configure the solution effectively.

However, in the last few years, top PAM vendors have made a number of acquisitions that include privilege-escalation endpoint management products in their portfolio.

Define Normal to Observe Abnormal

A key requirement of recent regulations such as GDPR and other breach notification laws is the timely detection of an attack. As a result, organizations can no longer wait for the daily newspaper to inform them of a data breach. An effective strategy for detecting the early signs of "something fishy" or anomalous behavior, should be to monitor the user and his/her behavior and actions across the network. This approach also applies to observing and baselining the behavior patterns of non-human accounts (think service accounts) to help detect compromise by a threat actor.

The premise of early detection of anomalous behavior is simple. Build a continuous baseline, over time, and detect deviations from the norm.

A respectable solution must also be able to identify fast and slow attacks:

> A fast attack occurs when the attacker simply takes one simple action away from the normal pattern to launch an attack. See Figure 3, on next page.
>
> A slow attack exhibits the qualities of a more patient and possibly smarter attacker, seeking to blend in and become part of the "normal" user activity. See Figure 4, on next page.

BUILD A BASELINE

The premise of early detection of anomalous behavior is simple. Build a continuous baseline, over time, and detect deviations from the norm.

The two kinds of attacks are illustrated in the diagrams shown here.

FIG. 3 LARGE SPIKE: POTENTIAL FAST ATTACK

FIG. 4 POTENTIAL LOW-AND-SLOW ATTACK

Sharing Credentials:
The Dark Art of Saving Money

If there is one practice that disheartens and enrages compliance auditors, it is the sharing of access credentials, i.e. sharing credentials assigned to a single user among two or more users. Often, the business justification of this ill advised practice is to save money, since many new and modern companies model their IT pricing structure on the number procured of privileged licenses.

Apart from the high likelihood of failing an audit, password sharing comes with an alarming set of risks that can be mitigated by:

> Maintaining an accurate audit log of when, where and for how long users are using the shared credentials.
>
> Monitoring the shared credentials to identify anomalous increased user activity
>
> Attribution or correctly identifying the user account responsible for a particular action.

ESSENTIAL CLOUD OFFERING

PAM providers must extend their traditional controls and management capabilities to enable the effective administration of this type of privileged user.

The Cloud and Privileges: The Complicated Privileged User

In most, if not all cases, efficiencies and costs savings are the biggest drivers in the ever-growing cloud dependence for infrastructure and software as a service. This efficiency led migration to the cloud, being led by business of all sizes, generates a corresponding demand from PAM vendors to deliver a cloud-native and easy to deploy solution that is both scalable and feature rich.

Additionally, the cloud introduces what we like to call the software-as-a-service-administrator or SaaS-Admin, an administrator that is often overlooked and unmanaged. Equally importantly, PAM providers must extend their traditional controls and management capabilities to enable the effective administration of this type of privileged user.

PAM Vendor Evaluation Criteria

To assess the state of the privileged identity management market and see how the vendors stack up against each other, Cyber Management Alliance Ltd evaluated the strengths and weaknesses of top providers. We spoke to customers and resellers of PAM products, analyzed user requirements and queried vendors and identity experts before developing a comprehensive set of evaluation criteria.

> We evaluated vendors against the criteria shown in the chart here, grouped into high-level categories:
>
> **IMPLEMENT & OPERATE, PRESENT OFFERING, INNOVATION & DEVELOPMENT**

IMPLEMENT & OPERATE

OPERATIONALLY FRIENDLY	Overall, the offering is easy to understand and run for operations teams.
OPERATIONAL MANAGEMENT	Straightforward lifecycle management of users, roles, integration with support tools and their respective roles.
MODERN UX & INTUITIVE INTERFACE	An easy-to-use, modern, intuitive interface makes it easier to for operation teams to understand and use, with little need to rely on training.
LITTLE TO ZERO LEARNING CURVE	A good solution must relinquish complexity and instead offer a zero learning curve approach that enables an organization to be an up running in a short period of time (See below: Time to Value).
INSTALL & IMPLEMENT	This looks at how easy is the product to deploy and implement across a business. A suitably configured and correctly implemented product can make a significant impact on the overall security posture of an organisation.
TIME TO VALUE	The timely derivation of product value and benefit from procurement to operations.

PRESENT OFFERING

BEHAVIOR ANOMALY DETECTION & RESPONSE	The ability to detect anomalous behaviour based on machine learning or otherwise coupled with the ability to respond, both passively, in terms of "monitor this suspicious behavior" or actively, in terms of "force additional controls, challenge with additional authentication."
CLOUD-ENABLED	Is the solution deployable on any of the top cloud platforms, Azure, AWS or Google Cloud?
ZERO TO LITTLE RELIANCE ON PROFESSIONAL SERVICES	To the financial detriment of businesses, several vendors and their resellers rely on the complexity of the solution to increase revenue by charging, often exorbitant amounts, for configuration changes, installation, implementation and integration.
DevSecOps API INTEGRATION	The ability of a solution to incorporate into the DevSecOps lifecycle easy to use application-to-application password management.
MANAGEMENT & TECHNICAL REPORTING	A robust framework for generating detailed reporting for both management and technical resources.
PRIVILEGE ESCALATION & DELEGATION	The ability of a solution to constantly manage and maintain the "Least Privilege Model" on endpoints (desktops/ laptops).
PRIVILEGED SESSION MANAGEMENT & RECORDING	Recording both visual (Windows) and Unix (example SSH) sessions and offering contextual searching and playback of those sessions.
ROBUST DISCOVERY & REMEDIATION	Managing the unknown unknowns through constant discovery and having robust remediation controls.

INNOVATION & DEVELOPMENT

INVESTMENT IN PEOPLE	Without good passionate people it's difficult to innovate or maintain innovative products.
INVESTMENT & FOCUS ON USER EXPERIENCE	How much is the company focusing on the user experience? A feature rich product with little focus on how the end-user will use the product is in our opinion a security risk since most of the features may never be configured or even worse, be wrongly configured.
INNOVATION ROADMAP	Is the organisation committed to constant and ongoing innovation and improvements across their product portfolio?
CUSTOMER SATISFACTION & FEEDBACK	How satisfied are the end users of the product and solution?
PRODUCT MANAGEMENT DIRECTION & STRATEGY	Are the product management teams passionate and communicative and able to passionately talk and discuss about the product?
MANAGEMENT TEAM	How determined, focused and importantly, committed is the management team about the product and the company?

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 specialised 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 organisational exposure to cyber threats.