KuppingerCole Report

LEADERSHIP COMPASS

By Paul Fisher

May 07, 2020

# Privileged Access Management

Privileged Access Management (PAM) is one of the most important areas of risk management and security in any organization. Privileged accounts have traditionally been given to administrators to access critical data and applications. But, changing business practices, hybrid IT, cloud and other aspects of digital transformation has meant that users of privileged accounts have become more numerous and widespread. To reduce the risk of privileged accounts being hijacked or fraudulently used, and to uphold stringent regulatory compliance within an organization, a strong PAM solution is essential.

By **Paul Fisher**
pf@kuppingercole.com

# Content

# 1 Introduction

This report is an overview of the market for Privilege Access Management (PAM) solutions and provides a compass to help buyers find the solution that best meets their needs. KuppingerCole examines the market segment, vendor functionality, relative market share, and innovative approaches to providing PAM solutions.

## 1.1 Market segment

Privileged Access Management (PAM) solutions are critical cybersecurity controls that address the security risks associated with the use of privileged access in organizations and companies. Traditionally, there have been primarily two types of privileged users.

Privileged IT users are those who need access to the IT infrastructure supporting the business. Such permissions are usually granted to IT admins who need access to system accounts, software accounts or operational accounts. These are often referred to as superusers.

There are now also privileged business users, those who need access to sensitive data and information assets such as HR records, payroll details, financial information or intellectual property, and social media accounts.

The picture has become more complicated with many more of these non-traditional users requiring and getting privileged access to IT and business data. Some will be employees working on special projects, others may be developers building applications or third-party contractual workers. With the onset of digital transformation, organizations have seen the number of privileged users multiply as new types of operations such as DevOps have needed access to privileged accounts.

In recent years, Privileged Access Management (PAM) has become one of the fastest growing areas of cyber security and risk management solutions. KuppingerCole estimates that the number of major vendors in the space is around 40 with a combined annual revenue of around $2.2bnm per annum, predicted to grow to $5.4bnby 2025 (see Figure 2).
That growth has largely been driven by changes in business computing practices and compliance demands from governments and trading bodies, as well as increased levels of cybercrime. Digital transformation, regulations such as GDPR, the shift to the cloud and, most recently, the growth of DevOps in organizations looking to accelerate their application development processes are all adding to the growth.

The reason for this mini boom is that all these trends have triggered an explosion in data and services designated as business critical or confidential and a concurrent rise in the number of users and applications that need to access them. IT administrators realised that without dedicated

solutions to manage all these, the organizations would be at great risk of hacks and security breaches. Hackers and cyber criminals have long targeted unprotected privileged accounts as one of the easiest routes to get inside an organization.

In recent years, PAM solutions have become more sophisticated making them robust security management tools in themselves. While credential vaulting, password rotation, controlled elevation and delegation of privileges, session establishment and activity monitoring are now almost standard features, more advanced capabilities such as privileged user analytics, risk-based session monitoring, advanced threat protection, and the ability to embrace PAM scenarios in an enterprise governance program are becoming the new standard to protect against today's threats. Many vendors are integrating these features into comprehensive PAM suites while a new generation of providers are targeting niche areas of Privileged Access Management.


Figure 1: The PAM market is seeing dynamic growth as vendors seek to add better functionality to meet security challenges and more players enter the market.

With the attack surface expanding and the number of attacks increasing every year, an integrated and more comprehensive PAM solution is required – one that can automatically detect unusual behavior and initiate automated mitigations. A successful attack can be conducted in minutes; therefore, a PAM solution must be capable of thwarting this attack without human intervention. Although we see more comprehensive PAM suites and solutions being offered, vendors are taking different approaches to solve the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts. Overall, it's one of the more dynamic and interesting parts of security and access management.

## 1.2 Delivery models

This Leadership Compass is focused on PAM products that are offered in on-premises deployable form as an appliance or virtual appliance, in the cloud or as-a-service (PAMaaS) by the vendor.

## 1.3 Required capabilities

In this Leadership Compass, we focus on solutions that help organizations reduce the risks associated with privileged access, through individual or shared accounts across on-premises and cloud infrastructure.

A simple PAM solution will provide an organization with the basic defences needed to protect privileged accounts, but most organizations today will need more to meet their more complex security and compliance obligations. Digital transformation and infrastructure changes mean that organizations will benefit from many of the advanced features now bundled with leading PAM solutions.

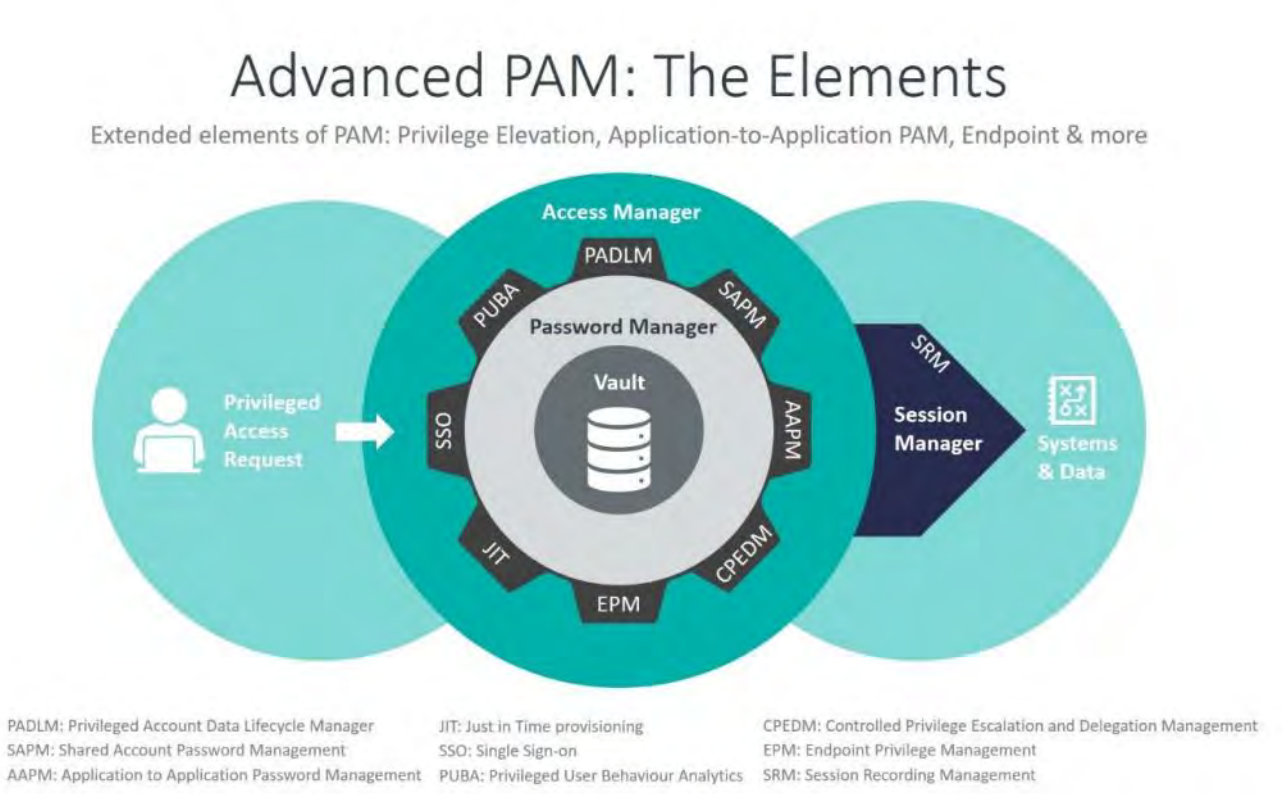



Figure 2: Advanced PAM elements. As the market demands have developed vendors have added more functionality to their solutions.

At KuppingerCole, we classify the Privileged Access Management (PAM) market into the following key technology functions with PAM vendors providing varied level of support for multiple PAM functions (see Figure 2).

### 1.3.1 Privileged Account Data Lifecycle Management (PADLM)

The usage of privileged accounts must be governed as well as secured. The PADLM function serves as a tool to monitor the usage of privilege accounts over time to comply with compliance regulations as well as internal auditing processes. If a breach occurs and a compromised privilege account is found to be a cause, investigators will want to know how well the account was managed and audited throughout its lifecycle.

### 1.3.2 Shared Account Password Management (SAPM)

Best practice demands that organizations switch to single identity privileged accounts, but shared privileged accounts still exist in many organizations and are a serious risk to security, especially if they are not monitored. The latest variants of PAM will have SAPM functionality built-in to oversee the management and auditing of shared accounts across the enterprise. An inability to account for number of usages of shared privileged accounts will almost certainly fail any relevant audit and could be a cause for prosecution under GDPR if it was proven that a shared account was responsible for the loss of credentials, that led to data being lost.

Organizations should discover and audit all privilege accounts – ensuring that only the right people or resources have access and bring them under the orbit of the SAPM so that access to shared accounts is monitored by the PAM solution and strictly controlled ideally with alerts set up for unauthorised usage of shared accounts. To put it into context a fully configured and set up PAM solution with SAPM will prevent instances of users accessing shared privileged accounts simply by knowing old passwords.

### 1.3.3 Application to Application Password Management (AAPM)

Part of digital transformation is the communication between machines and applications to other applications and database servers to get business-related information. Some will require privileged access but time constraints on processes means it needs to be seamless and transparent as well as secure. AAPM is therefore being added as part of the SAPM function to allow applications to access credentials, making PAM suitable for the digital age by treating people, machines and applications as equal entities to be secured, without slowing down communication or file access. The activity of applications can also be tracked in the same way as users in the Session Manager.

### 1.3.4 Controlled Privilege Elevation and Delegation Management (CPEDM)

This is another increasingly important function related to the fluid and fast changing needs of digital organizations. As the name suggests it allows users to gain elevation of access rights, traditionally for administrative purposes and for short periods typically, and with least privilege rights. However, some vendors are adapting the traditional role of CPEDM to become more task focused and adaptable to more flexible workloads that modern organizations require. This is known as Privileged Task Management (PTM), enabling least privilege access to resources to get

things done. Such processes can be pre-assigned for distribution or may well be a response to a specific request. The challenge for all PAM vendors is to integrate CEPDM and PTM securely and transparently. Inevitably, some will do it better than others.

### 1.3.5 Endpoint Privilege Management (EPM)

EPM offers capabilities to manage threats associated with local administrative rights on laptops, tablets, smartphones or other endpoints. EPM tools essentially offer controlled and monitored privileged access via endpoints and include capabilities such as application whitelisting for endpoint protection.

### 1.3.6 Session Recording and Monitoring (SRM)

Session Recording and Monitoring offers basic auditing and monitoring of privileged activities. SRM tools can also offer authentication, authorization and Single Sign-On (SSO) to the target systems.

### 1.3.7 Just in Time (JIT)

Just-in-time (JIT) privileged access management can help drastically condense the privileged threat surface and reduce risk enterprise-wide by granting secure instant access to privileged accounts. Implementing JIT within PAM can ensure that identities only have the appropriate privileges when necessary, as quickly as possible and for the least time necessary. This process can be entirely automated so that it is frictionless and invisible to the end user

### 1.3.8 Privileged Single Sign-On (SSO)

Single sign-on is a user authentication system that permits a user to apply one set of login credentials (i.e. username and password) to access multiple applications. This is very useful for speeding up workflows but allowing single sign on to privileged accounts carries risk if not subject to PAM controls. Therefore, PAM solutions are increasingly supporting integration with leading SSO vendors to address this challenge.

### 1.3.9 Privileged User Behaviour Analytics (PUBA)

PUBA uses data analytic techniques, some assisted by machine learning tools, to detect threats based on anomalous behaviour against established and quantified baseline profiles of administrative groups and users. Any attempted deviation from least privilege would be red flagged.

## 1.4 Other advanced features

PAM should accommodate the presence of a multitude of privileged users within an organization which includes temp workers, contractors, partner organizations, developers, DevOps, IT security admins, web applications and in some instances, customers. The more advanced features available

within PAM to manage the demands of the modern organization are discussed in more detail in the next chapter.

Other advanced capabilities may also be available such as privileged user analytics, risk-based session monitoring and advanced threat protection - all integrated into comprehensive PAM suites now available. These include:

- PAM for DevOps which some vendors are now providing as extra modules or standalone products. Any such solution should be designed to accommodate the unique challenges of DevOps such as rapid project turnaround and JIT provisioning.
- Privilege IT task-based automation is a new feature that brings PAM to more granular level by combining JIT access to specific tasks, often one time only. While integration with existing PAM solutions is currently limited, this is likely to change.
- Remote access for end users to privilege accounts is more relevant in digital environments. PAM solutions will increasingly support this in the future to help secure access for third parties such as customers and vendors, as well as remote workers.
- Privileged Access Governance deals with offering valuable insights related to the state of privileged access necessary to support decision making process. PAG includes privileged access certifications and provisions for customizable reporting and dashboarding.

# 2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof-of-Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership


Figure 3: The Overall Leadership rating for the PAM market segment

The PAM market is highly dynamic, and there have been a few changes in our Overall Leaders and Challengers for 2020. We had more vendors join the full Leadership Compass (including some who were Vendors to Watch last year) – with 24 vendors compared to 19 last year, which has influenced the order right throughout the Overall Leadership rankings. The Challengers area remains crowded as new entrants join the fray and vendors such as Hitachi ID, SSH.COM and Wallix move into the Leaders section.

CyberArk has maintained its overall leadership position thanks to continued investment in new features and by not resting on its laurels in the market. Just behind CyberArk the order has changed a little with Thycotic now moving just ahead of rivals BeyondTrust and Centrify thanks to

some good product enhancements in the last year. Broadcom's acquisition of CA technologies has brought extra financial muscle which keeps the solution as a Leader but we hope to see commitment from its new owners to refresh the suite so that it continue to compete among the Leaders. The PAM market is becoming more competitive and size alone will no longer keep vendors at the top. This is especially true in a period when vendors like SSH.COM can go from Challenger to Leader in one year due to a strong focus on technology and innovation. Less significant a move but still notable is the shift to Leader by Wallix, which has been steadily improving its product and sales and looks committed to continue to do so. One Identity has maintained its place among the Leaders with a solid solution that offers good scalability and ease of use. Hitachi ID has also both made good strides in its feature set to now sit among the Leaders.

Behind the Leaders we have a rather crowded bunch of Challengers split into two groups. The leading group is led by Kron which has leapt into this position by adding competitive new features and gaining strong ratings across the board. Joining Kron at the head of the Challengers are Micro Focus, Arcon, ManageEngine, Systancia and Stealthbits – all offering fine solutions that just fall short of overall leadership. Then we have a rather crowded bunch of Challengers in the second group comprising of Onion ID, EmpowerID, Senhasegura, Osirium, Xton Technologies, Sectona, Devolutions, Fudo Security and Remediant. These constitute a dynamic group that individually may lack the tools and sophistication of the leading Challengers bit still contain some great innovation and specialist applications that potentially could develop into highly capable PAM suites for the modern era. This area is more than likely where next year's higher rated Challengers and even Leaders may come from as the market continues to grow and solutions develop.

**Overall Leaders are (in alphabetical order):**

- BeyondTrust
- Broadcom
- Centrify
- CyberArk
- Hitachi ID
- One Identity
- SSH
- Thycotic
- Wallix

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

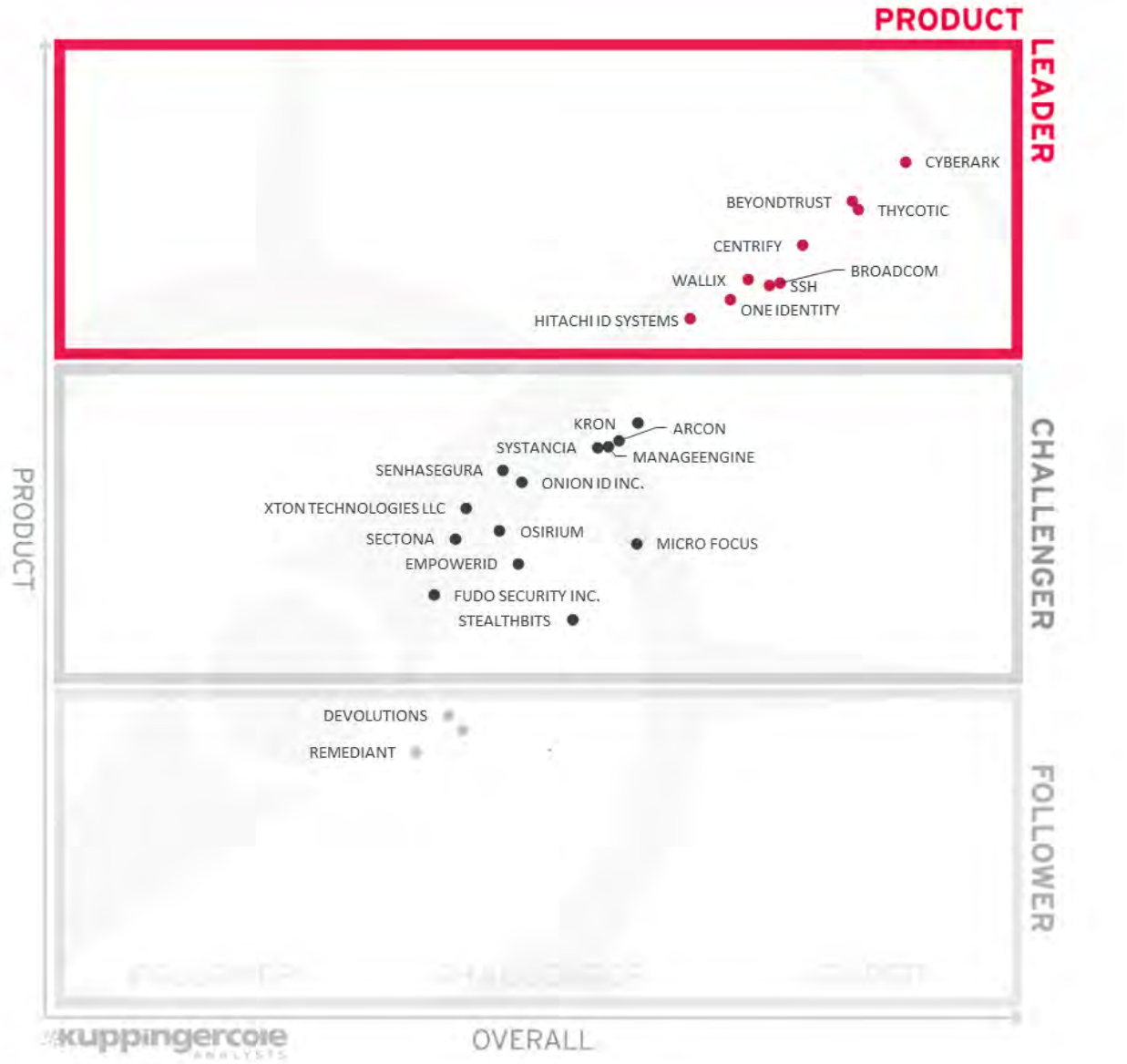



Figure 3: Product Leaders in the PAM market segment

Again, CyberArk is rated as the leading vendor, followed by BeyondTrust and Thycotic with a hair's breadth between them. While the three have some differences, all have a comprehensive set of features and capabilities which form a strong foundation for a Privileged Access Management implementation and would be an excellent choice for many organizations. Behind the Big Three are the same pack that feature in the Overall Leadership with some slight variants in positioning: Centrify, SSH.COM, Broadcom, Wallix, One Identity and Hitachi ID – which demonstrates that having a broad set of features and innovative features will put a product among the leaders. Wallix and SSH have both done much to improve their portfolio propositions in the last year.

There are changes in the Challengers section with Kron, Systancia, Senhasegura, Onion ID, ManageEngine and Arcon now among the leading Challengers – all have added or improved feature sets since 2019. All these vendors now offer strong PAM features that might fit well for specific PAM requirements of customers.

Elsewhere, Xton Technologies, which was not in the full Compass last year, is making its presence felt in the Challengers reflecting the dynamic changes in the market. It is closely aligned with Sectona, Osirium, Micro Focus, EmpowerID, Fudo Security and Stealthbits. All have specific strengths but present certain gaps in the depth and breadth of supported functionalities.

In the Followers section we see Devolutions and Remediant. Both have individual strengths especially in addressing the SMB market and providing out of the box solutions for the cloud however and should be considered by those looking for specialist applications.

**Product Leaders (in alphabetical order):**

- BeyondTrust
- Broadcom
- Centrify
- CyberArk
- Hitachi ID
- One Identity
- SSH
- Thycotic
- Wallix

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested cutting-edge features, while maintaining compatibility with previous versions.

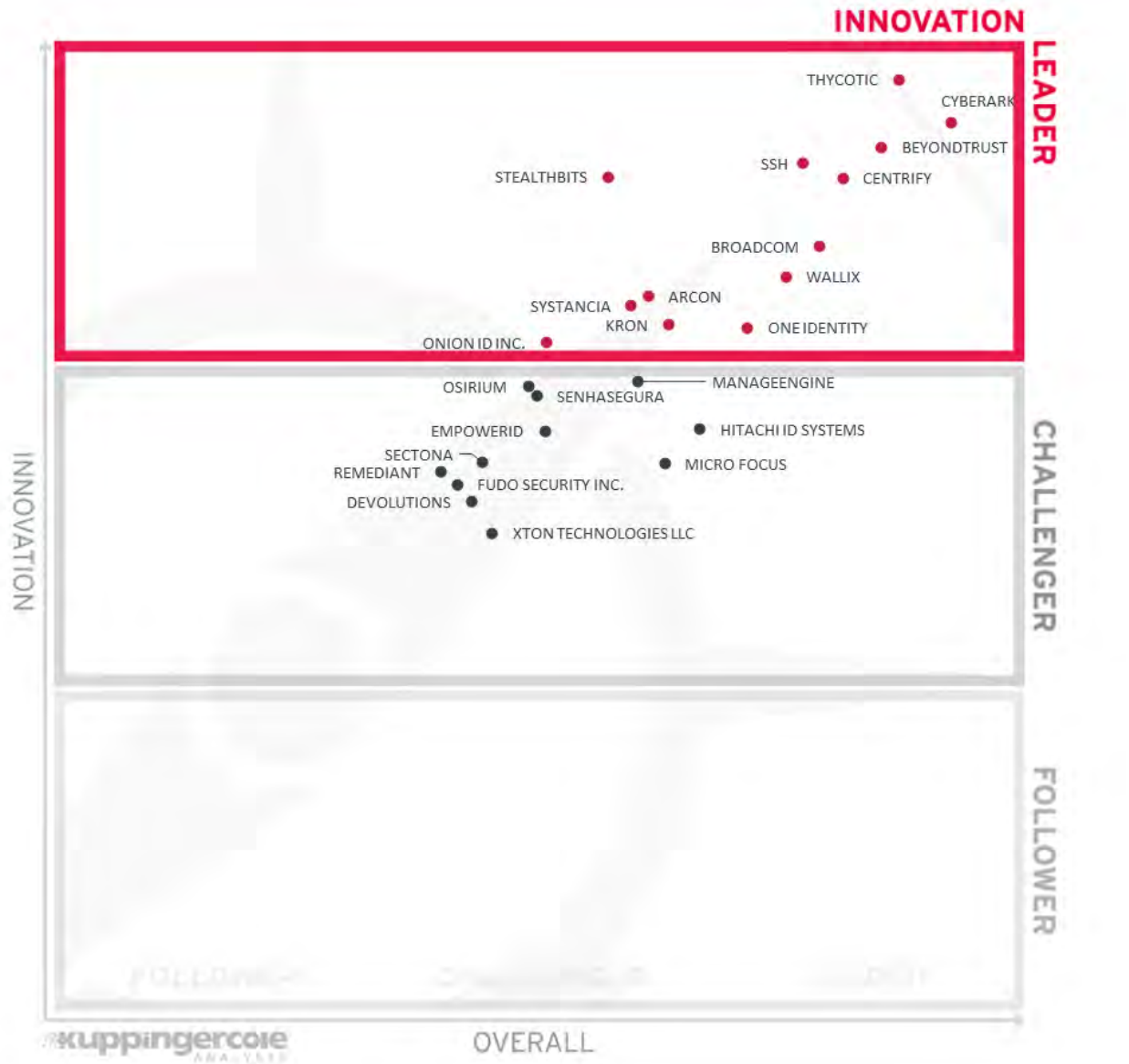



Figure 3: Innovation Leaders in the PAM market segment

The pacing in innovation has changed with five companies vying at the top of the innovation space, reflecting the growing awareness of the importance of innovation among product managers and engineers at Thycotic, CyberArk, BeyondTrust, Centrify and SSH.COM. This is welcome and reflects response to changing demand in the market for more features and faster time to value after deployment. Also, among the Innovation Leaders are Stealthbits, Broadcom, Wallix, Arcon, Systancia, Kron, One Identity and Onion ID. Leading the Challengers are Osirium, ManageEngine and Senhasegura – all of whom have added good new features and improvements in the last year. The Challengers are rounded out by EmpowerID, Sectona, Micro Focus, Remediant, Hitachi ID, Fudo Security, Devolutions and Xton Technologies. The trend towards greater innovation is further

borne out by the fact there are no Followers in this matrix.

KuppingerCole believes this result shows that all vendors are looking where they can innovate in order to gain some competitive advantage in the market, but also within certain sectors such as SMB or in the emerging area of PAMaaS. It shows a market that is changing fast as the impact of digital transformation and increased levels of compliance has forced greater demands onto PAM solutions.

**Innovation Leaders (in alphabetical order):**

- Arcon
- BeyondTrust
- Broadcom
- Centrify
- CyberArk
- One Identity
- SSH
- Stealthbits
- Thycotic
- Wallix

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, number of managed identities, ratio between customers and managed identities, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

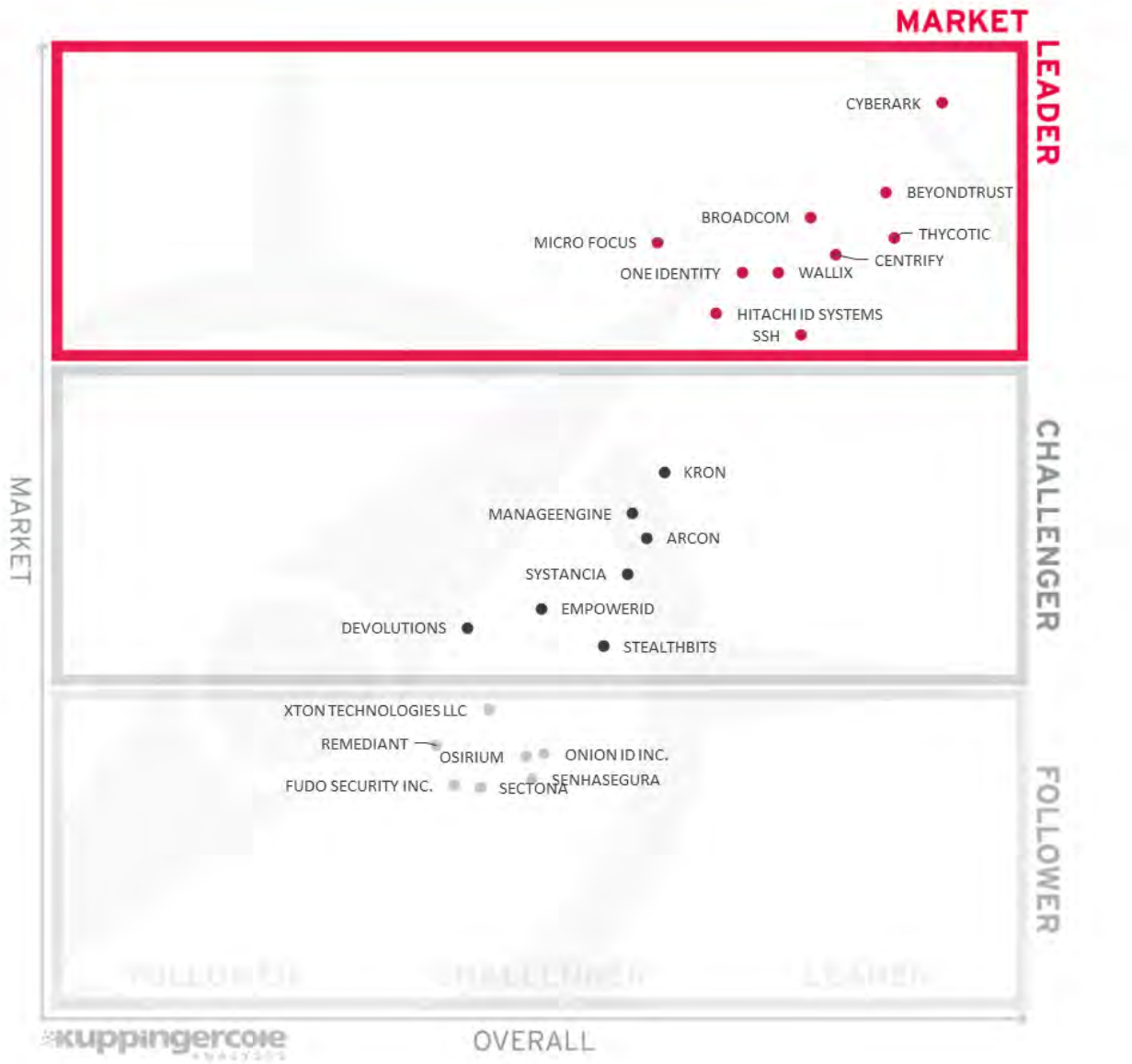



Figure 3: Market Leaders in the PAM market segment

In this section there are few surprises as the biggest longest-serving companies tend to dominate although even here there is some flux with a flattening of vendors in the chasing pack.

CyberArk continues to be the overall Leader with a gap between it and the chasing pack that includes BeyondTrust, Broadcom, Centrify, Hitachi ID, Micro Focus, One Identity, SSH.Com, Thycotic and Wallix. Broadcom while not the most innovative or active in the past year is undeniably benefiting from the financial muscle and clout of one of the world's largest chip manufacturers as it relaunches its PAM solution under the Symantec brand. Wallix, Micro Focus and Hitachi ID have all joined the leaders from previously being Challengers, reflecting growth in the market and space for more vendors at the top end.

Kron has leapt into the top of the Challengers section as it has made good improvements to its product and its marketing and its parent, one of Turkeys' leading technology businesses is also growing fast, providing it with the backing it needs to compete with the more established players. It is joined by Arcon, ManageEngine and Systancia, EmpowerID, Devolutions and Stealthbits, all of whom have improved their standing with improved products and better market positions over the last 12 months. We do have some followers: Xton Technologies, Remediant, Osirium, Onion ID, Senhasegura, Fudo Security and Sectona. All have individual merits in terms of features or innovations, and all should benefit from a growing market with careful marketing in the next 12 months.

**Market Leaders (in alphabetical order):**

- BeyondTrust
- Broadcom
- Centrify
- CyberArk
- Hitachi ID
- Micro Focus
- One Identity
- SSH.COM
- Thycotic
- Wallix

# 3 Correlated view

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

## 3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership. This is where we see a more granular breakdown of the results of the Leadership Compass. The more to the upper right edge, the better is the combined position. Vendors above the line are said to be "overperforming" in the market. It comes as no surprise that these are mainly larger vendors, while vendors below the line frequently are not as established in the market, but commonly show a comprehensive and innovative feature set.

Therefore, we can see that the top right box contains few surprises with CyberArk retaining a similar lead over the rest of the larger providers including BeyondTrust, Thycotic, Broadcom, Wallix, Centrify, One Identity, Hitachi ID and SSH.COM – which stands out for innovation in this group as in earlier matrices. The financial clout of Micro Focus has pushed what was NetIQ into a high market position but its relative lack of new or improved features has held it back as a true Market Champion in the top right sector.

Beneath the Market Champions we have a cluster of companies that share a good mixture of technology features along with a relatively strong market position. These are Kron, ManageEngine, Arcon, Systancia, EmpowerID and Stealthbits. Devolutions is to the left of this group lacking comprehensiveness, but it has some good features that will appeal to smaller companies or those looking for an out of the box basic PAM solution.

Finally, we have a group of vendors that so far lack market clout by nature of being smaller operations but again do offer some unique tools that bode well for their future development such as vaultless solutions or automation tools. This group comprises of Xton Technologies, Fudo Security, Osirium, Onion ID, Senhasegura and Sectona. Osirium, Sectona Onion ID and Senhasegura do well to score better than some larger rivals for innovation and features. Remediant has some work to do to move across the matrix but it is a young company with lots of potential to improve.

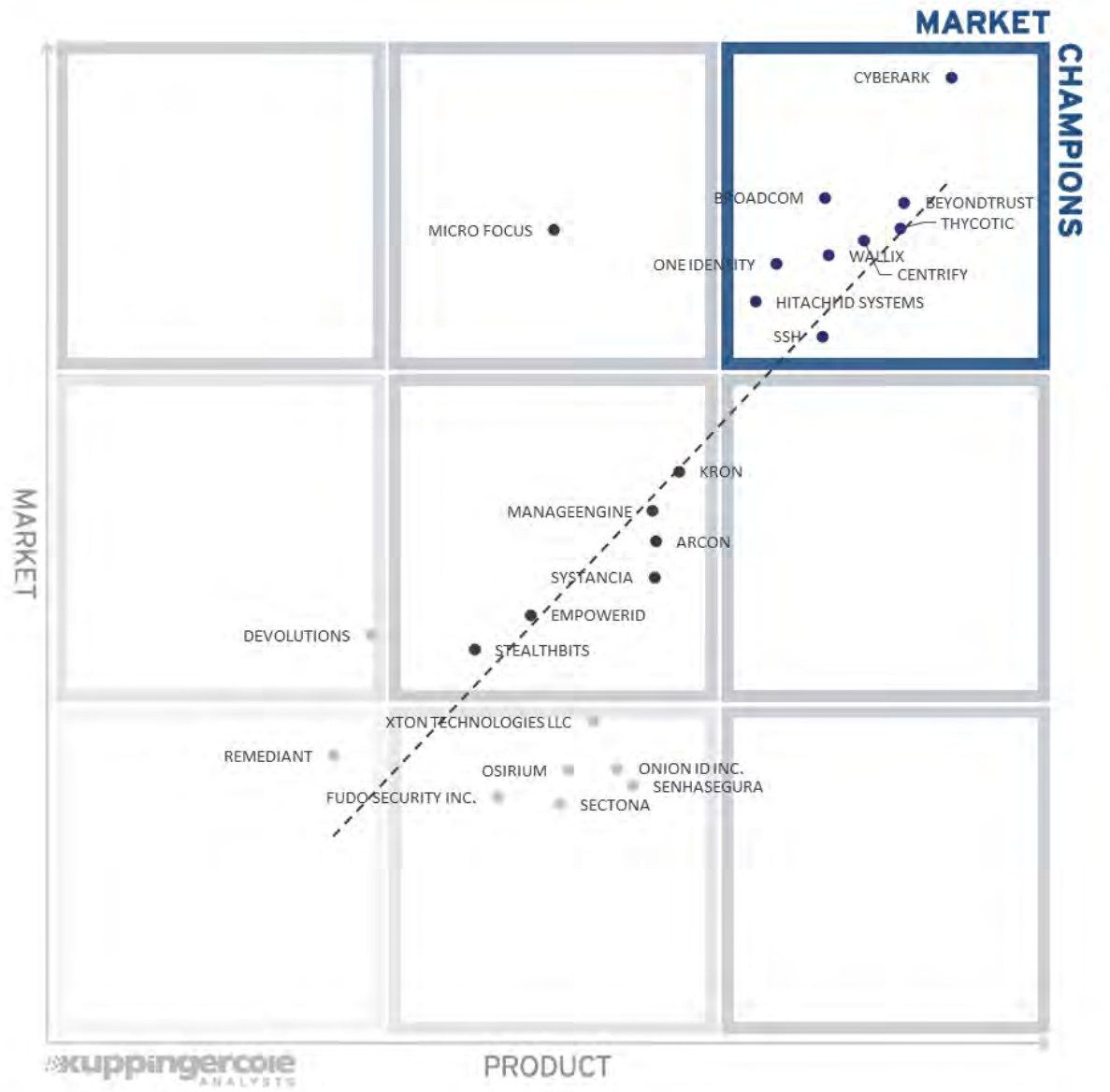



Figure 7: The Market/Product Matrix.

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

## 3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. This distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

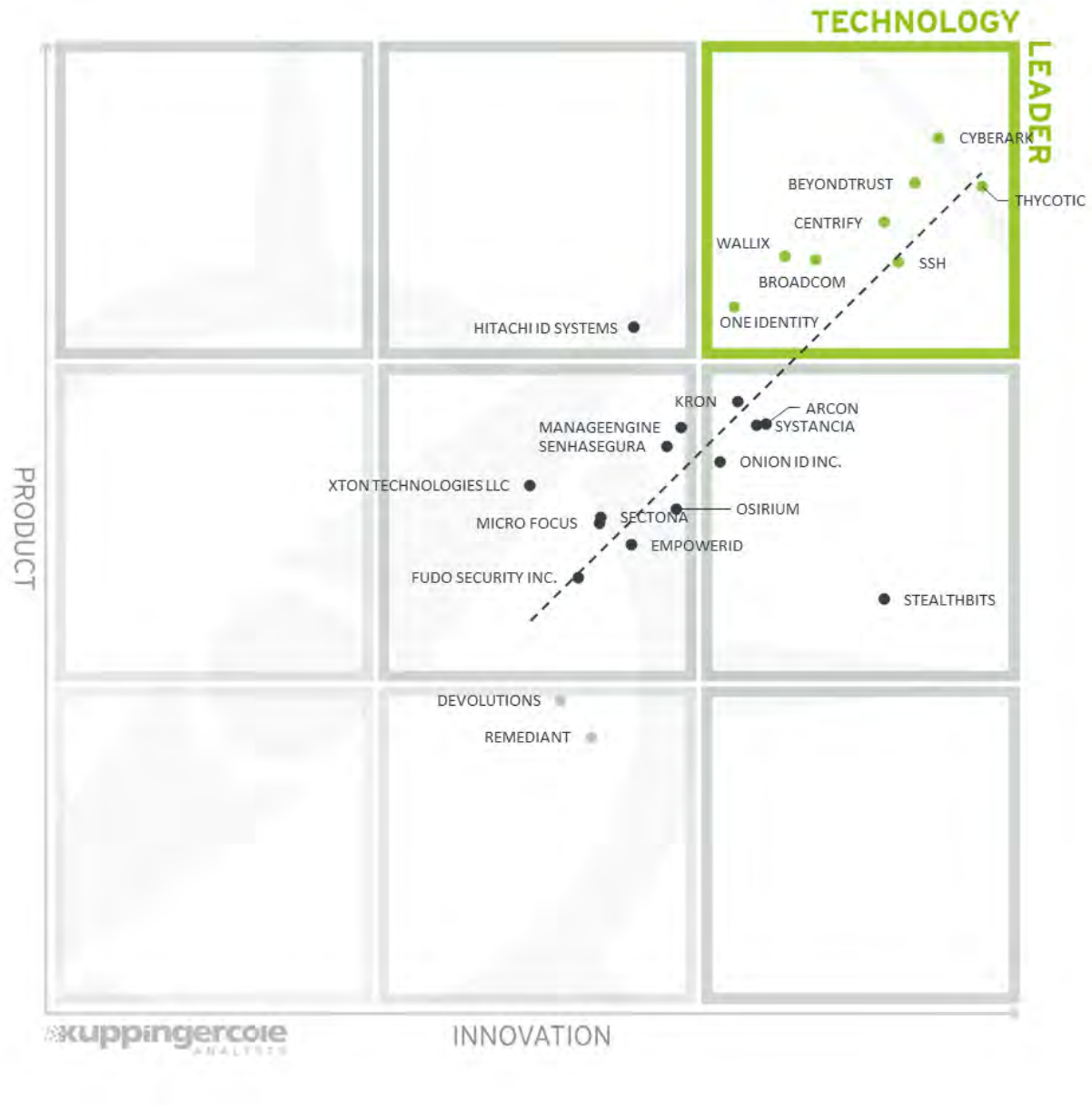



Figure 8: The Product/Innovation Matrix.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

In this matrix we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most of the leading vendors in the upper right corner, scattered throughout the box.

These include CyberArk, Thycotic, BeyondTrust, Centrify, SSH.COM, Wallix, Broadcom, and One Identity while Hitachi ID falls just outside by not quite matching the innovation levels of those

rivals but remains highly rated for its product overall. Thycotic scores best for innovation but still lacks the overall product strength of CyberArk and BeyondTrust.

Below the Technology Leaders we have a cluster of vendors: Kron Technologies, Arcon, Systancia, ManageEngine, Senhasegura, Onion ID, Xton Technologies, Micro Focus, Osirium, Sectona, EmpowerID, Fudo Security and Stealthbits – something of an outlier by scoring well for innovation thanks to its JIT ephemeral approach to PAM.

Finally, we have two vendors that do well for innovation but lack overall product completeness. These are Devolutions and Remediant. These still score well for ease of use and will appeal to smaller companies – both have some good ideas.

## 3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

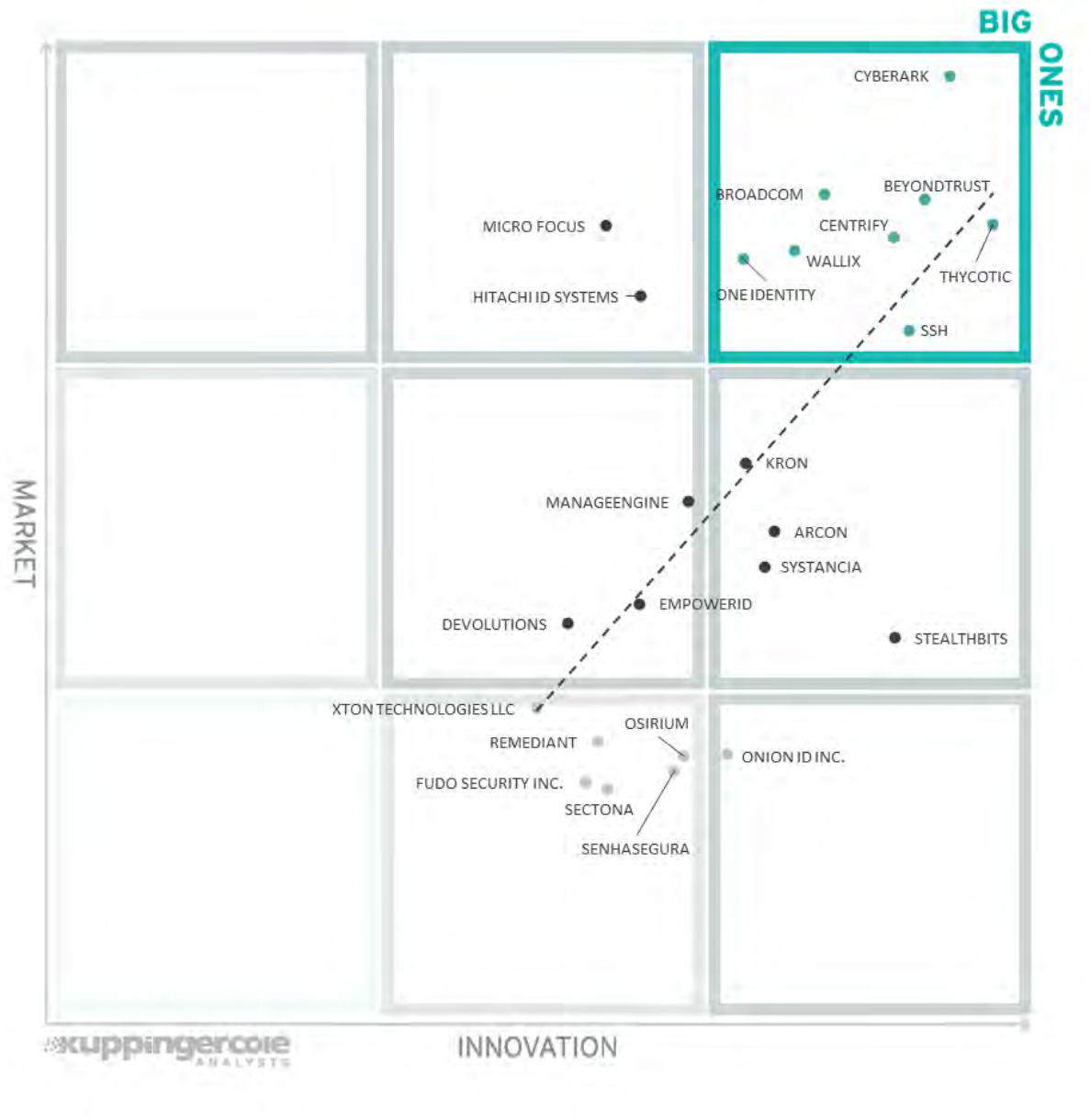



Figure 9: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating; while vendors below the line show an ability to innovate, and thus the biggest potential for improving their market position.

This Matrix then gives a good overview of how vendors are using innovation to improve their position in the market and those which need to do more. It splits the bigger companies with Micro Focus, Hitachi ID needing to do more to innovate closer to the group in the top right box: CyberArk, Broadcom, BeyondTrust, Thycotic, Centrify, Wallix, One Identity and SSH.COM. Even within the top right box we can see that a smaller vendor, SSH.COM has out innovated some

bigger rivals while Thycotic has shown more innovation than CyberArk, BeyondTrust and Centrify. But once again, choosing any of the vendors here would result in a good purchase for many organizations with the promise of reliability, innovation and solidly financed support.

Below the Big Ones we see a group clustered around the line: Kron, ManageEngine, Arcon, Systancia, EmpowerID and Devolutions. Stealthbits retains its high rating for Innovation for the reasons mentioned in the last section.

Then we have a group that so far lack market presence to compete with the bigger vendors and may need to broaden their innovation across their solutions to momentum and critical mass in the market. This group, which all have some great tools individually, includes Xton Technologies, Remediant, Fudo Security, Sectona, Osirium, Senhasegura and Onion ID.

# 4 Products and vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on PAM. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

## 4.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

| Product | Security | Functionality | Interoperability | Usability | Deployment |
|---|---|---|---|---|---|
| ARCON Privilege Account Management | positive | positive | positive | strongly positive | positive |
| BeyondTrust PAM | strongly positive | strongly positive | strongly positive | positive | strongly positive |
| Broadcom Symantec PAM | positive | strongly positive | strongly positive | strongly positive | positive |
| Centrify Privilege Access Service | strongly positive | strongly positive | positive | positive | strongly positive |
| CyberArk PAM | strongly positive | strongly positive | positive | strongly positive | strongly positive |
| Devolutions PAM | neutral | neutral | weak | neutral | neutral |
| EmpowerID PAM | neutral | positive | weak | neutral | neutral |
| FUDO Security PAM | neutral | positive | neutral | positive | strongly positive |
| Hitachi ID HiPAM | strongly positive | strongly positive | strongly positive | positive | positive |
| Krontech Single Connect | positive | positive | positive | positive | neutral |
| ManageEngine PAM360 | positive | positive | positive | strongly positive | neutral |
| Micro Focus NetIQ | positive | strongly positive | neutral | neutral | neutral |
| One Identity Safeguard | positive | positive | positive | strongly positive | positive |
| OnionID PAM | positive | positive | positive | positive | neutral |
| Osirium Privilege Access Security | positive | positive | neutral | positive | neutral |
| Remediant SecureOne | neutral | neutral | neutral | strongly positive | strongly positive |
| Sectona Spectra | neutral | neutral | positive | positive | positive |
| Senhasegura PAM (by MT4 Networks) | positive | positive | positive | positive | strongly positive |
| SSH.COM PrivX | positive | positive | positive | positive | strongly positive |
| STEALTHbits Privilege Activity Manager | neutral | positive | neutral | strongly positive | neutral |
| Systancia Cleanroom | positive | positive | neutral | positive | neutral |
| Thycotic Secret Server | strongly positive | strongly positive | strongly positive | strongly positive | positive |
| WALLIX Bastion | strongly positive | strongly positive | positive | positive | positive |
| Xton Access Manager (XTAM) | positive | positive | positive | neutral | neutral |
| Legend | | critical | weak | neutral | positive | strongly positive |

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

| Vendor | Innovativeness | Market Position | Financial Strength | Ecosystem |
|---|---|---|---|---|
| Arcon | positive | neutral | positive | positive |
| BeyondTrust | positive | strongly positive | strongly positive | positive |
| Broadcom Inc. | neutral | positive | strongly positive | strongly positive |
| Centrify | positive | positive | positive | strongly positive |
| CyberArk | positive | strongly positive | strongly positive | strongly positive |
| Devolutions | neutral | weak | neutral | neutral |
| EmpowerID | neutral | neutral | positive | positive |
| Fudo Security | positive | weak | weak | neutral |
| Hitachi ID Systems | positive | positive | strongly positive | strongly positive |
| Krontech | neutral | weak | neutral | strongly positive |
| ManageEngine | positive | neutral | positive | neutral |
| Micro Focus | neutral | positive | strongly positive | strongly positive |
| One Identity | neutral | positive | strongly positive | strongly positive |
| OnionID | positive | weak | weak | weak |
| Osirium | positive | weak | weak | neutral |
| Remediant | strongly positive | weak | neutral | weak |
| Sectona | neutral | neutral | neutral | weak |
| Senhasegura | positive | neutral | positive | neutral |
| SSH Communications Security | positive | positive | positive | neutral |
| STEALTHbits Technologies | strongly positive | neutral | neutral | neutral |
| Systancia | positive | weak | neutral | positive |
| Thycotic | positive | strongly positive | strongly positive | positive |
| WALLIX | neutral | positive | strongly positive | positive |
| Xton Technologies | strongly positive | weak | neutral | neutral |
| Legend | critical | weak | neutral | positive | strongly positive |

# 5 Product/service evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

**Spider graphs**

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For PAM, we look at the following eight areas:

- Privileged Account Data Lifecycle Management (PADLM)
- Shared Account Management
- Application to Application Privilege Management (AAPM)
- Controlled Privilege Escalation and Delegation Management (CEPDM)
- Endpoint Privilege Management (EPM)
- Privilege Session SSO
- High Availability & Failover
- Session Management

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on PAM.

## 5.1 Arcon

Founded in 2006 and based in Mumbai (India), Arcon offers its Privilege Account Management Suite to manage privileged access across various delivery models. Arcon takes a reliable modular approach to PAM, with modules that are licensed separately and offered in software, virtual and physical appliances with a PAM as a Service (PAMaaS) option. Most standard capabilities are offered as well as more advanced functions such as PUBA and CPEDM. However, EPM is provided by a separate product also available from Arcon.

Primarily built on an ASP.NET framework, Arcon extends a set of APIs to integrate user configuration, vault and service access functions into Web UIs. With built-in support available for most commercially available operating systems, servers, network devices and SaaS applications, Arcon offers password management, granular access and command control for databases – a capability missing from several leading PAM vendors in the market.

Arcon's ability to develop customized connectors for password and account management for legacy applications and systems could be an advantage for organizations that deem legacy infrastructure important to support critical business functions. Other key features for Arcon include SSO for admins, user onboarding facility, centralized and single admin control, MFA support and text and video recording of all sessions.

In addition to native software-based OTP authentication methods for session initiation, Arcon offers Out of the Box (OOB) integration with RSA and Entrust for hardware OTP tokens and with Gemalto for biometric authentication methods. Overall, a solid set of PAM functions offered to meet the requirements of different sized organizations. Arcon is an ambitious company and has plans in its pipeline to develop further AI and facial recognition capabilities into its PAM product suite.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●○ |

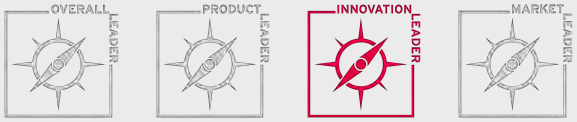
## Strengths

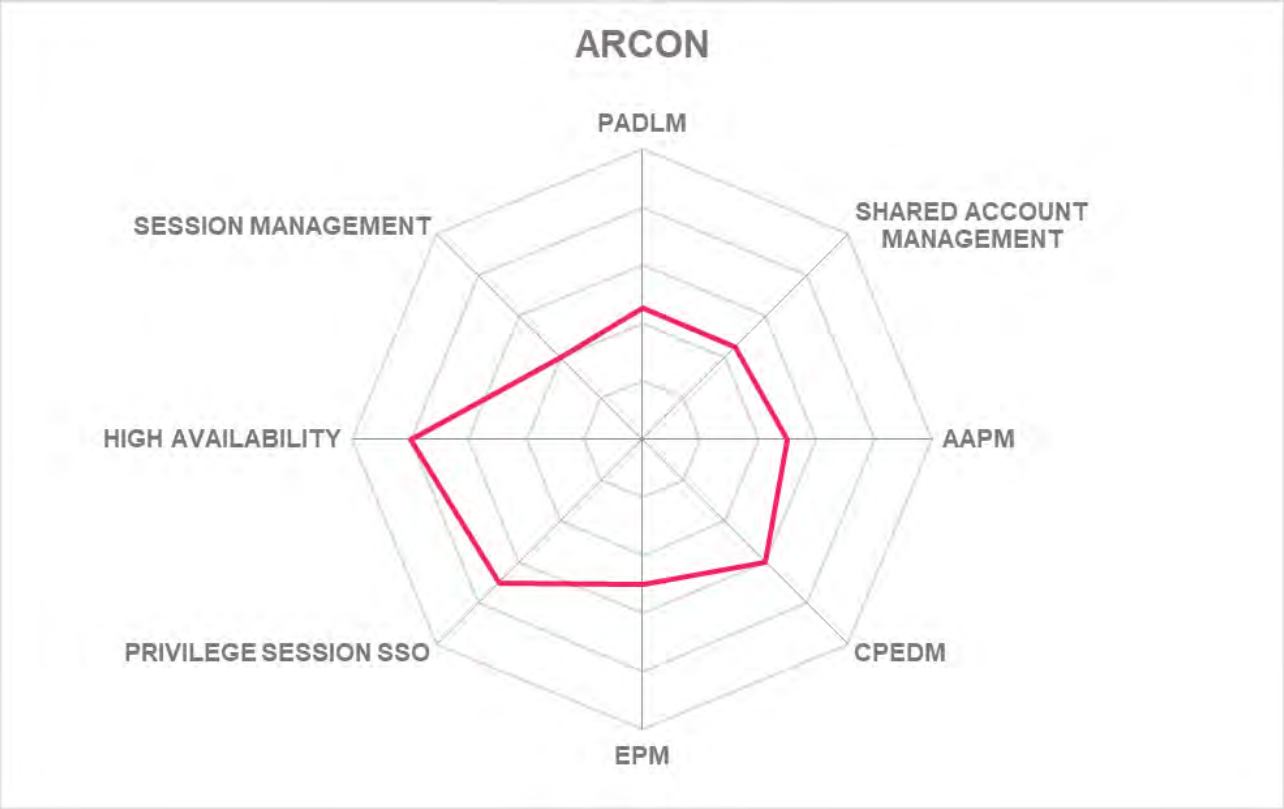
- Design works well with strong focus on compliance
- Feature-rich comprehensive PAM solution
- Soft OTP and biometric authentication included
- Readily integrable with standard SIEM and help-desk tools
- Ease of deployment and administration
- Available as a hosted and managed service, and PAM as a Service

## Challenges

- Interface needs a refresh to meet current best standards
- Increasing but limited penetration in North America and European markets
- EPM is not included in core product

## Leader in




ARCON
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.2 BeyondTrust

After acquiring Avecto, Lieberman software and BeyondTrust, Bomgar decided to merge the businesses and keep the BeyondTrust brand for the new entity. It now potentially represents one of the largest PAM vendors in combined revenue and customer size numbers.

BeyondTrust's main suite of products is now streamlined for Privileged Password Management, Endpoint Privileged Management and Secure Remote Access. Password management is provided for by three key solutions: Password Safe (formerly PowerBroker), Cloud Vault and DevOps Secrets Safe. There is also the BeyondInsight analytics module which is now serving vulnerability management duties as BeyondTrust's Enterprise Vulnerability Management tool went EOS in December 2019, and will be EOL by December 2020.

Like many others, BeyondTrust PAM can be deployed on cloud, hybrid and on-premises . Similar to CyberArk, which BeyondTrust clearly has in its sights, buyers can choose from a variety of modules – start small and work up - all modules from the three main categories will integrate so it shouldn't matter in which order you buy depending on need and each supports a common interface. The Bomgar acquisitions have now been integrated making BeyondTrust better placed to move forward as one unit, although it can be hard to determine which package is best for an organization from the vendor web site, which can be confusing.

BeyondTrust says that it has increased R&D spend by 22% to keep pace with changes in the market. It is looking to improve time to value and automate more processes within the product – both good moves for today's market. There is a good selection of third-party integrations with SailPoint and Splunk on the list, and its long-time partnership with ServiceNow now looks a good bet as digital workplace and service desk tools are becoming part of the PAM universe. BeyondTrust offers OOB integrations to support 2FA or MFA with any LDAP/LDAPS, RADIUS or SAML based providers. There is also host based CPEDM support.

Like others in the field, BeyondTrust is aware of the need to support PAM for DevOps. However, its approach has gone beyond paying lip service with existing functionalities and it has debuted a whole new vault dedicated to DevOps and agile environments. The new DevOps Secrets Safe goes beyond securing passwords and stores secrets used by applications, tools and other non-human identities. BeyondTrust also claims native integration with DevOps tools such a Jenkins, Puppet and Chef.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●● |
| Usability | ●●●●○ |
| Deployment | ●●●●● |

BeyondTrust

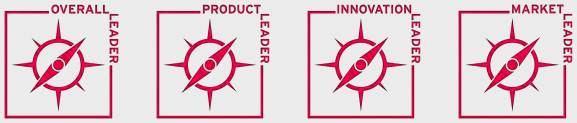
## Strengths

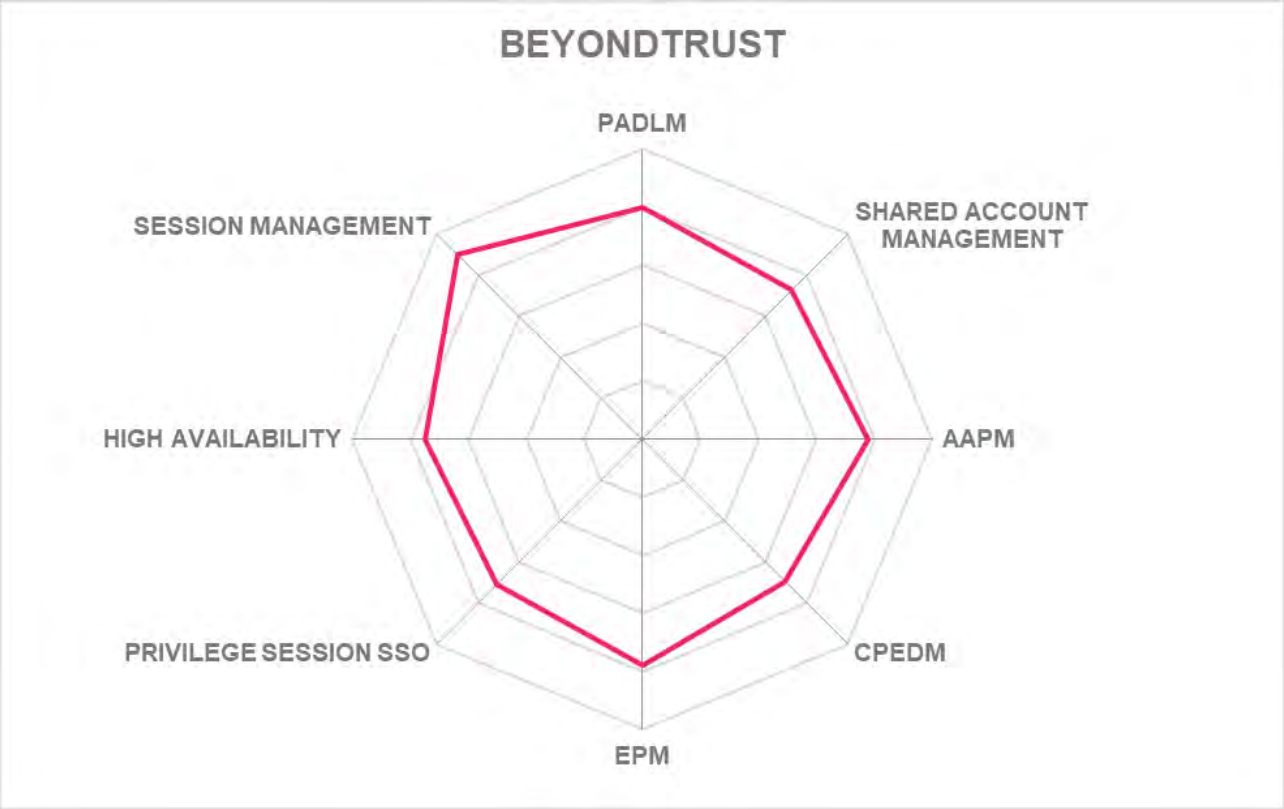
- Acquisitions now much better integrated making this a viable joined-up PAM suite
- Has taken support for DevOps much further than some rivals
- Host-based approach for CPEDM delivers strong and granular command control for privilege elevation
- Ability to mix and match solutions across three main categories provides flexibility
- Strong endpoint and remote access functionality, good visibility and control of third-party remote access

## Challenges

- BeyondTrust vulnerability management tool has gone EOS
- Vendor website can be confusing in presenting the features of PAM products making selection harder
- PAMaaS option would be a welcome addition

## Leader in




BEYONDTRUST
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.3 Broadcom Inc.

A new name in the PAM Leadership Compass but the presence of the US chip manufacturing giant is explained by its acquisitions of CA Technologies and subsequently, Symantec. Having digested the former CA collection of IAM technologies, it now intends to market its PAM solution under the Symantec brand, well known in IT security.

Symantec is a brand long famous for its sturdy endpoint protection products and Broadcom obviously hope the brand will work well for what was CA's PAM suite. It may play well in the SMB market where Symantec has always been strong. Certainly, Symantec's PAM solution should have some investment dollars behind it with Broadcom's 22.5bn annual revenue and it will be run as a subsidiary. CA's previous Identity solutions will also be marketed and developed under the Symantec flag from now on.

As the acquisition is still bedding in there is no great technical leap forwards from the CA platform of 2019 but there are changes in presentation. Symantec now talks of a "OnePAM" solution which will incorporate an access manger including vault, and a PAM Server control, giving agent-based control of servers and a threat analytics module. The solution is designed for hybrid environment with AWS and Azure support and Symantec claims its appliances can be stood up very quickly, with auto discovery of privileged accounts getting basic PAM up and running in 2- 3 days.

Given that many competitors are now happily marketing PAM suites with optional modules available off the shelf this fully integrated approach could be risky, however modules can still be purchased optionally.

In terms of technology then not much has changed. There are still robust SAPM, AAPM and PSM capabilities in the solution. The Threat Analytics engine delivers advanced threat analytics leveraging machine learning techniques for automated detection of risky privileged behavior. The PAM Server Control offers an agent-based architecture to intercept control and restrict commands at OS Kernel level enabling a fine-grained command control and privilege elevation while enabling authentication of UNIX and Linux users using AD and Kerberos credentials for Unix-AD bridging. The affinity with CA's former IAM product remains. Overall, something of a holding pattern for this product. Symantec is promising development for 2020 in DevOps and other key areas.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●● |
| Interoperability | ●●●●● |
| Usability | ●●●●● |
| Deployment | ●●●●○ |

BROADCOM®

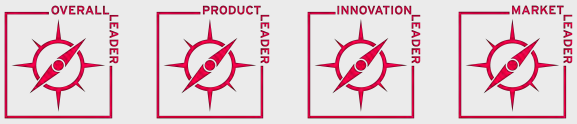
## Strengths

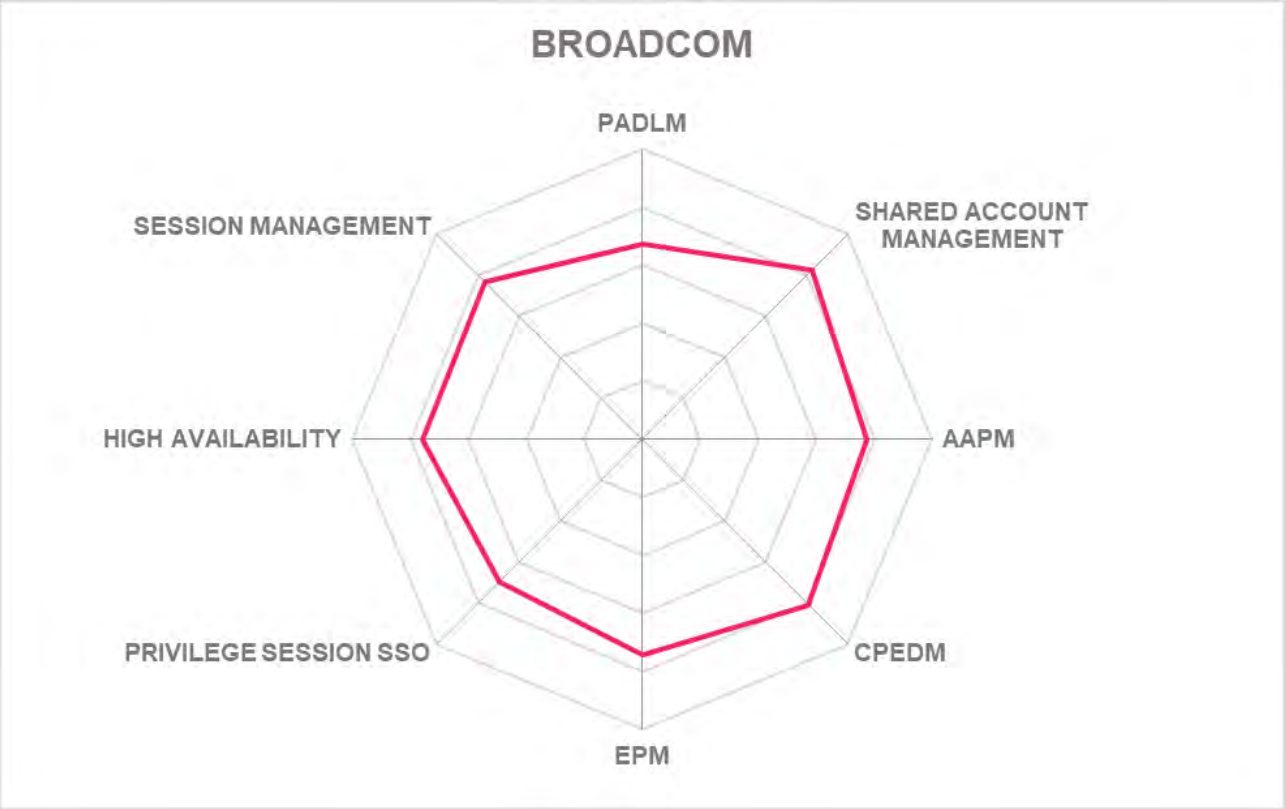
- Supports a broad range of target IT systems
- Full support for AAPM
- Support for virtualized and Cloud environments
- Fine grained command control
- Support for both host and proxy-based approaches to PAM
- Strong partner ecosystem
- Strength and reputation of Symantec brand in cybersecurity

## Challenges

- Support for DevOps is present but is in early developmental stage
- Product needs period of stability and renewed commitment from its new guardians
- Lack of focus on mid-market segments

## Leader in




BROADCOM
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.4 Centrify

Based in the US, Centrify offers several PAM modules as part of an overall suite which includes privilege access, authentication, privilege elevation and analytics. Privileged Access Service is Centrify's central PAM solution that leverages its access management capabilities.

Centrify also offers Privilege Elevation Service and Privilege Threat Analytics to round out its PAM capabilities. The Privileged Access Service supports DevOps up to a point with its vault also being able to store IP addresses, API keys, SSH credentials and AWS IAM credentials, and it enables secure communication between applications, containers and microservices.

The platform offers access to databases such as TOAD, SQL Server Management Studio and VMWare vSphere. Access is provided via a sandboxed remote desktop environment to prevent exposure to malware. Deployment options include SaaS, customer-managed private cloud, and on-premises while Centrify's Vault is available to customers on AWS marketplace with up to 50 systems free of charge.

CPEDM is available with Just in Time privileged access via built-in workflows or available through integration with 3rd parties such as ServiceNow and SailPoint Technologies. The session manager includes auditing and monitoring at both the host and gateway levels and there is also built in adaptive MFA for privileged access and privileged analytics.

The Centrify Privileged Access Service provides password vaulting, offering SAPM, secure administrative access via a distributed local jump box and secure remote access for privileged users to target systems. Centrify Authentication Service offers adaptive MFA and identity consolidation in addition to Unix/Linux -Active Directory (AD) bridging. The Centrify Privilege Elevation Service delivers delegated privilege role and policy management, time-based role assignment. Finally, the Centrify Privilege Threat Analytics Service uses a degree of machine learning techniques to provide greater intelligence on user and threat analytics and enforces new access policies based on user behaviour.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●●● |

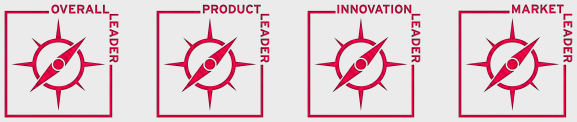

## Strengths

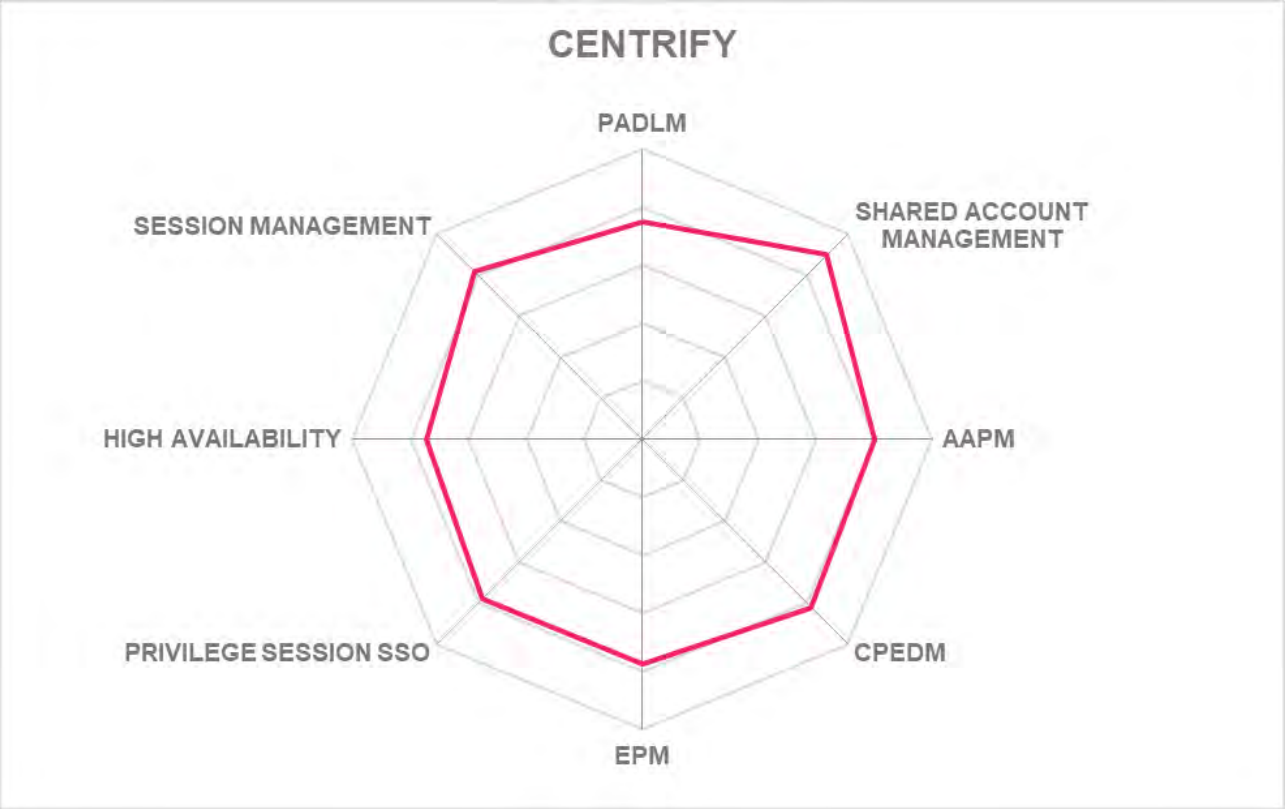
- Deep AD integration supporting complex multi-domain/ forest configurations
- Strong MFA and identity federation support with risk adaptive capabilities
- Strong CPEDM support
- Mature PAM as a Service offering in addition to a managed, on-premises delivery
- Strong privileged analytics with advanced machine learning techniques
- DevOps are provided for, good suitability for hybrid and containerized IT environments

## Challenges

- Lack of comprehensive Endpoint Privilege Management capabilities for desktops
- Pricing is on the higher side of the spectrum
- Strong focus on North America with yet limited but growing partner ecosystem in other regions

## Leader in




CENTRIFY
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.5 CyberArk

Headquartered in Israel and the US, CyberArk is one of the more mature providers of PAM solutions having been in the market since 1999. It has continued to add technical functionality to its broad suite of products in response to changing market demands.

CyberArk has been a leader in the PAM field for many years and continues to offer one of the broadest offerings in the market, and regularly adds new functionality to keep up with market demand. Its various PAM modules support on-premises, Hybrid and Cloud infrastructures. It has a commanding position in the market and remains the solution to beat for many rivals.

CyberArk say that buyers often start off with the basic PAM module and then move onto more advanced solutions as needs change – locking buyers at an early stage into one PAM ecosystem is a smart move as it become harder to change the more you invest.

In the last 12 months CyberArk has added the following new features to its suite: Just in Time (JIT) access for admins and CyberArk Alero, a new SaaS solution that combines biometric multi-factor authentication provisioning for remote users who need access to critical internal systems via CyberArk, without the need to use passwords. CyberArk's back up and failover capabilities are now reinforced with an active-active architecture and multiple vaults across geographies. Designed to offer flexibility, scalability and high availability, most CyberArk components can be installed on hardware, VMs and in AWS, Azure or Google Cloud. CyberArk also has a PAM as a Service (PAMaaS) offering to manage credentials for both human and non-human users and session management.

CyberArk has really made some great advances in providing PAM for new agile environments such as DevOps. CyberArk Conjur provides secrets management across native cloud, DevOps, containerized and other dynamic environments enabling developers to secure and manage secrets used by users, applications, microservices, containers, APIs etc. throughout the DevOps cycle. CyberArk continues to offer in depth analytics, session management, elevation management and AAPM technologies across its suite of products. It also offers a wide range of third-party applications and CyberArk is doing much to ensure its solutions are ready for the next set of privilege access challenges related to digital transformation across many organizations.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |

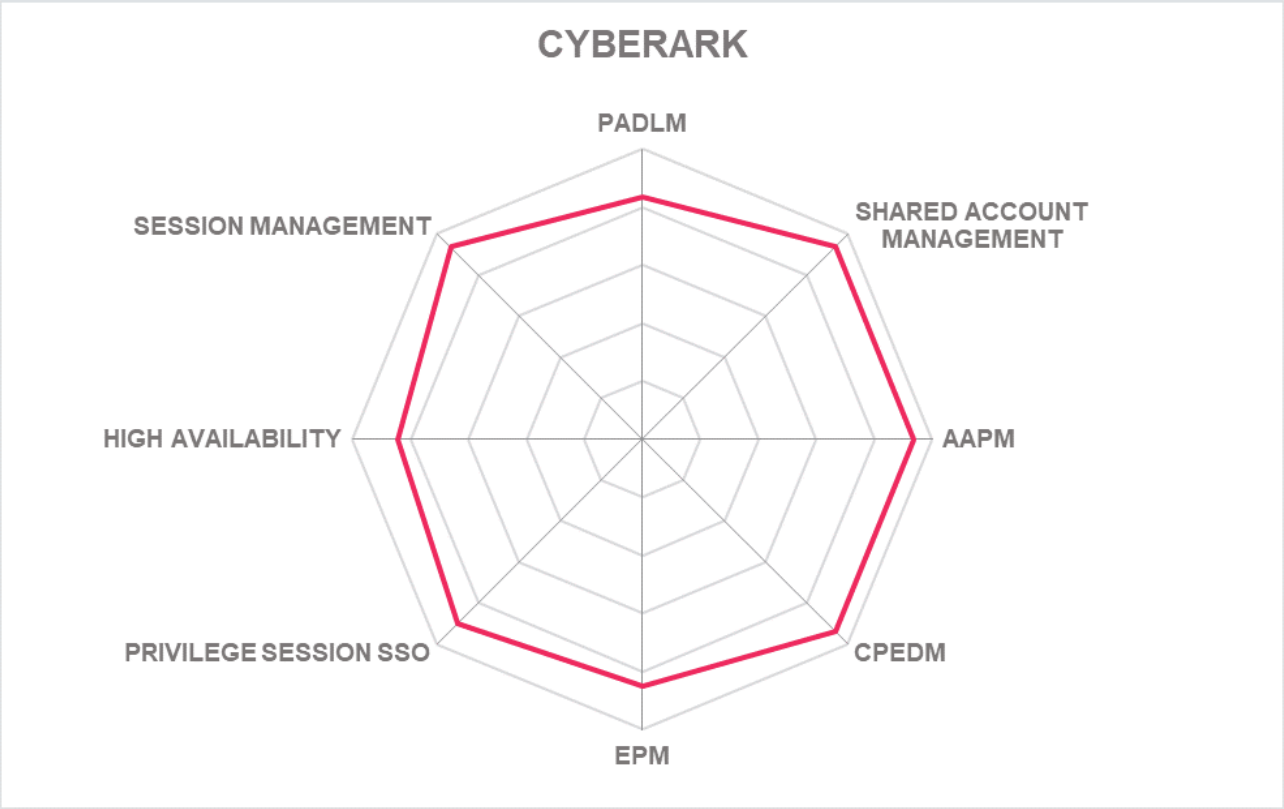

## Strengths

- One of the widest support levels for platforms and deployments
- Has continued to add features in the last year
- CyberArk is a PAM only company which breeds trust for customers along with its history
- Intuitive and robust UI design
- Strong threat analytics capabilities offering real time threat detection and remediation
- Effective DevOps support
- Broad support for cloud applications and infrastructure
- A strong and functional partner ecosystem

## Challenges

- High modularity of solution could be unfavorable for certain deployments
- Complete solution may be overkill for some PAM deployments but PAMaaS is a step forward here
- A SMB focused product would be a good addition

## Leader in


CYBERARK
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.6 Devolutions

Founded in 2010, Canadian firm Devolutions started out by providing remote access solutions to SMBs. It has since added PAM solutions to its portfolio with its Password Server and Password Hub products, serving the same market.

Devolutions offers a PAM solution that is targeted at SMBs and aims to offer the best of enterprise level solutions with an ease of use favoured by smaller organizations. It offers essential features such as a central password and credentials vault which can integrate with Microsoft Active Directory. It also offers account discovery and secure remote access.

The remote access capabilities are broad and support various types of access patterns across a variety of target operating systems. It also comes with good reporting capabilities that provide information about the use of accounts, successful and failed login attempts, login histories per user and accounts, and other information.

The main addition is in network discovery, focusing on identifying privileged (and specifically, shared) accounts across the various systems in a network and putting them under control. Together with the ability to remotely manage target systems running various operating systems such as MacOS, Windows, and Linux, and the password vaulting and management capabilities, this forms a PAM solution covering the essential capabilities required by SMBs, while remaining lean and easy-to-use.

Aside of the central password vaults, there is also an option of having user-specific, private vaults that are only accessible to individual users, for their privileged accounts. In conjunction with the new discovery capabilities, the managed accounts can be automatically identified across the network. Once added to the list of systems and grouped into folders, these accounts can be fully protected by the Devolutions PAM solution.

Being focused on the entry-level of the PAM market, certain more advanced capabilities are lacking, including elaborated session monitoring and recording. However, the base product can be integrated with Thycotic, CyberArk, Centrify and BeyondTrust with Remote Desktop Manager acting as the main PSM with those solutions. Devolutions, as of now, does not offer a cloud variant of the product, which would be attractive specifically to SMBs, but the Password Server can be hosted by a third-party cloud provider of the customer's choosing.

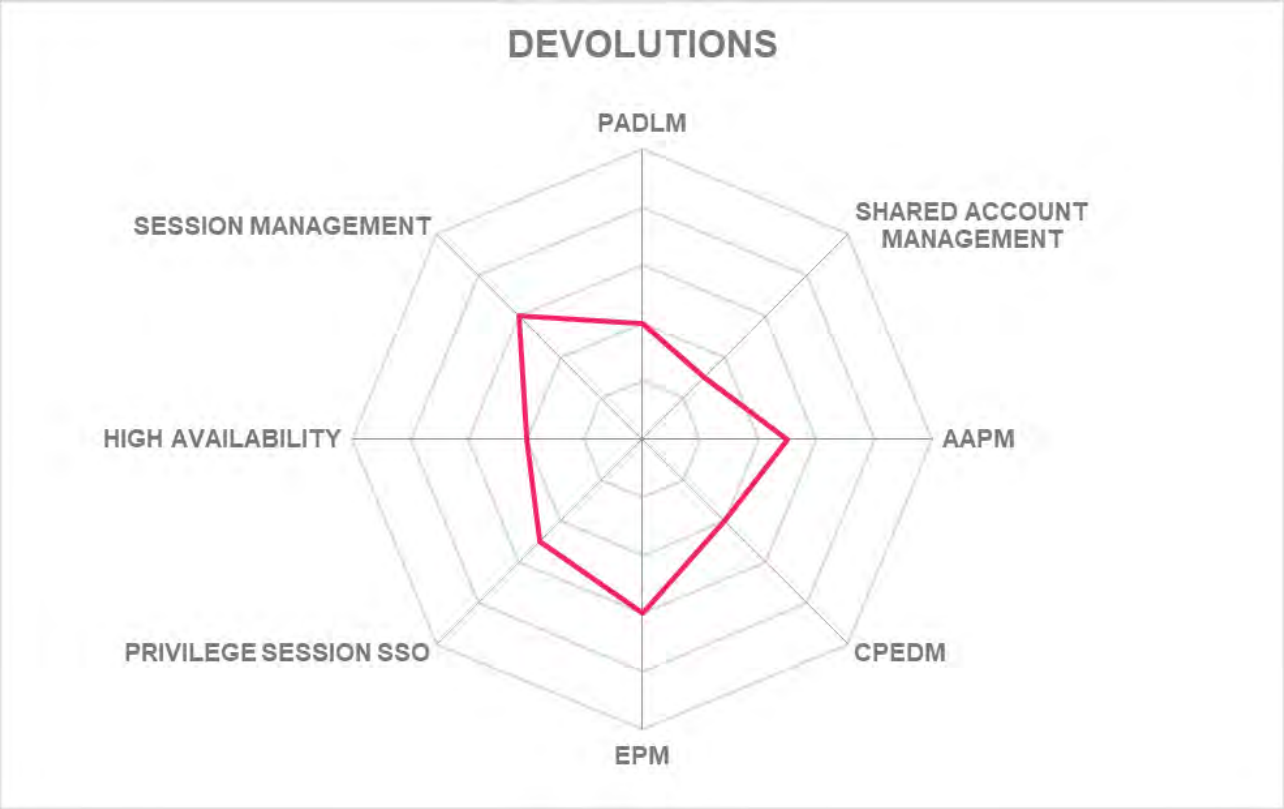
| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Functionality | ● ● ● ○ ○ |
| Interoperability | ● ● ○ ○ ○ |
| Usability | ● ● ● ○ ○ |
| Deployment | ● ● ● ○ ○ |


## Strengths

- Good solid PAM solution for SMBs that understands that sector's needs
- Ease of use and ease of delivery
- Broad remote access capabilities
- Strong reporting capabilities of users and accounts
- Private vaults available for end users provides extra layer of security

## Challenges

- Lacks some more advanced PAM features and currently no scalability option
- On-premises only, no cloud version currently available for modules apart from Password Server
- Limited functionality may restrict market growth into larger enterprise sectors


DEVOLUTIONS
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.7 EmpowerID

Based in Ohio (US), EmpowerID offers several products within its broader IAM portfolio, of which EmpowerID Privileged Access Management (PAM) is its recent addition targeted at managing privileged shared access and session recording and auditing for common access protocols. Largely built on Microsoft technology, EmpowerID offers integration and performance benefits for Microsoft-centric organizations, particularly for existing customers of its user provisioning and identity governance products. EmpowerID has largely focused on large enterprise customers, with 40% of those now in Europe.

The product is completely workflow based which EmpowerID claims is unique. It has a drag and drop creation of forms capability and 1000 ready-made workflows ship with the product to get started. It uses conventional vault technology which hides passwords from users in RDP, SSH or web browser SSO. All privilege sessions are recorded. However, as a complete PAM solution, it only really lacks PUBA as one of the key functions and has good support for AAPM and JIT which is of use to agile environments but not yet DevOps or microservices specific.

MFA support is good and offered through Ubikey Universal 2nd Factor Authentication, Duo Push, knowledge-based authentication (Q&A), and an OATH token server for issuing one-time password tokens. There is also an app for Android and iOS that includes Push, OATH TOTP, Change Password, Forgot Password and Forgot Username.

The interface is good, with an e-commerce like structure which enables end users to add access request to a shopping cart icon. There is also a unique chat bot for help which is a nice touch.

Reporting is good with real-time alerts inform key personnel of critical activities such as privileged account usage, password changes, lockouts, and changes to sensitive group membership. Advanced analytics is less sophisticated although security admins and auditors can view actionable intelligence on the go from their mobile devices or subscribe to reports.

The product does a good job of complimenting EmpowerID's existing IAM products and adds PAM to those. It is basing its development roadmap on Kubernetes and microservices which should make for an interesting development in our next assessment.

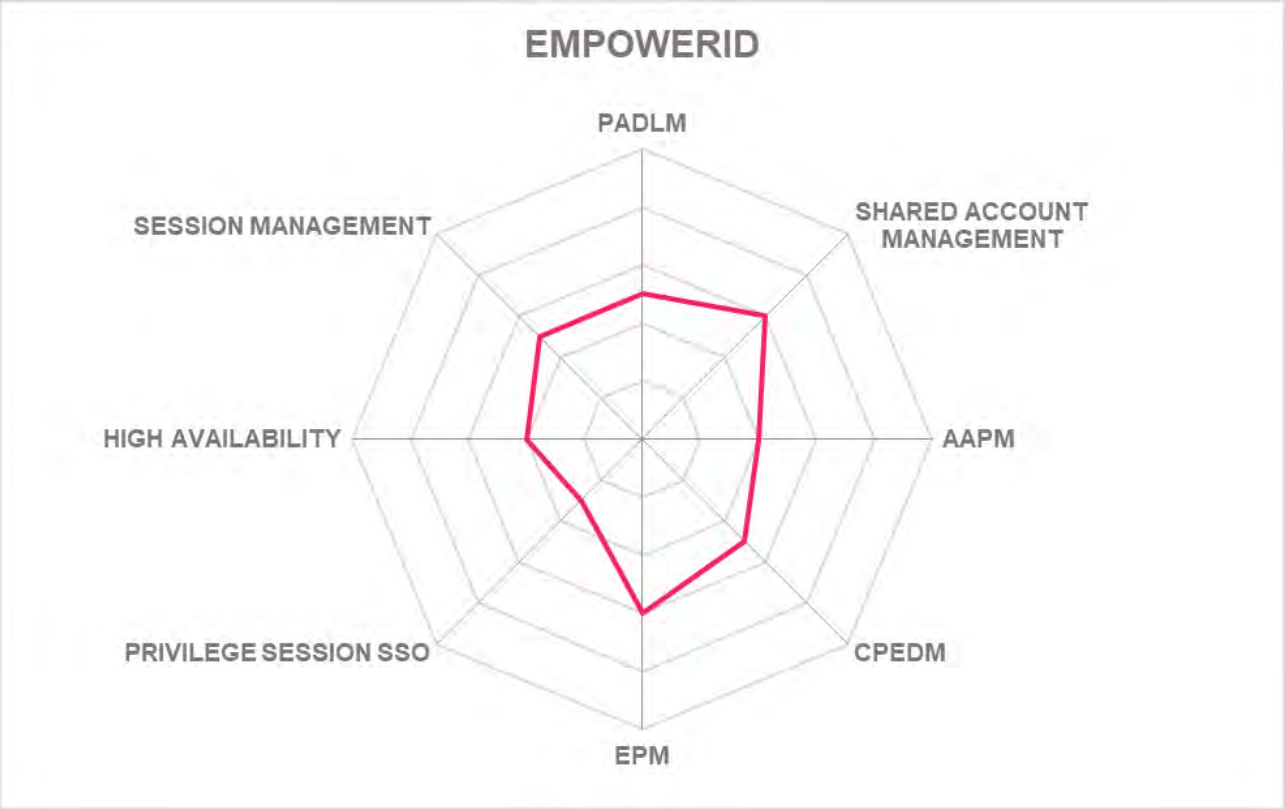
| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Functionality | ● ● ● ● ○ |
| Interoperability | ● ● ○ ○ ○ |
| Usability | ● ● ● ○ ○ |
| Deployment | ● ● ● ○ ○ |


## Strengths

- Good integration with Microsoft technology and organizations that rely on AD
- Innovative and friendly interface with unique shopping cart request feature as well as chat bot for help
- Wide range of MFA support including Ubikey
- Admins can access session data from mobile devices
- Good reporting tools with real time alerts

## Challenges

- Runs primarily on Windows platforms (apart from Linux based session manager)
- Endpoint Privilege Management lacks some features such as whitelisting
- Will benefit from DevOps and microservices development


EMPOWERID
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.8 Fudo Security

FUDO Security, with offices in California and Poland was founded in 2012. It offers FUDO PAM as its primary PAM product in the market. FUDO Security has an install base across North America, Europe and Middle East.

As befitting a relatively young product, it has a modern and crisp interface and allows a good degree of customization with drag and drop and resizable tiles available, a little like Windows 10. The same customization can be used for data presentation – useful for reporting and pattern management.

The company believes that session management is the most important part of PAM, which explains why this solution is basic with only a password manager and session manager. That does not mean it is not competent, however. The session manager is a good one; it supports HTTPS recording of user's interaction with web services as well as RDP, VNC.
SSH and Telnet. Password management offers password changes through pre-defined scripts and in-house plug-ins can be used to automate password management to a degree. External user password can be created by hand or standard LDAP password.

FUDO claims support for JIT access but this is really pre-assigning time frames for access to privilege accounts. It does supports SIEM including ArcSight and Splunk but there is much missing from this solution in terms of PUBA, AAPM and PADLM which would rule it out for many customers although its well thought out interface and limited machine learning tools that can detect unusual behavior will appeal to some smaller organizations. Its claimed one-day deployment time may be possible due to its compact self-contained appliance footprint, but real-world delivery times will clearly depend on circumstance and skill sets.

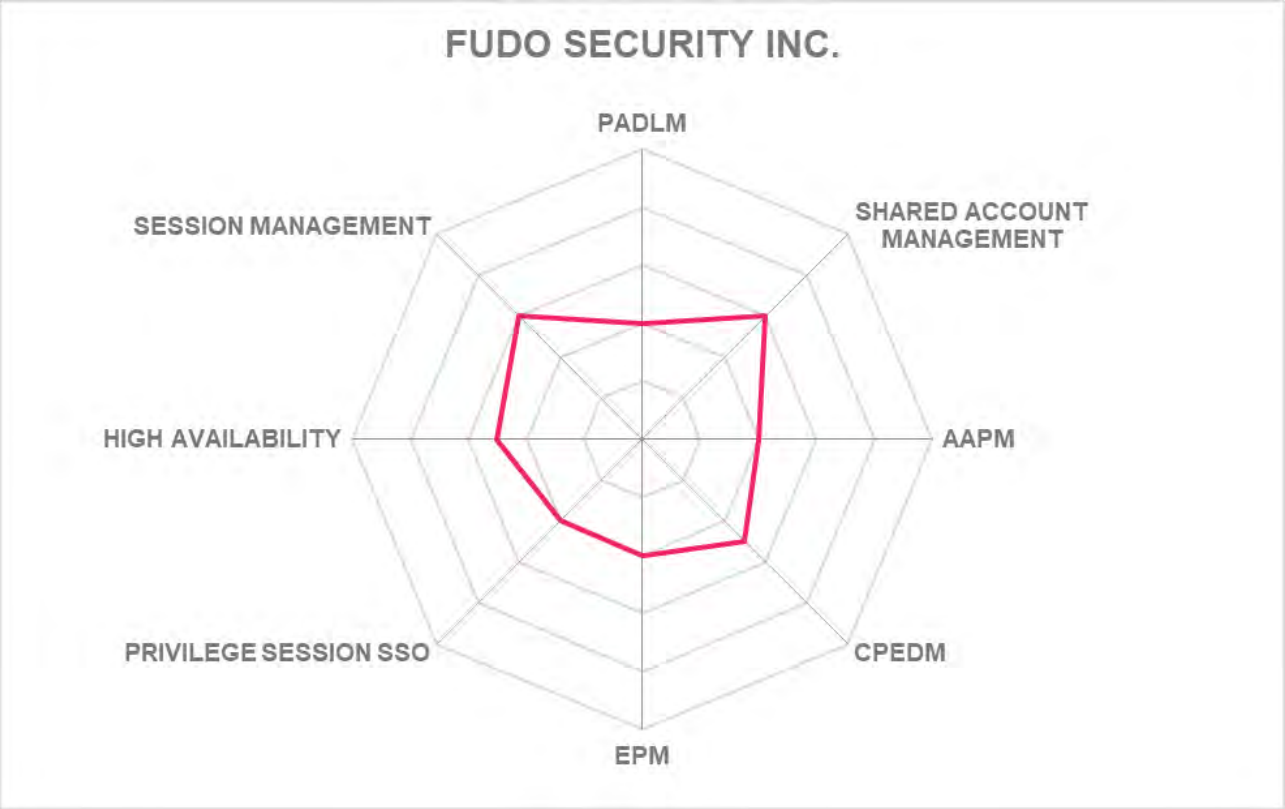
| | |
|---|---|
| Security | ●●●○○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●○○ |
| Usability | ●●●●○ |
| Deployment | ●●●●● |


## Strengths

- Crisp design, drag and drop customizable interface
- Strong SRM and PSM functions
- Appealing to smaller organizations looking for compact solution that does the basics well
- Appliance and agent less based delivery offers faster deployment and configuration, no agents
- Feels modern and should lend itself well to future development

## Challenges

- A little feature light, needs more critical capabilities to succeed in wider market
- Lack of support for cloud platforms and DevOps
- Limited partnerships and interoperability with 3rd party security tools


FUDO SECURITY INC.
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.9 Hitachi ID Systems

Hitachi ID, headquartered in Canada, is a global IAM software provider that originated as MTech Information Technology and acquired by Hitachi in 2008. It offers HiPAM as its primary offering for the PAM market and claims 14m licensed users in North America, Europe and APAC.

The product consists of three modules: an identity manager, password manager and an access manager. So far, all quite normal. It has 2FA and federated access built into the password manager. Like other solutions in the Leadership Compass Hitachi is aware of the risks of shared passwords and accounts and static accounts being left open. Single Sign On is supported and admins can check out multiple accounts in one request. APIs are used to replace embedded passwords and to enable DevOps and similar tools to onboard and deactivate managed PAM endpoints.

Hitachi ID HiPAM supports either direct connection to endpoints or via a proxy while users' access to the solution is via a direct UI, or web proxy or via HTML5. Endpoints are connected behind the walled garden of Hitachi ID HiPAM and mobile users use an iOS or Android app and access via proxy service. Session recording allows recording with confidential information such as social security numbers to be redacted – good for GDPR. There are 2 levels for authorization for viewing – not all vendors consider the compliance aspects of session recording and monitoring like this.

A strength is the disaster recovery features – better than most PAM vendors and not something that you would normally expect – and high availability features that offer real time data replication, and active-active architecture and data that is geographically distributed. Hitachi ID HiPAm also offers multiple copies of the vault and access manager in different cities or continents. A highlight of the interface is the "recent" button which, like Microsoft Office applications, allows users and admins to rapidly open previous requests and sessions.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●● |
| Usability | ●●●●○ |
| Deployment | ●●●●○ |

Hitachi ID

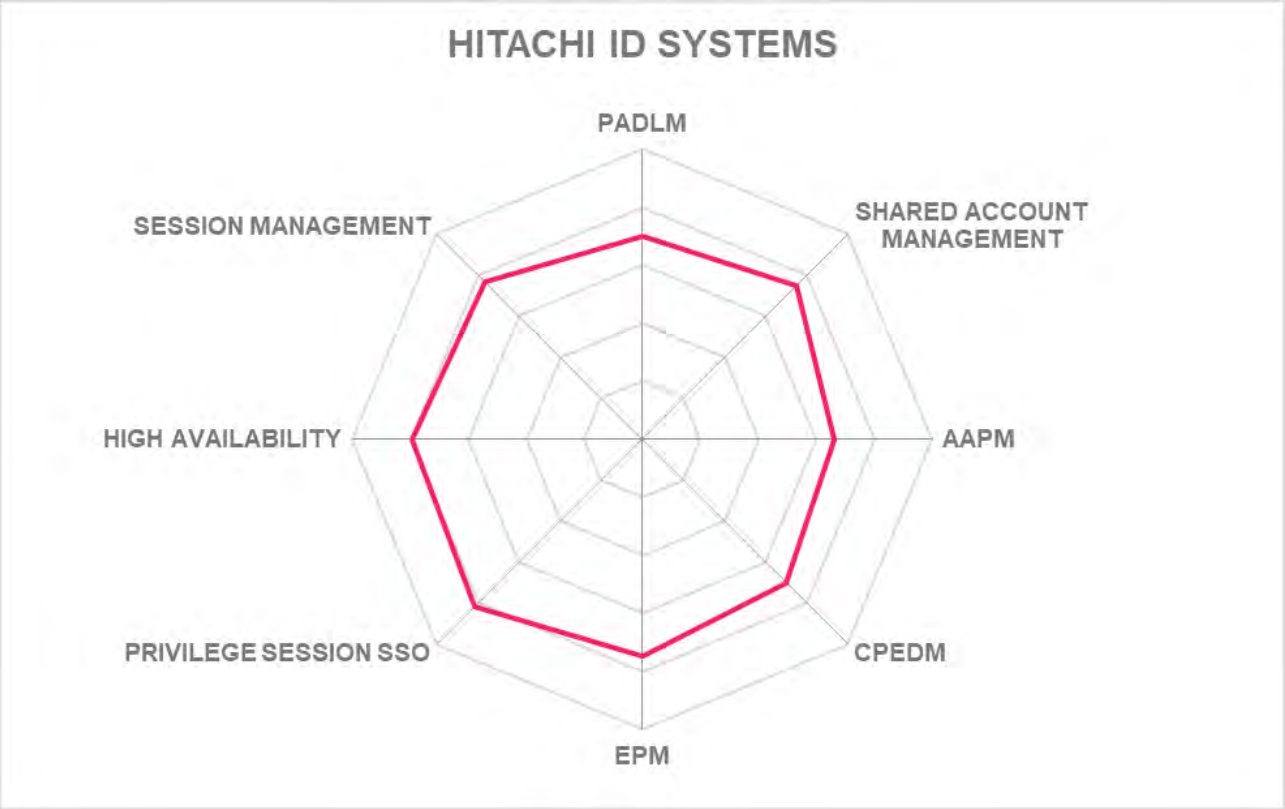
## Strengths

- Strong contextual support for API/ service authentication
- Clear interface with unique "recent" button
- An active-active architecture supporting High Availability
- Built-in 2FA for authentication
- Detailed account discovery and provisioning support
- Strong disaster recovery tools which are unusual in this sector
- Redaction of personal data in session recording
- Access certification capability of Hitachi ID Identity Manager is included at no additional cost

## Challenges

- Limited CPEDM capabilities
- Lack of an effective sales and marketing machinery
- OOB connectors for cloud applications are limited but growing
- Limited partner ecosystem impacts market outreach and growth

## Leader in


HITACHI ID SYSTEMS
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.10 Krontech

Based in Turkey, Krontech is the technology arm of Kron, a telco firm publicly listed on the Istanbul stock exchange. Krontech offers its Single Connect PAM suite that comprises of several modules aimed at managing privileged access. A relatively new entrant in the market with its first product launch in 2013, Krontech's business mostly comes from Europe, followed by North America, Canada and Asia.

Unusually, Single Connect has a built-in MFA manager called the Unified Access Manager which also includes support for SSO. The Data Access Manager supports video recording and can enforce policy at the query level. The product can be accessed as a desktop client, web app or via a mobile app. While also supporting Putty, it features token based application to application password management. All sessions are recorded as MP4 files while there is good support for SIEM integration. In terms of interface, some work could be done to match the leaders in the field as parts of the UX remains very "admin" like and quite dated in our opinion. There is support for CPEDM, PUBA and PADLM which should be expected at this level of PAM solution. Supported third parties include Duo and Okta and management of access to cloud applications is supported on AWS, Azure and Google.

With easy to use SAPM and PSM capabilities, Krontech Single Connect may appeal to small and mid-size businesses (SMBs) with a need for routine task elimination by privileged task automation, thereby accelerating leaner privileged operations. That said the company has a large number of large enterprise customers. Single Connect Data Access Manager is the module targeted at privileged database access and enables activity monitoring for privileged database sessions. This allows for managing DB admins roles and assigned DB privileges with granular command control and dynamic data masking. Single Connect Privileged Task Automation (PTA) Manager is targeted primarily at Telecom service providers and allows for better operational efficiency by delegating tasks instead of privileges and automating routine privileged operations.

This undoubtedly is a powerful solution that does all the essentials but misses out on more advanced features that more organizations need. It will present a steep learning curve and Krontech needs to update its user interface. Later in 2020, Single Connect will be rebranded as Ironsphere with a rollout beginning in the US but the product will remain technically the same. The future roadmap includes PAMaaS and an Ai based anomaly detection tool, according to the company.

| | |
|---|---|
| Security | ● ● ● ● ○ |
| Functionality | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ● ○ |
| Deployment | ● ● ● ○ ○ |

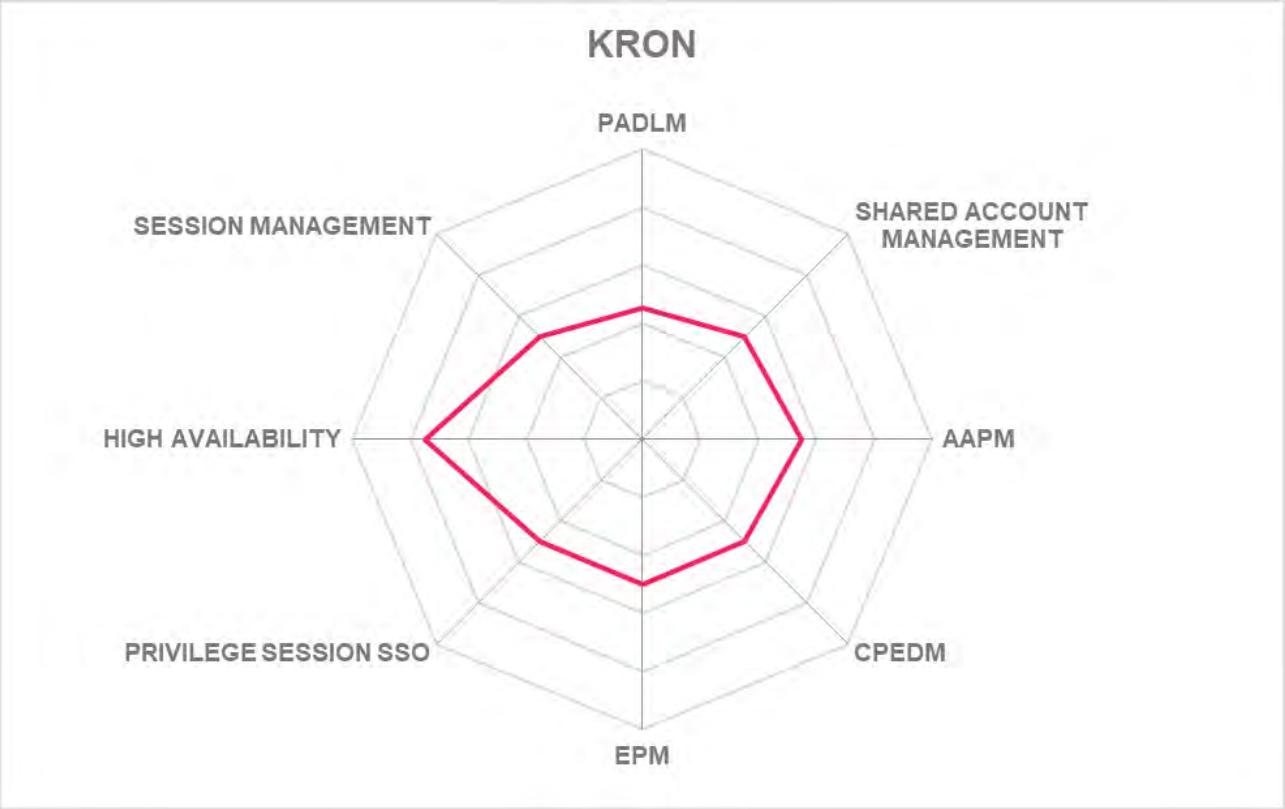
Single Connect™

## Strengths

- Separate modules for distinct PAM functions, integrated under a common PAM platform
- Good market and technology understanding
- Good UI design for enhanced UX
- Strong support for database administrative privileges
- Early and effective emphasis on privileged task automation
- Support for limited but most commonplace IaaS platforms

## Challenges

- Misses some advanced features and needs to update its UX
- Relatively new entrant in an established market still needs to make its mark against leaders
- Corporate telco background tends to favour telco customers currently


KRON
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.11 ManageEngine

Headquartered in Pleasanton, US, ManageEngine is a part of the India-based Zoho Corporation founded in 1996. PAM360 is the company's main offering to the PAM market and offers key functionalities in an integrated modular fashion.

PAM360 comprises tools for PAG, access management, session management, PUBA, SSL and SSH key management and workflow automation. Account discovery works across Windows, Linux, Network devices and databases. Session management masks passwords from users while launching RDP, VNC, SSH and SQL sessions. All session can be recorded.

ManageEngine benefits from machine learning capabilities now added to its PUBA functions which assists with user behavior patterning to detect anomalies. The interface for PUBA shares the same modern look as the rest of the solution and delivers a high level of risk scores including current high-risk servers, current high-risk users and total number of anomalies. A highly useful resource for admins which offers drill down into more granular data on users.

There is a good standard of SSH and SSL certificate management with periodic key rotation and enforcement to remove existing unused keys or to deploy a new key pair, leaving the existing keys undisturbed. There is also integration with Microsoft CA, root CA or third-party CA's such as GoDaddy, and Verisign LetsEncrypt. ManageEngine makes a play of its "smart" workflow automation and there is credibility to this with integration with Automation Anywhere and integration with ITSM ticketing systems such as ServiceDesk Plus and Service Now. On a more fundamental PAM issue, PAM360 offers strong SIEM integration with Splunk, SumoLogic and Log360. DevOps is covered up to a point with integrations for Jenkins, Ansible, Chef and Puppet.

Reporting is strong too, with reports available to meet checks on PCI-DSS, NERC, ISOx and GDPR. Although not essential for many customers, ManageEngine's provision of customization in the product is welcome for those organizations that want to create custom fields for end points or users for example, as well as attach files. There is separate pricing for Enterprise and MSPs.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●○○ |

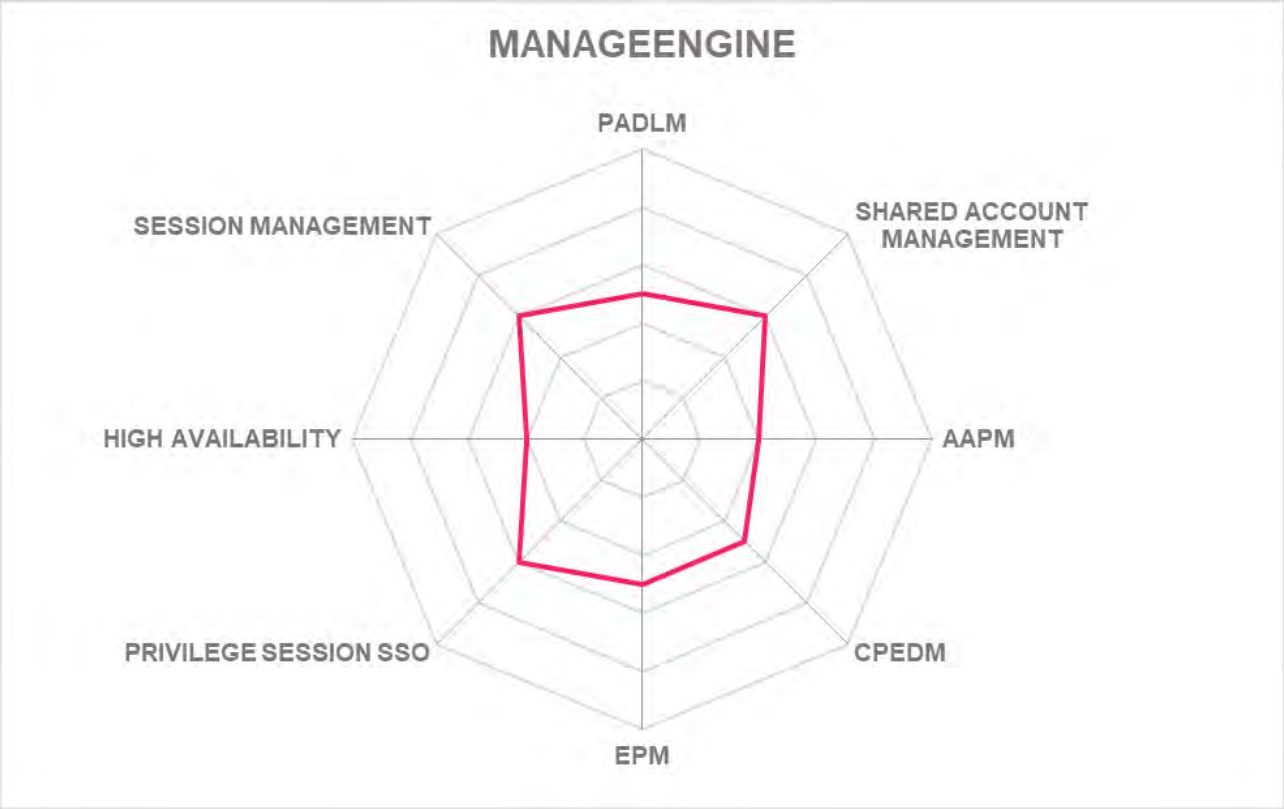
ManageEngine

## Strengths

- PUBA tools very good with machine learning now added to functionality
- Customization tools are welcome at this level
- Strong auto discovery capabilities and risk-based scoring system for activities
- Integrates well within broader security and IT software portfolio
- Reasonable pricing and easy licensing arrangement
- Strong integration with digital workflow management tools

## Challenges

- Only available in an on-prem software delivery format
- Lack of integration with IGA tools
- Lack of connector support for cloud applications and cloud-based delivery


MANAGEENGINE
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.12 Micro Focus

UK based Micro Focus has seen some tribulations in recent years following the not so smooth acquisition of HPE's former software assets. The company remains a player in the PAM market and has reverted to the NetIQ brand for its PAM platform - NetIQ was an earlier acquisition by Micro Focus.

Whatever else Micro Focus is doing, it has not to date done much with its PAM product which is a disappointment. Many of the features its claims as unique are not: it is not the only solution with a customizable drag and drop interface (welcome though that is) or 100 percent keystroke logging and video capture of all credential-based environments.

NetIQ has the basics of PAM: discovery, vault, session management and recording and includes some more advanced features: AAPM, EPM and SIEM which has been boosted by the strong addition of ArcSight that came with the HPE acquisition. There is as yet no support for DevOps, however. The only mention of JIT is the ability to terminate suspicious activity "just in time". All of these are likely to function efficiently as they are tried and tested technologies from the old NetIQ stable but there needs to be more in 2020 – particularly from a vendor with the resources of Micro Focus.

It at least has some degree of machine assisted analytics to support audit and investigation functions of PAM. It does offer a gateway approach to privileged access and supports privileged session management across a variety of systems including enterprise business applications such as SAP, databases and popular SaaS applications. Overall, while still a good PAM solution, it feels like the product has not been developed since our last Leadership Compass and is in danger of falling behind a little - this would be a shame given the legacy value of the NetIQ brand.

| | |
|---|---|
| Security | ● ● ● ● ○ |
| Functionality | ● ● ● ● ● |
| Interoperability | ● ● ● ○ ○ |
| Usability | ● ● ● ○ ○ |
| Deployment | ● ● ● ○ ○ |

MICRO FOCUS®

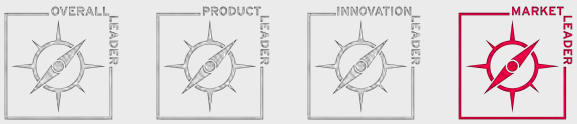
## Strengths

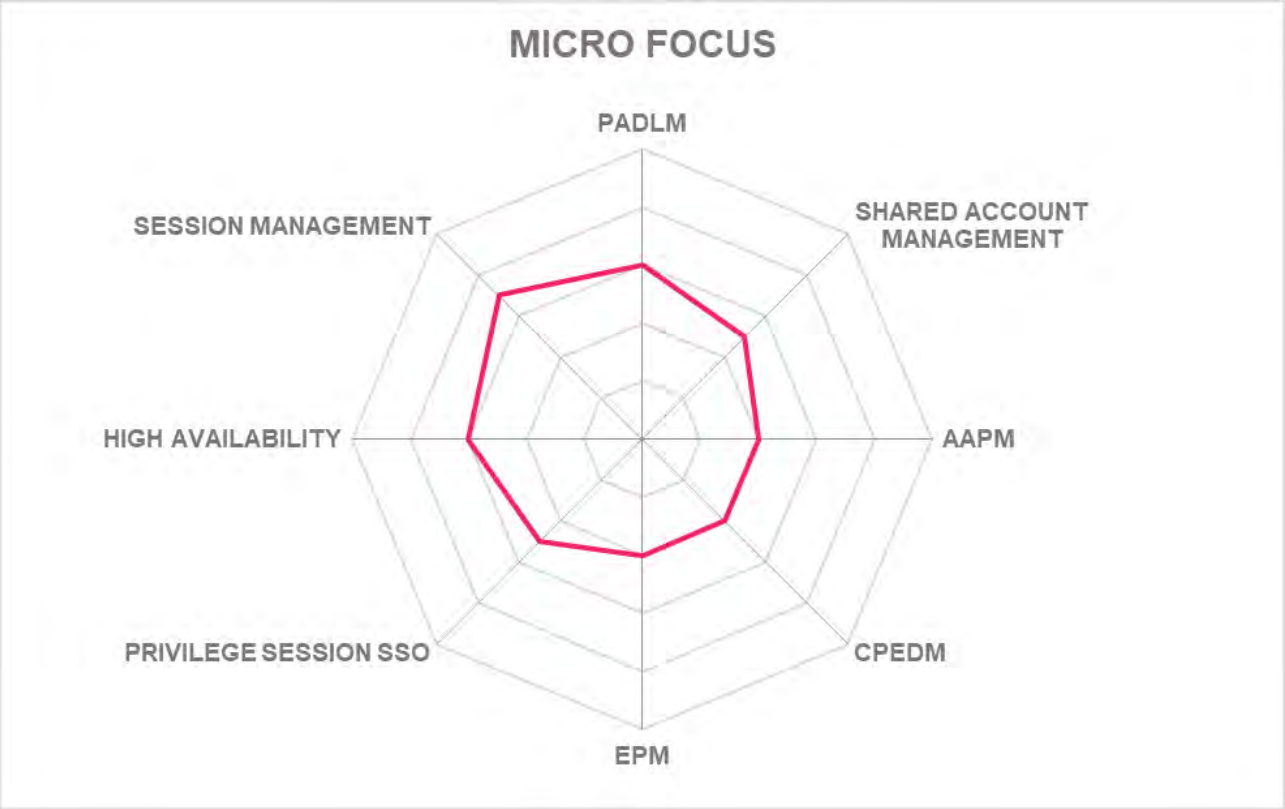
- Good for organizations that already adopt other NetIQ IAM products
- Strong basic PAM solution for enterprises
- Support for SAP and other major database platforms
- Reliable and trusted solution for its basic capabilities
- Retains a good interface with user friendliness
- Financially Backed by a large enterprise software vendor

## Challenges

- The product would benefit from DevOps and other digital capabilities
- Marketing and product stories need sharpening: zero trust is not a feature, for example
- Product feels a little unloved by its new owners, needs robust development to keep up with leaders

## Leader in




MICRO FOCUS
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.13 One Identity

California-based One Identity, which specializes in IAM solutions also offers a good range of products that fulfill the fundamentals of PAM. It provides its Safeguard PAM solution for password management, session management, and analytics. In addition, the company provides additional PAM capabilities for Unix/Linux AD bridging and privilege delegation.

The platform itself consists of Safeguard for Privileged Passwords, Safeguard for Privileged Sessions and Safeguard for Privileged Analytics for vaulting, session recording and analytics. There is also Privilege Access Suite for Linux, Privilege Manager for Windows (for Windows PEDM and endpoint control) and for Windows AD PEDM, One Identity provides its Active Roles product. Safeguard for Privilege Analytics tracks user activity in real time and compares activity to session data collected from the wider IT environment. Safeguard for Privileged Passwords grants role-based access with automated workflows designed to speed up provisioning and authentication. Administrators can sign into the tool from a web browser with support for mobile devices while the tool is itself protected by two-factor authentication further enhancing security.

All of One Identity's solutions offer an easy to use dashboard interface to control specific settings and task loads. The product can be implemented as a protocol proxy so that minimal changes are required to the network and monitoring, recording, and analysis of privileged sessions is achievable without having to onboard any assets. Session activity can be captured via keystroke, mouse movement and windows viewed. All sessions are recorded as video and stored in a secure, searchable database.

One Identity offers CPEDM and AD Bridge products as installable client packages Available in installable client package, Privileged Access Suite for Unix (PASU) is a comprehensive suite delivering Unix-AD bridging, authentication, root delegation (SUDO enhancement) and a centralized management of policies across Unix-based systems. Privilege Manager for Windows offers CPEDM capabilities for Windows-based platforms. Another key product, Active Roles, provides privileged account management for on-premises and hybrid AD environment. Finally, SIEM support is delivered with support for market leaders Splunk or Micro Focus ArcSight and MFA comes courtesy of One Identity Defender or via plug-ins for RSA, Yubico, Okta and Duo.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●○ |

ONE IDENTITY

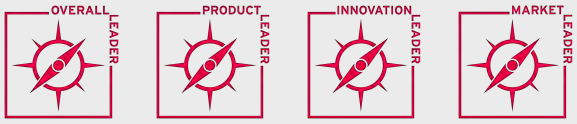
## Strengths

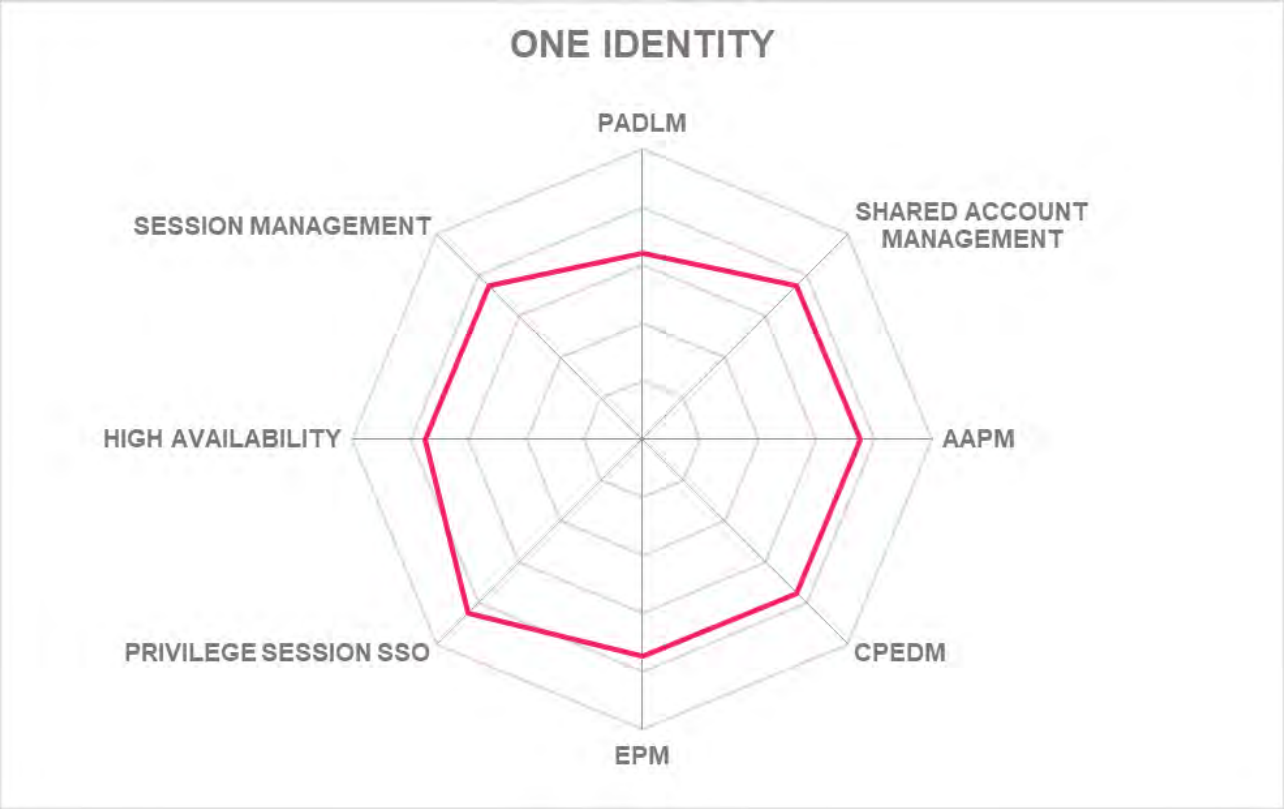
- Easy to use interface shared across all modules with support for CLI and GUI
- Easy for growing organizations to deploy and scale
- Simple integration with One Identity IAM products will appeal to organizations already invested in the ecosystem
- Good support and back up from long established firm

## Challenges

- Does not yet feature a dedicated DevOps tool within its suite
- No support for PAMaaS currently which would be good addition
- Limited support for SaaS applications with only SAP Hana and AWS currently on the list

## Leader in




ONE IDENTITY
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.14 OnionID

Onion ID which has offices in the US and India specializes in PAM solutions for cloud applications, servers, hosted databases, containers, APIs, and secrets. The company claims to put the emphasis on making PAM transparent and easy to use.

Onion ID is compatible with AWS, GCP and Azure for those customers who wish to run it in the cloud. It supports SSO to authorized systems, rule based privileged escalation, CPEDM and of more interest to future applications it supports API authentication, JIT and ephemeral accounts. Support for major SaaS applications is strong with SFDC, Workday, Google G-Suite, O365 and SAP Hana all included. However, what makes Onion ID stand out is its support of DevOps tools including GitHub, Docker, Kubernetes, Puppet and Ansible. Another key feature for modern PAM running in more digital environments is broad based support for AAPM and here Onion ID also does well with strong support for programming languages (including JavaScript) and access to both API and CLI protocols. On a more fundamental level, Onion ID also has provisioning for CPEDM, EPM and PUBA capabilities.

Just in Time provisioning is supported in its truest sense by giving admins the power to grant immediate access to a user and then kick them off after use. JIT access activity is also recorded through the standard session recorder module. Third-party integrations include Splunk and Sumologic for SIEM and log management purposes and there is also integration with vulnerability management tools.

The user interface is up to date with easy access to information and customization and single pane of glass access to user activity for admins. Biometrics are used to replace one-time passwords speeding up one part of the privileged access process. Onion ID also allows admins to provide shared access to employees with a single click. An agent less onboarding process can be done directly on the dashboard.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●○○ |

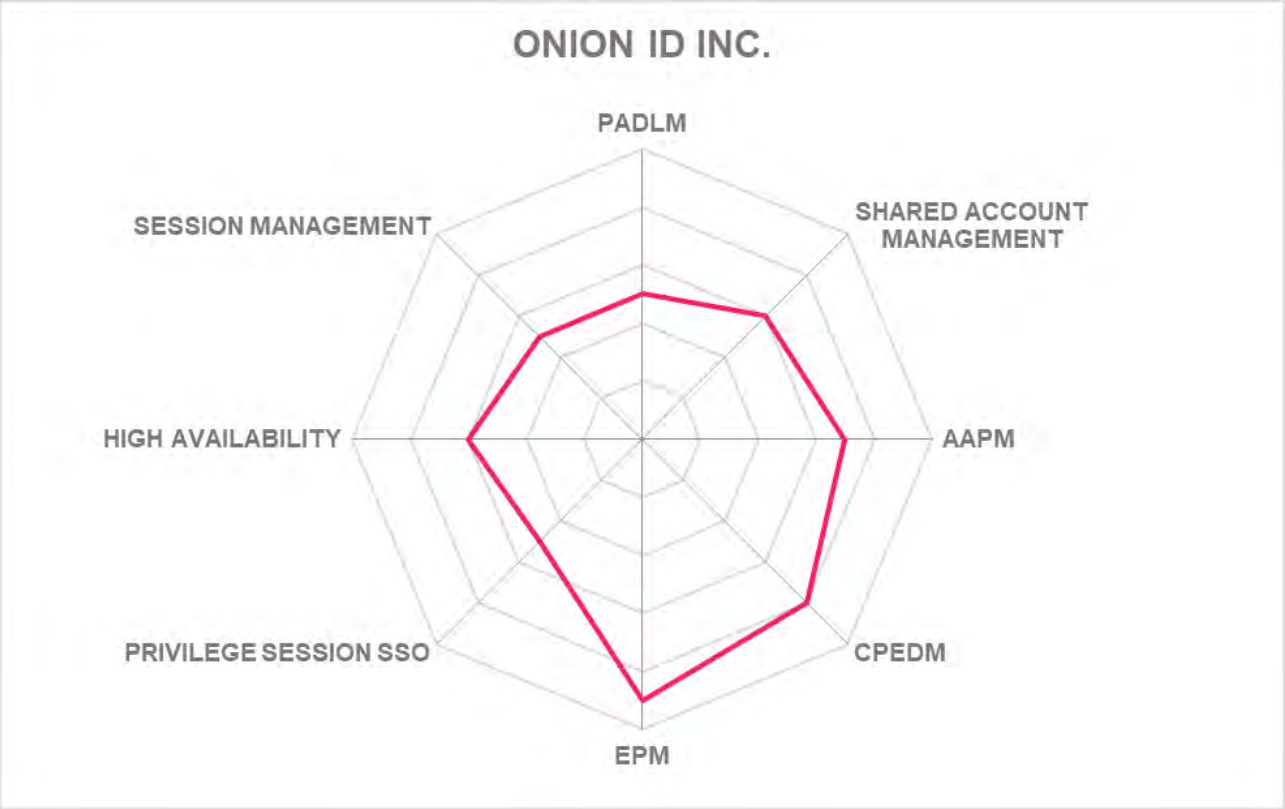
Onion ID

## Strengths

- Excellent interface design and admin tools
- Software design has really thought about ease of use and making PAM suitable for digital and agile environments
- Strong support for DevOps applications
- Good, practical use of biometric access
- Just in time capabilities are on the mark
- Feels modern and highly capable

## Challenges

- Cannot view hard-coded credentials in scripts in session auditing and recording
- No support for third-party User Behavior Analytics as yet
- Technical support could be more localized to NA and Europe


ONION ID INC.
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.15 Osirium

Based in the UK, Osirium offers a range of Privileged Access solutions. This includes basic PAM that includes session management, task management and behavior management. The company added PPA (Privileged Process Automation) in 2019, which it describes as a framework for automating privileged IT and business processes traditionally requiring expert skills and PEM (Privileged Endpoint Management), to reduce risk by removing local administrator accounts and cut down the IT help desk load.

Osirium's approach to PAM is to move from giving users access to passwords and instead focus on a role based or task-based approach instead. It is an approach that in the age of digital transformation and ever-increasing numbers of users wanting privilege access to accounts and may well become more common among other vendors – but some customers will always prefer the safety of a vault. However, task-based access is useful for routine admin tasks such as maintenance and software updates for example and the Osirium solution keeps credentials hidden from users.

The PPA solution is provided for routine tasks as well as more complex IT tasks. Osirium is confident that the solution can cope with the risk of automating IT tasks because of its role-based approach and the fact that credentials are always hidden. Certainly, this reduces risk but does not eradicate risk.

Osirium's task-based approach can eliminate the need for CPEDM through the packaging of elevated privileges in a pre-defined task and allowing for task delegation. With a range of in-built templates for pre-configured tasks and broad protocol support, tasks can be executed against a variety of devices and interfaces. Endpoint management is supported by removing local admin accounts and removing some of the threat of rogue access from the endpoint and stops upload of non-whitelisted applications.

Osirium also offers an entry level PAM product called PxM Express which has basic PAM capabilities but on free licence for up to 10 servers. A solution that smaller organizations may find worth looking at for basic PAM without full commitment.

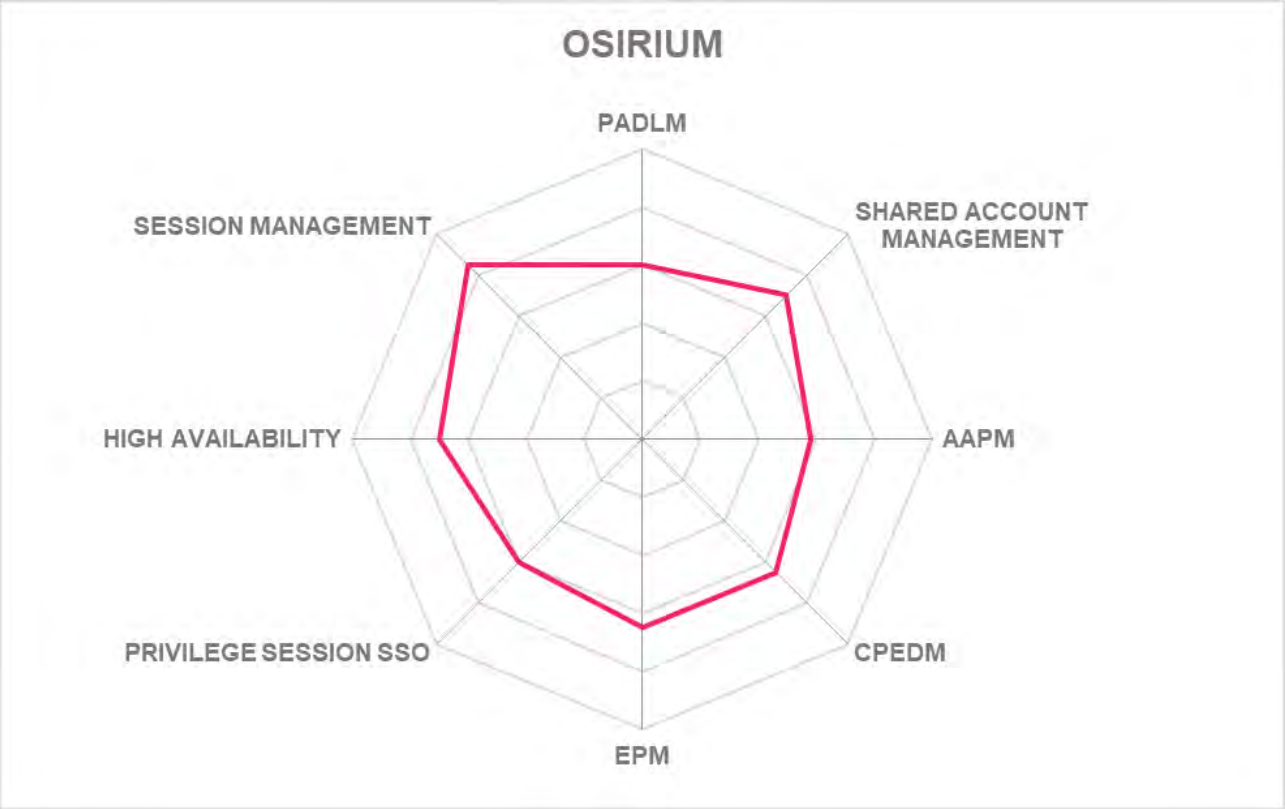
| | |
|---|---|
| Security | ● ● ● ● ○ |
| Functionality | ● ● ● ● ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability | ● ● ● ● ○ |
| Deployment | ● ● ● ○ ○ |


## Strengths

- Role-based model promises convenience and efficiency
- End user friendly and role-based access give users confidence to carry out IT tasks normally reserved for IT admins
- Good value entry level product available
- Applications can be elevated instead of users
- Local admin accounts are removed, reducing attack points in EPM

## Challenges

- Some organizations will still want the assurance of a vault at the centre of PAM
- Osirium may struggle to convince market of its task-based approach
- Lacks the marketing muscle to compete with the biggest players despite innovative approach


OSIRIUM
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.16 Remediant

Based in San Francisco, Remediant is a single product PAM company founded in 2013. Its SecureONE product uses agent-less and vault-less technology at the core of its approach to PAM. Remediant has created a PAM solution that provides JIT access for ALL privileged accounts, abolishes shared accounts and stores no credentials at all - quite bold. The fact that Remediant has acquired some key, highly security minded customers says something for this approach. In theory, the advantage of this approach makes auditing and session management easier as there is a single source of distribution to monitor and with no stored credentials there is less risk of theft.

It also supports role-based access control as well as attribute access control – however it lacks dedicated support for some more traditional advanced PAM capabilities such as AAPM. This is where pure JIT may fail for larger organizations that still need to vary privilege access safely. An agent less approach to endpoint access also lowers risk of third-party breaches and speeds deployment times – which already promise to be quite rapid due to the small footprint of Remediant SecureONE. The company claims that 100,000+ endpoints can be managed within 2 hours. All access is backed up with integrated 2FA technology.

While Remediant is focused on marketing an integrated JIT privilege access management solution, it also covers the basics well. It supports all major operating systems across desktops and servers and is available on cloud, on-premises or hybrid. For DevOps, it provides Restful API support and directory bridging. As for High Availability SecureONE supports HA, DR and HA+DR configurations. It can support HA configurations with up to 4 node fault tolerance. It supports integration with several SIEM systems.

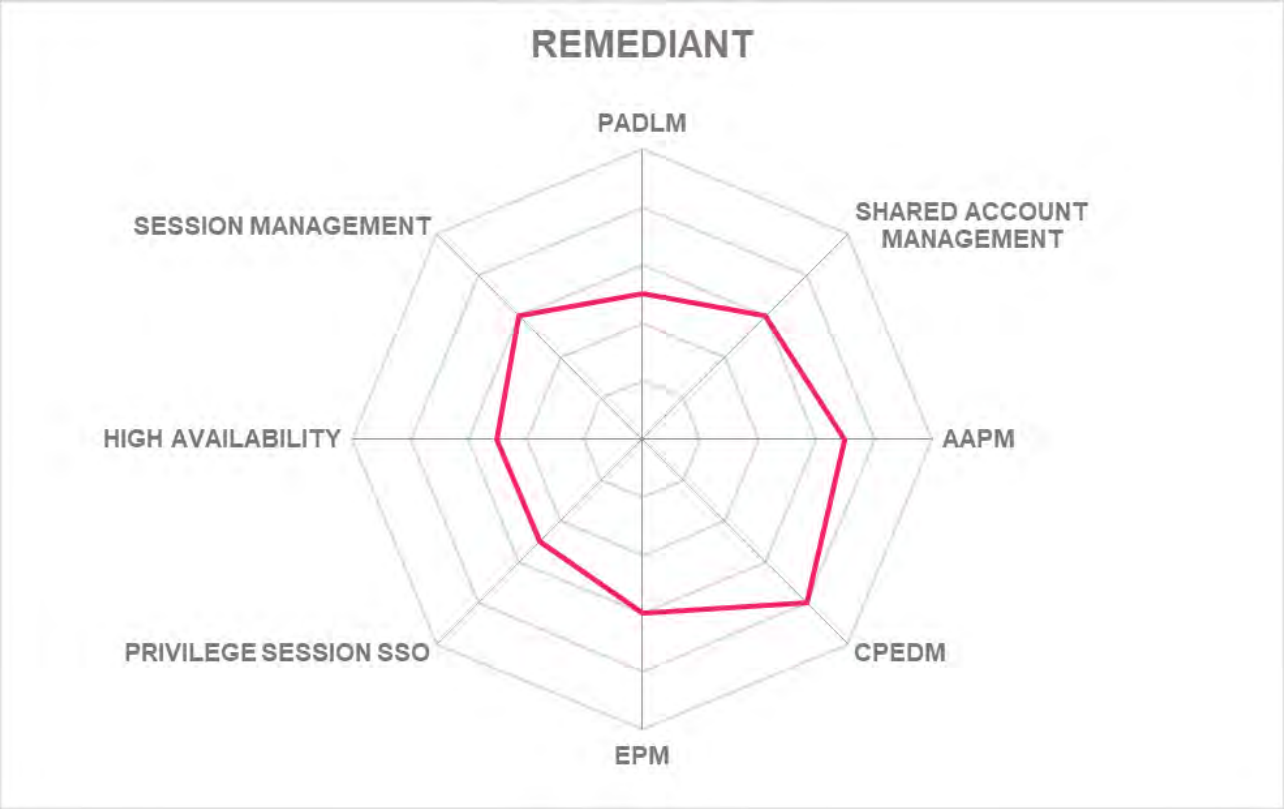
| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Functionality | ● ● ● ○ ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability | ● ● ● ● ● |
| Deployment | ● ● ● ● ● |


## Strengths

- Theory of agent less and vault less operation makes sense and will appeal to some organizations
- Simple to install with modern interface
- Basic solution that does a good job of access control and management
- Role-based access control
- Potentially the basis of a future leading PAM solution

## Challenges

- Needs stronger support for functions such as PADLM and SAM
- Needs wider DevOps support
- May deter some organizations who still like a vault-based solution and a more traditional approach to PAM functions


REMEDIANT
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.17 Sectona

Founded in 2017, Mumbai (India) based Sectona is one of the youngest of PAM market entrants and sells Spectra PAM as its PAM solution. Sectona is funded by its initial founders and has raised angel investments to support its ongoing operations. Having done well to secure some 100+ customers in the Middle East and India the company is looking to grow in Europe and North America.

Sectona describes its Spectra solution as ideal for hybrid environments with authentication available from any browser, OS or Sectona's own client and offers access to privileged sessions over any HTML5 supported browser from any platform without the need of agents or plugins to be installed. It is not restricted to hybrid environments however with customers deploying on cloud or on-premises as well.

Its prime tasks are Discovery and User Management. Spectra can automatically onboard assets across AWS, Azure, VMWare and network discovery. It offers some degree of automation: deprovision privilege accounts without admin involvement as well as automate Privilege Task Management. It can also automate policy assignment with a hybrid discovery process. Automation, done well, is likely to become more important to PAM in the coming years.

Spectra offers an in-built Plugin Designer Kit (PDK) that allows customers to develop their own connectors to facilitate PSM and SAPM for non-standard applications and does not require extensive coding experience thereby avoiding development costs. Spectra's major strength is the PSM technology that offers access to privileged sessions over any HTML5 supported browser from any platform without the need of agents or plugins to be installed.

It's up to speed with features such as Adaptive Authentication which will become more common on PAM in the future as well as application to application password management by using APIS and SSKs for many platforms. It is well positioned then to manage DevOps and containerization demands in the future. Given how the short time that has elapsed since the company was founded, it is maturing at an impressive rate. It has certainly grown its support of third-party applications – now numbering 150 – including support for MFA from Okta DUO and OneLogin among others.

A highlight of the platform is the Session Risk scoring for threat analysis which gives an at-a-glance view of performance against pre-existing security and data theft categories. Sectona also offers an MSP edition of Spectra aimed at IT service providers to offer managed PAM services.

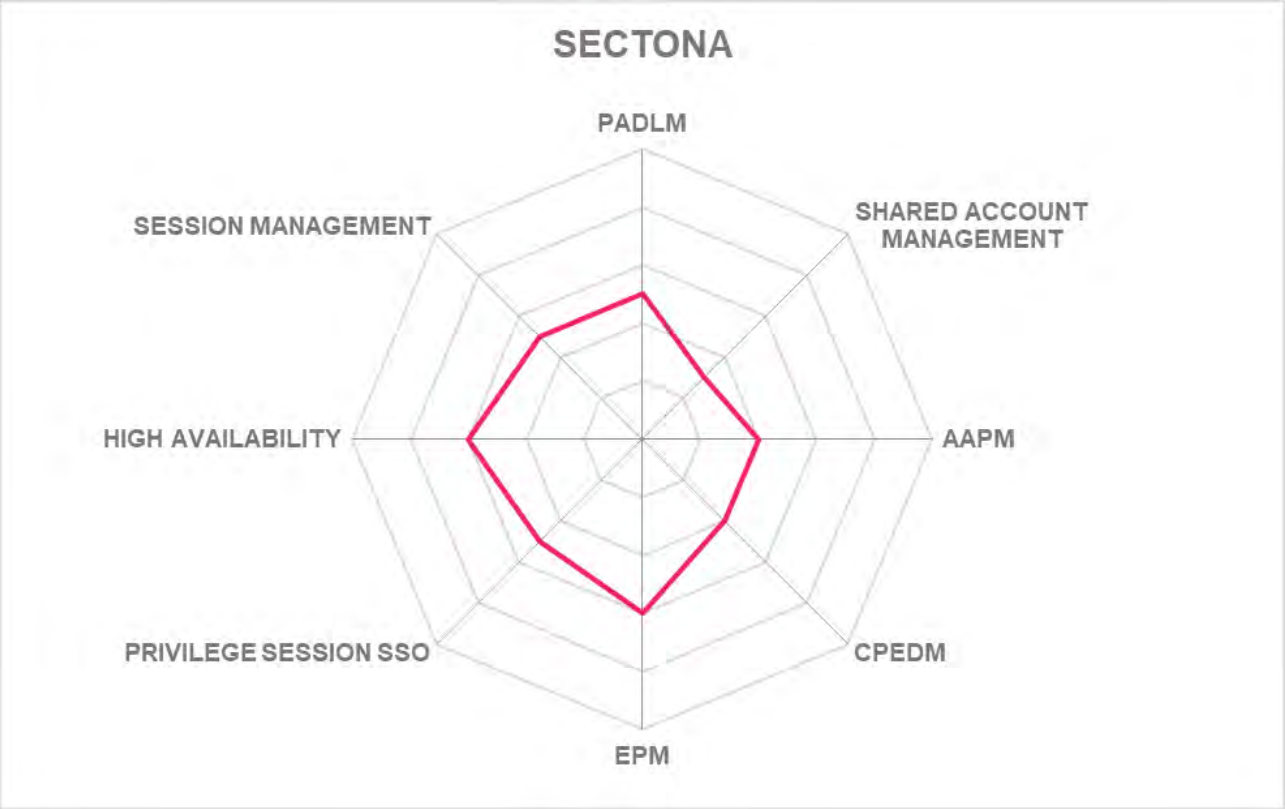
| | |
|---|---|
| Security | ●●●○○ |
| Functionality | ●●●○○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●●○ |


## Strengths

- Easy to understand and use dashboard, PDK does not need coding
- Access from wide range of platforms without agents or plug-ins
- Strong support for cloud-based services to onboard assets
- A collaborative, cross-platform approach allows for integrations offering desired flexibility
- Despite its relative youth the company has done well to present some advanced ideas on PAM and application integration

## Challenges

- While undoubtedly innovative, Spectra needs to offer more capabilities to succeed in Europe and North America
- May struggle to fund the marketing it deserves
- Functionally limited to PSM with lack of proven AAPM, CPEDM capability


SECTONA
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.18 Senhasegura

Based in São Paulo, Brazil, MT4 Networks produces Senhasegura as its flagship PAM product. Comprised of multiple modules, Senhasegura offers comprehensive PAM capabilities. With its customer base primarily concentrated in Brazil, Senhasegura finds natural progression into Latin America due to the cultural affinity and language support it offers. Senhasegura is built over 15 tightly integrated functional components and is available in virtual or hardware appliance delivery formats.

Available in over 20 countries the company reports strong growth in Europe, with 60% growth overall. It has several large banking and ecommerce contracts in Brazil, as well as one with the Brazilian government department. The company has won some deployments against big rivals. Offering a functional module for almost every PAM function in the market, Senhasegura has a broad feature-set but might lack the depth of capabilities in some areas including endpoint privileged management. However, in comparison to most newer market entrants, Senhasegura offers a rather comprehensive PAM product.

MT4 Networks now has a more rounded PAM proposition. In addition to all basic PAM modules for account and password management, Senhasegura offers SSH key management, accounts discovery, AAPM, an endpoint MFA module plus much needed PUBA capability.
An agentless architecture allows for easy installation and configuration while preserving the administrator UX. A set of infrastructure modules offer high availability, load balancing and advanced monitoring capabilities. The company has developed its own Machine Learning algorithm that can read individual user keystrokes to detect unauthorized shared access on endpoints.

CPEDM capabilities are now much improved, enabling logging even when the machine is offline, with a redesigned interface for a better user experience. PAG is now supported but there are integrations also with many SIEM appliances and risk-based analytics now includes user behavior data logs and MT4 Networks has now added multi-lingual versions and support for its product.

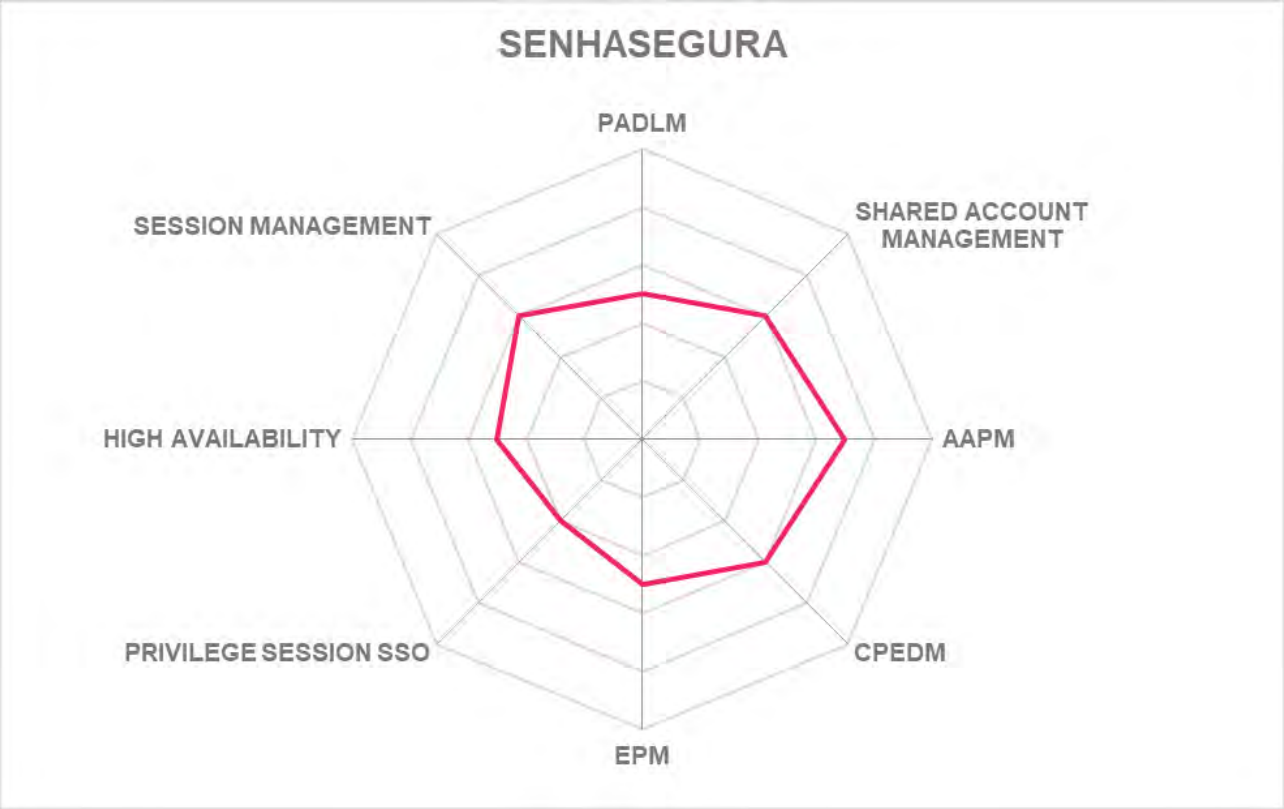
| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●●● |


## Strengths

- Ease of deployment
- Easy to use, clean interface
- Can be customized by admins and end users
- Good efforts made to address challenges
- Keystroke analysis tool is unique and bodes well for future development
- Much improved analytics tools including safety rating status of company

## Challenges

- Needs stronger marketing to be better known in Europe and North America
- Support services currently only available in English and Portuguese
- Wider support for 2FA and MFA partners would be welcome


SENHASEGURA
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.19 SSH Communications Security

Based in Helsinki, Finland, SSH.COM offers PrivX as its primary product in the PAM market. PrivX is a relatively new offering in the market by SSH.COM that attempts to offer an alternative to conventional shared account password management technology by providing a certificate authority based Just-In-Time access for SSH and RDP. Instead, PrivX dispenses with the need for a vault full of credentials and issues short-lived, or ephemeral, certificates for on-demand access. It's an innovative approach but one that does bring functional and security advantages – access is faster, onboarding and offboarding of privileged users is quick and there are no passwords to issue or lose, since there are no permanent leave-behind credentials. Furthermore, users never handle or see any credentials or secrets at any point when accessing servers. Access is also based on roles to further restrict access to only those authorized. PrivX comes in three sales options: PrivX Free for up to 20 hosts, PrivX Business - a monthly subscription that supports up to 500 hosts and PrivX Enterprise that offers tailored pricing for 500+ hosts.

Privileged users log into a clean looking browser-based interface via Single Sign On (SSO) and can see what resources they can access based on their current role and click though appropriately. Access rights are automatically updated as roles change in in either AD, LDAP or OpenID directories or from IAM system that work with PrivX including Okta, ForgeRock and Ubi Secure and One Login.

While the core product is deliberately lean, it integrates with third parties to add functionality for SIEM ticketing systems and HSM. There is support for session recording and compliance, and recordings are encrypted. All SSH/RDP/HTTPS sessions are audited and logged and can also be recorded if needed for compliance, forensics or training purposes. PrivX also offers accountability of user activities even if admins are using shared accounts, since PrivX associates a user ID to every session. PrivX integrates with SIEM, UEBA/BAD systems. Other important areas of functionality covered include SAPM, AAPM, PADLM, PUBA and CPEDM but endpoint privilege management is missing here.

With PrivX, SSH.COM presents a unique approach for managing certificates based SSH and RDP access by offering a certificate authority to issue transient one-time access credentials. SSH.COM appeals to organizations that either need a vault-less approach to manage RDP and SSH access with basic PSM capabilities or are looking to complement their existing PAM solution with these features.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●●● |

SSH.COM

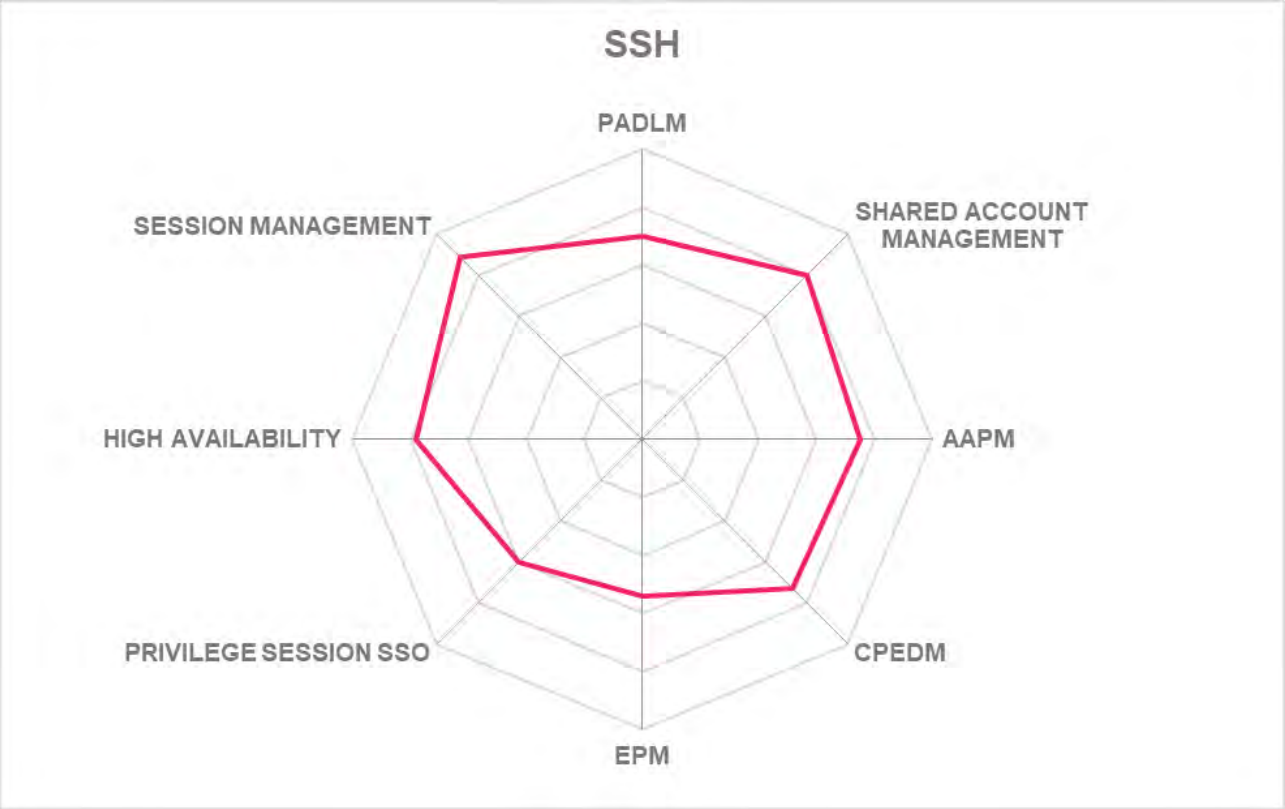
## Strengths

- Lean footprint and rapid access make it ideal for DevOps and agile environments
- Reduces one level of vulnerability by eliminating static passwords and vaults
- Eliminates the risk of redundant credentials being stolen or misused
- Quick deployment
- For a lean product, it still supports many core PAM capabilities

## Challenges

- Lacking endpoint privilege management keeps the solution lean but may be missed
- Vault less and agentless approach may deter some buyers
- Would benefit from an SSH delivered SaaS based version

## Leader in


SSH
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.20 STEALTHbits Technologies

Founded 2002, in Stealthbits is a US based company that offers several solutions designed to help organizations meet their GRC obligations. Part of this portfolio is SbPAM, which manages access to privileged accounts with a task-based approach.

There are four key functions in the product: access control, session recording, auditing and what it describes as zero standing privilege accounts. The theory is to simplify PAM as much as possible by providing a fully JIT ephemeral approach to access and provisioning with as little as possible stored in the product itself. The company believes that day to day accounts should not use admin roots. Instead, privileged accounts don't exist until someone is doing something, then they disappear. However, the product does also support the management and rotation of dedicated admin accounts as well as ephemeral accounts.

The key is BYOV or Bring Your Own Vault. Customers have the option to integrate a third-party vault with a REST API from several leading PAM providers including CyberArk, Broadcom (CA) BeyondTrust and HashiCorp. Stealthbits recommends a vault is still needed for due diligence of admin accounts and has a built-in vault for protecting service accounts used for privilege escalation and can manage the password for existing dedicated privileged accounts used by administrators.

On the dashboard there is no long list of accounts, instead users select what they want to do and then the system provides access and provisions the account. When the session is finished the user is automatically logged out and all privileges are removed. It uses mesh architecture and provides scalability supporting Windows, Linux and Docker built on a .net core and can be hybrid, on-premises or cloud. Built-in task-based certifications are supported.

The downside of all this is that the product lacks some capabilities that many organizations still need: it's really a task-based PAM solution that can work well with the traditional features of other PAM solutions – it may well find a home in specific DevOps environments. In line with its DevOps suitability, Stealthbits promises new releases of the product every three months with new features coming in 2020.

| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Functionality | ● ● ● ● ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability | ● ● ● ● ● |
| Deployment | ● ● ● ○ ○ |

stealthbits

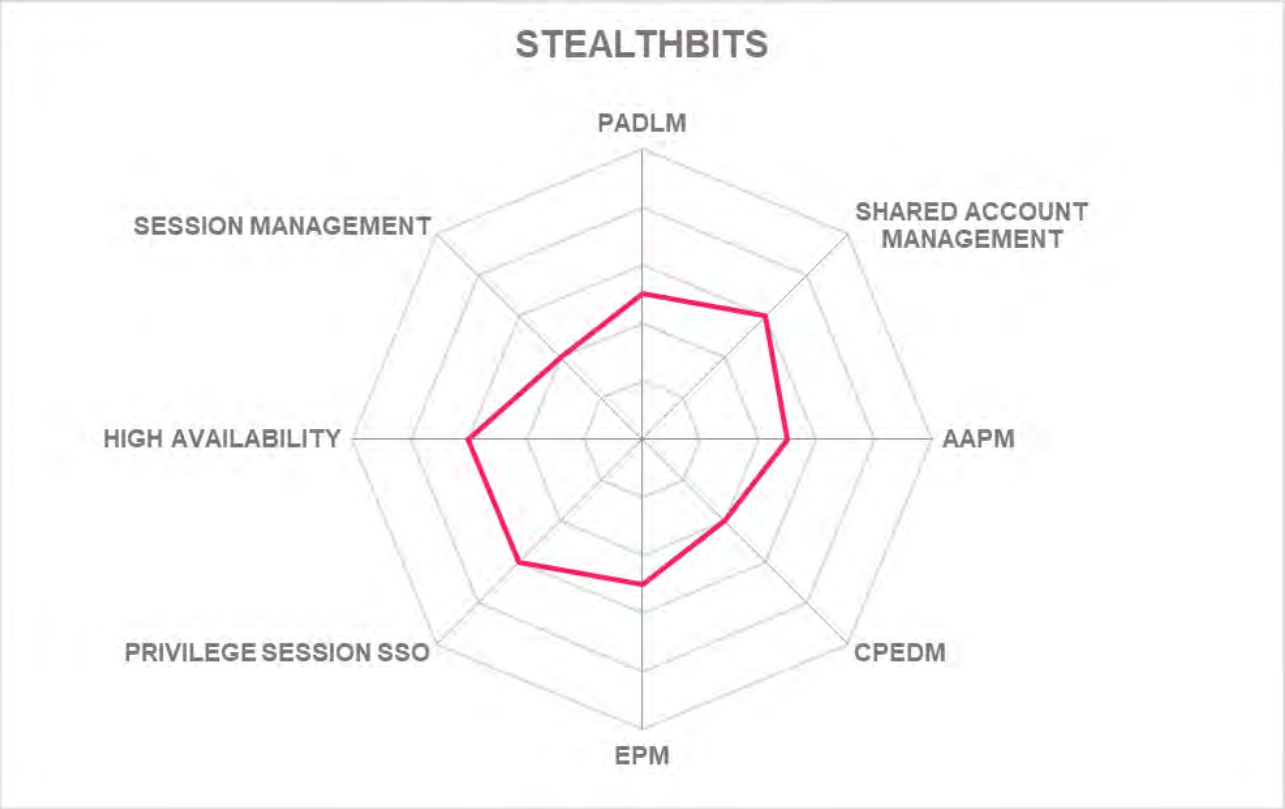
## Strengths

- Potentially the future of PAM in terms of ease of use and ephemerality
- Highly suitable for DevOps environments
- Easy to use and administer, very rapid deployment
- Ephemeral approach means a reduced attack surface
- Would work well with smaller less legacy incumbered organizations

## Challenges

- Organizations may need the back up of existing PAM
- Going vault less may be a step too far for some more complex organizations, who need it for operational reasons.
- Needs to do more to effectively market this approach to PAM

## Leader in


STEALTHBITS
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.21 Systancia

France based Systancia has several workplace and application virtualization tools. As part of this it offers the Cleanroom platform, which it developed as its PAM offering to the market. It is available on-premises or as a service. There are three levels of the cloud-based service: Systancia Cleanroom Starter Service, Systancia Cleanroom Session Private and Systancia Cleanroom Desk Private.

Systancia offers another new angle to privileged access management with a JIT approach based around virtualization. But instead of just providing ephemeral credentials it provides a totally virtualized environment for admins, separated from the real admin server and which can be disposed of after use. A vault and session manager are contained within the virtualized environment for sessions. The idea is that the core functional parts of PAM can be separated from log files, applications and unused secrets which remain on admin servers and only accessed for sessions as needed.

Systancia Cleanroom transparently injects login credentials into managed resources and applications. As soon as an administrator tries to run an application (whether web, software or "in-house"), or a resource (RDP, SSH, VNC or other), the password vault module allows the injection of login credentials linked to the administrator in the authentication windows without any action from them.

Other features include full video recording of sessions and search of those recordings, SSO login available for all admin's resources and applications, and the ability to block suspicious activity in real time. MFA support is available vis email, SMS, mobile app or RSA SecureID. For Mail and SMS OTPs, the algorithm used to generate the temporary password is fully customizable (number of characters, allowed characters, validity period etc.). The OTPs via mobile applications (TOTP) and RSA SecureID being based on standards, are not customizable. Systancia Cleanroom is designed to work in tandem with Systancia Identity, its IAM suite.

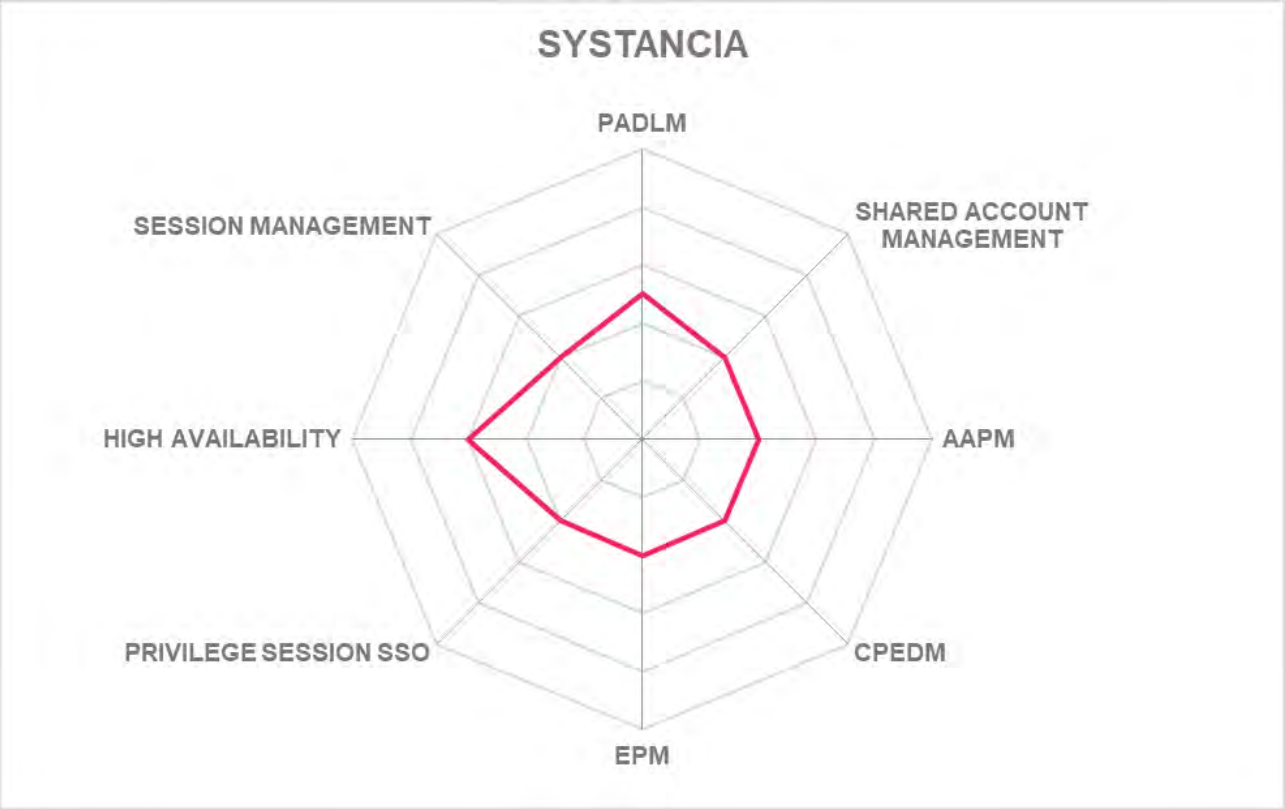
| | |
|---|---|
| Security | ● ● ● ● ○ |
| Functionality | ● ● ● ● ○ |
| Interoperability | ● ● ● ○ ○ |
| Usability | ● ● ● ● ○ |
| Deployment | ● ● ● ○ ○ |


## Strengths

- New improved UI even better than before, bang up to date
- VM works well to isolate sessions and keep secrets secure
- Clever use of automation for login and credential management
- Supports in-house IAM suite from Systancia
- Good job of developing product for more advanced applications

## Challenges

- Lack some fundamental PAM capabilities that it will need to fully compete
- Some organizations may need convincing of the security and robustness of the automation features in product
- Some may feel put off by integration with other Systancia products


SYSTANCIA
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.22 Thycotic

Based in Washington D.C. (US), Thycotic offers the Secret Server platform as its primary PAM. Secret Server is known for its comprehensiveness, ease of deployment and configuration that can reduce product deployment and upgrade cycles substantially. Thycotic's partnership with IBM has accelerated Thycotic's global market expansion through IBM's large customer base.

Thycotic remains one of the well-known names in PAM and while it has benefited from the "blue labelling" of its product by IBM it has remained very much its own company and able to reach big corporate customers of its own. Thycotic's platform consists of four PAM modules: Secret Server itself, Privilege Manager, Account Lifecyle Manager, DevOps Secrets Vault plus the Connection Manager (its RDM product). Thycotic has committed to frequent product updates including for DevOps Security Vault, and the Account Lifecycle Manager. Thycotic is on the right lines by saying that PAM for DevOps is more about secrets management and code etc., than just passwords. To that end, credentials will get embedded into microservices, not a vault, in Thycotic's approach.

Privilege Manager is Thycotic's agent based EPM solution for Windows and Mac endpoints that supports extensive EPM capabilities including application control and privilege elevation (available on-premises or as a SaaS-hosted solution in Azure. The Thycotic Privilege Behavior Analytics solution monitors user activities across Secret Server deployments and can alert upon detection of anomalies based on an alert threshold.

Secret Server is launched from an SSH terminal, but the product also benefits from a brand-new user interface as of 2020 to hide the command lines interface from most users – unless they want to use it. For SSO it has a strategic partnership with Duo Security and the company promise that JIT functionality is coming for later in 2020. Scalability and fast deployment are also strengths.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●● |
| Usability | ●●●●● |
| Deployment | ●●●●○ |

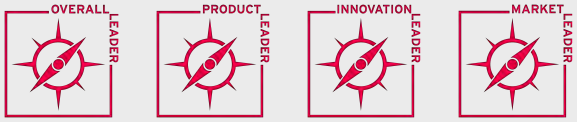

## Strengths

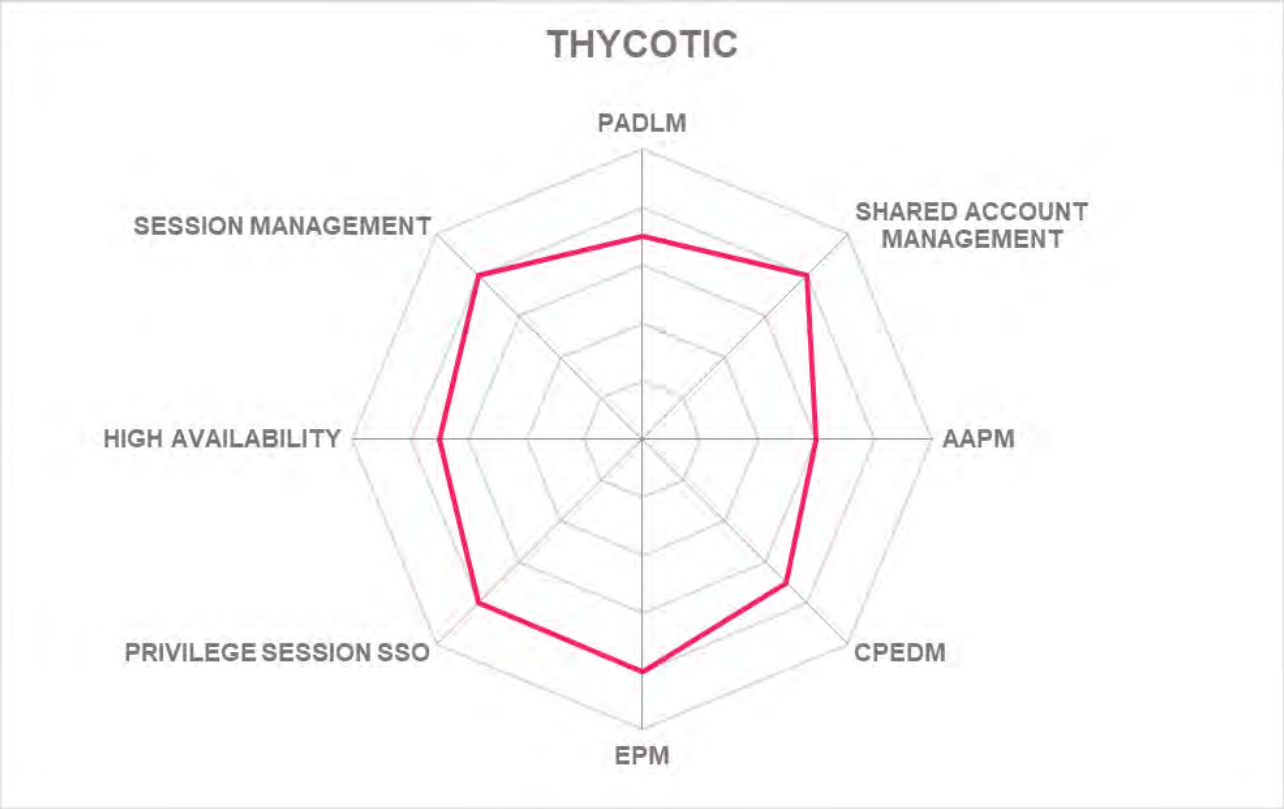
- Solid and well-known brand that has used its relationship with IBM to its advantage
- Ongoing product development and frequent updates show commitment
- Thycotic understands that DevOps for PAM needs to take account of coding environment
- Good new user interface leverages current UX trends for ease of use
- Strong endpoint management capabilities good for digital environments
- Supports most advanced capabilities

## Challenges

- No support for SAP Business One or Oracle E-business suite
- Lacks always-on discovery scans and scans not available as XML
- May need to convince larger organizations of the need to replace legacy PAM

## Leader in




THYCOTIC
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.23 WALLIX

Based in France, WALLIX provides WALLIX Bastion as its primary PAM product in the market. At the core of Bastion is password management, session management and access management with built-in access request and approval capabilities. WALLIX has a large install base across Europe and Middle East with a limited presence in North America and Asia regions. In 2019 it began to sign its first MSSP customers and claims a 40% market growth CAGR.

Designed as an integrated PAM platform suite, activity recording, session monitoring and password management are part of the standard WALLIX Bastion proposition. WALLIX Bastion suite is available in hardware as well as virtual appliance formats and supports multi-tenancy configuration for hosted and managed service providers and is available on the public cloud marketplace. It can be hosted on-premises or in the cloud depending on preference and suitability for the organization.

The Bastion Session Manager includes session establishment, auditing, monitoring and recording of privileged activities. The Bastion Password Manager offers password management and automated rotation of a managed systems' credentials. Session sharing is now supported with embedded four eyes protection and collaborative four hands. Different admins can now share the same session while logging into the same account and supervisors can block privileged users in real time if they detect suspicious behaviour.

WALLIX's AAPM is designed to complement Robotic Process Automation (RPA), to simplify DevOps security or any automatic administrator activities. It can be integrated into scripts or called by applications like Terraform or Ansible to extract credentials from the Bastion vault in order to eliminate hard-coded passwords and provide credentials to DevOps tools. WALLIX Discovery is used to identify all privileged accounts across the IT environment, including local accounts The WALLIX Bastion can be deployed in several ways according to customer's environment, budget and risk profile: on public cloud platforms, in virtualization infrastructure or on-premise options are available to best fit need.

By centrally managing privileged access requests across hybrid and multi-tenanted architectures, admins and IT managers have a single view from the administration portal. Supervisors can see in real-time what privileged account users are doing and take appropriate action if needed. The recording function built-in to WALLIX Bastion gives organizations the opportunity to track and trace potential malicious insiders or attackers and reduces the chance of costly data breaches.

The WALLIX End Point Management features increase users' privileges on their Endpoint by eliminating local administrators' rights and by granting specific rights to each user and distributing privileges to the applications and processes instead of the users themselves.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●○ |
| Deployment | ●●●●○ |

BASTION

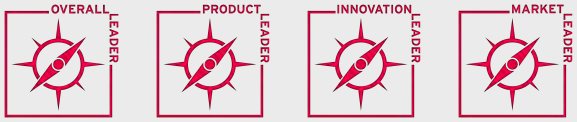
## Strengths

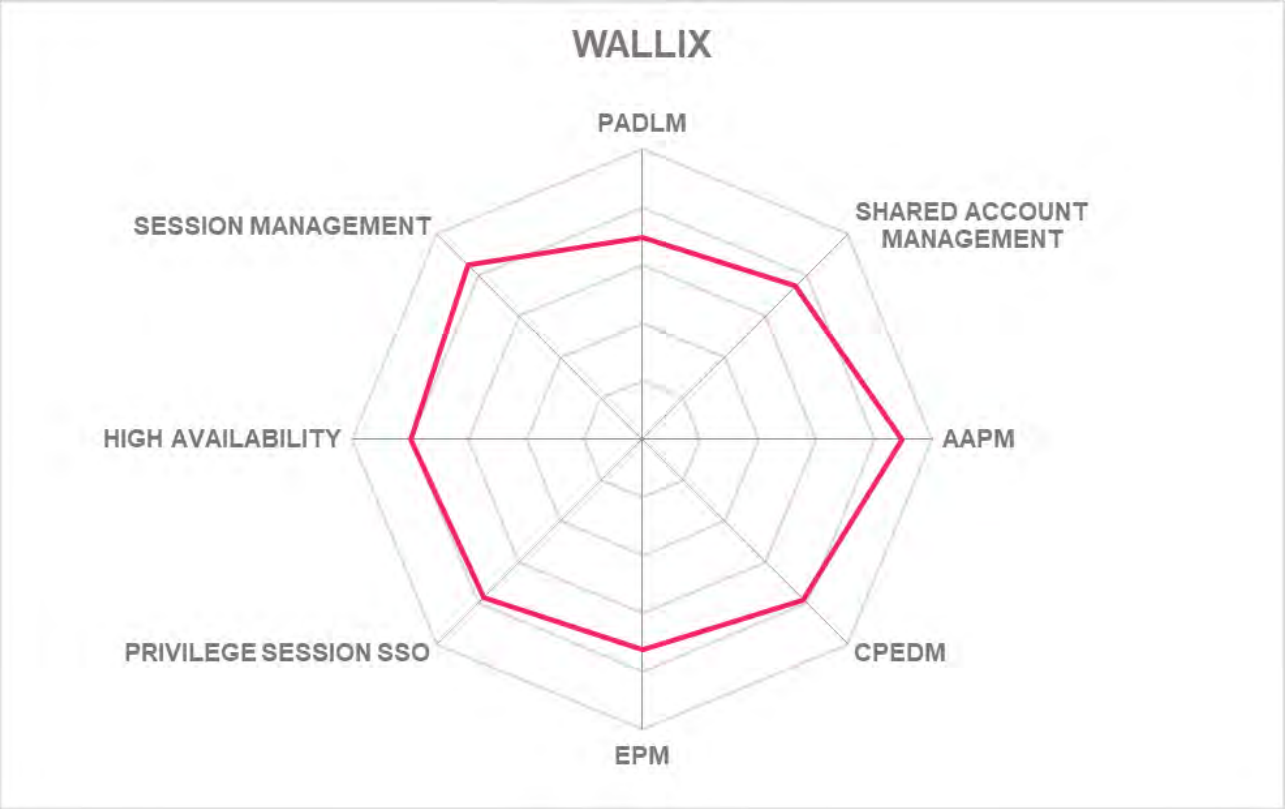
- Supports a broad range of target systems, primarily for on-premise systems and cloud environments
- Proven in multiple operating environments including OT, industrial and SCADA
- Leading privilege session management (PSM) capabilities
- Web access gateway and a single administrative console for all Bastion instances
- Strong support for multi-tenancy and HA options

## Challenges

- Lack of strong support for cloud platforms
- Some aspects of platform UX are still behind the curve on current design practice
- WALLIX needs to expand its presence beyond EMEA with this improved proposition

## Leader in




WALLIX
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

## 5.24 Xton Technologies

Founded in 2017 and based in the US, XTON Technologies offers its XTON Access Manager (XTAM) platform to enterprise customers with a strong emphasis on making PAM simpler to meet compliance requirements.

Still a very new player on the block, XTON claims that its solution was built from the ground up in 2017 and can be installed in less than 10 minutes. It uses an API for MFA providers. The solution relies on agentless technology, so no passwords are distributed. The company say that its solution is genuinely agentless and has both advanced RDP, SSH and HTTP(s) proxies and HTML 5 that can record sessions, keystrokes and file transfers. In addition, XTAM can rotate passwords automatically and discount privileged systems and accounts. The solution benefits from weekly updates including feature requests and bug fixes – part of the company's philosophy that security software should be updated often. Updates are deployed via the GUI.

XTAM is a self-hosted solution that supports Windows, Linux Server installations (including RedHat) on-premises or for the cloud There are two versions: Quantum Vault which provides basic PAM functionality and XTON Access Manager for Enterprise that adds workflows, password rotation, discovery remote access and full API integration among other features. MFA and SSO is supported through integration with AzureAD Okta, WatchGuard and Duo Security. Credentials never leave the vault and the solution also supports Just-in Time provisioning.

XTAM, provides a web-based password vault and offers accounts discovery, shared account password management and privileged session management capabilities including password rotation, access request workflows and session and keystroke recording with playback. While XTON doesn't provide controlled privilege elevation and delegation management (CPEDM) capabilities, it offers support for elevated script automation for routine privilege escalation tasks, enhancing administrator efficiency.

For a new market entrant, XTON offers a wide PAM technology portfolio that aligns well with the market direction and supports emerging PAM requirements of organizations. XTAM is offering integrations with ITSM, SIEM and MFA providers, and is a scalable solution for on-premises , hybrid and cloud deployments.

Based on open software and standards, XTON offers an unlimited subscription pricing model and thereby presents a viable alternative to many established PAM vendors, particularly in the mid-market segment but doesn't offer a technological lead in any area such as DevOps for example.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●○○ |
| Deployment | ●●●○○ |

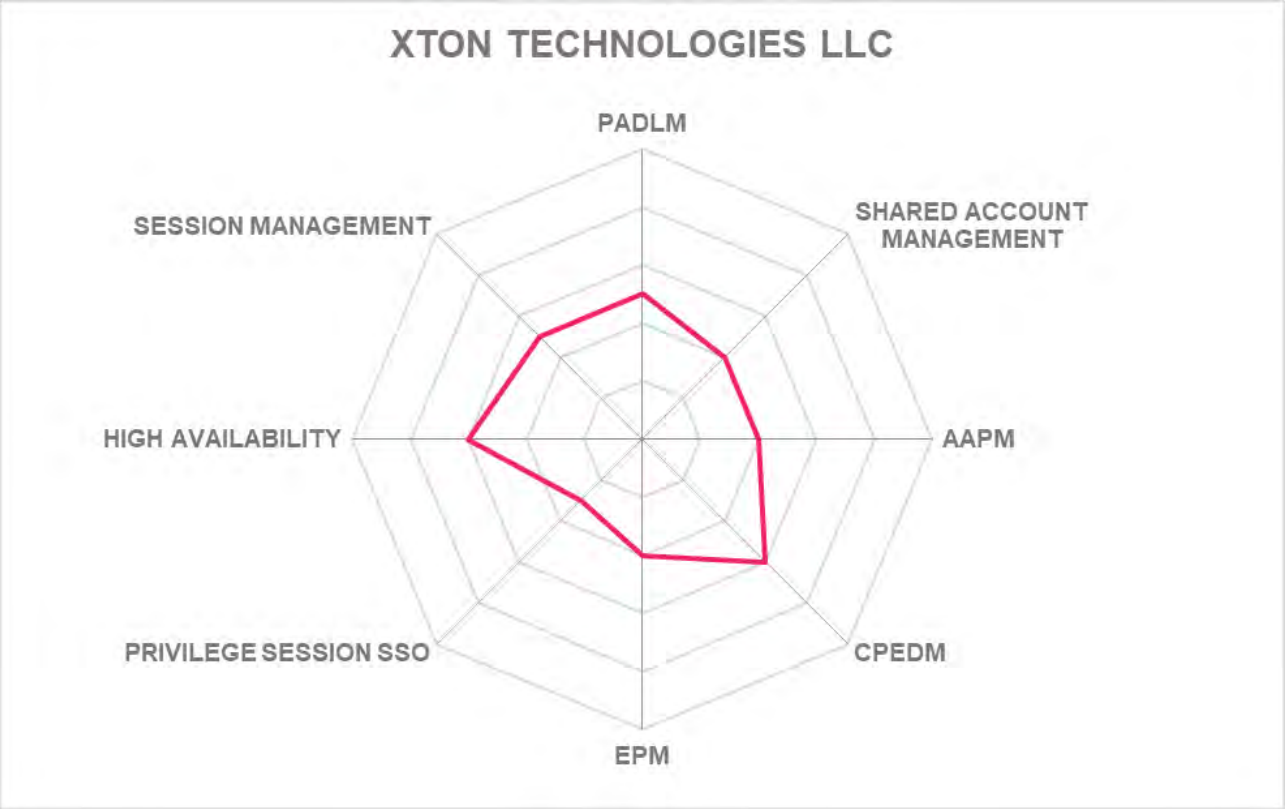
XTON technologies

## Strengths

- Solid overall package that supports most of the advanced PAM functions needed for larger organizations – comprehensive for such a new player
- Wide number of options available for 2FA and MFA implementation
- Passwords and key never transmitted to the end user
- Can be offered as-a-service from third-party MSPs
- Agentless architecture speeds deployment and time to value for organizations

## Challenges

- Still lacks an EPM module which may deter extended organizations
- Lacks multi-lingual documentation for non-English speaking regions
- Ephemeral capability would improve its JIT proposition


XTON TECHNOLOGIES LLC
PADLM
SHARED ACCOUNT MANAGEMENT
AAPM
CPEDM
EPM
PRIVILEGE SESSION SSO
HIGH AVAILABILITY
SESSION MANAGEMENT

# 6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of PAM or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

## 6.1 Deep Identity

Based in Singapore, Deep Identity is a regional provider of Identity Management software, offering Deep PIM as its primary PAM product which is essentially built as software plug-ins over Deep Identity Manager and comes with Privileged Access Server (PAS) acting as a gateway to establish and manage access to the target systems. While Deep IM extends account provisioning and access request approval workflows to privileged access, Deep PIM lacks several basic PAM features that include privileged accounts discovery, shared account password management (SAPM) and controlled privilege elevation and delegation management (CPEDM).

Though PIM gateway provides support for privileged RDP connections to Windows servers and offers session logging and recording with text-based search and review capabilities, it lacks support for management of privileged accounts and activities in cloud applications and platforms.

With some good local presence in Asia, particularly South East Asia (SEA), Deep PIM is a good addition to existing Deep Identity Manager deployments to onboard additional privileged session management features. It also appeals to organizations with basic PSM needs along with the requirements of regional delivery and integration support.

## 6.2 HashiCorp Vault

San Francisco (US) based HashiCorp is a provider of application development and delivery management software for datacenters. Built on an open source foundation, HashiCorp offers a secure password vault that integrates with its application development and delivery management modules to offer a tightly integrated DevOps platform.

The vault is offered in three variants for individuals, teams and enterprises depending on the complexity of development and deployment processes involved. While the basic password vaulting features such as encryption, secure storage, keys rotation, vault agent, access control policies and credential checkout workflows are included in all the three vault variants, MFA, governance and features necessary to support multi-datacenter environments such as disaster recovery and replication are only available as part of team and enterprise versions.

Not a complete PAM platform, HashiCorp offers password vaulting and secure application to application password management capabilities to support enterprise DevOps initiatives. While several other PAM vendors are now offering similar capabilities to suit DevOps, HashiCorp offers a good start for organizations looking to onboard PAM with application development and deployment processes.

## 6.3 Identity Automation

Houston (US) based Identity Automation is an IAM solution provider that offers RapidIdentity Privileged Access Management as its PAM product in the market. System integrator turned identity software provider; Identity Automation offers a broad range of IAM technologies with privileged access management being one of the latest additions to its RapidIdentity portfolio. RapidIdentity offers a baseline PAM feature-set with shared account password management, application to application password management and basic auditing and logging of privileged activities. Support for SSH keys is included.

Using automated workflows for privilege escalation, RapidIdentity PAM supports in-built MFA for privileged access but lacks controlled privilege elevation, session management and endpoint privilege management capabilities. The acquisition of Healthcast, a provider of access management solution targeted at healthcare industry brings Identity Automation the required connectors for specialized healthcare systems along with the domain expertise. RapidIdentity PAM appeals to organizations, particularly in the healthcare industry, with a need for an integrated PAM solution that offers password management, MFA and basic auditing.

## 6.4 IRaje

India based IRaje offers Privileged Identity Manager (PIM) as a complete PAM solution with a compelling feature set and the flexibility to customize according to business requirements. Offering an agentless approach to PAM, Iraje supports a wide range of target systems and is available in software as well as virtual and hardware appliance formats.

Iraje offers a native database client, schema extender and database monitoring module in conjunction to its PIM product targeted at securing privileged database operations. There are additional modules available for 2FA and SSO but lacks endpoint privilege management and advanced AAPM capabilities such as application or process fingerprinting.

Iraje's PIM is targeted at offering a complete PAM solution for SMBs in Asia and should appeal to customers that require the flexibility to customize PAM for a deeper auditing and monitoring of database operations across a distributed IT environment, however, in addition to what seems more like an inconsistent marketing, there's lack of sufficient industry feedback to validate Iraje's product maturity and customer information.

## 6.5 NRI Secure Technologies

Japan based NRI Secure Technologies offers SecureCube Access Check primarily providing Privileged Session Management (PSM) capabilities. Operating in a gateway-based approach, SecureCube Access Check extends BeyondTrust Powerbroker Password Safe for password management. NTT Software Corporation builds its iDoperation PAM solution based on Access Check to offer session recording, monitoring and review capabilities. Supporting approval request workflows with role-based access control policies, Access Check offers a distinct approach aimed at access control of privileged users. Access Check lacks Application to Application Password Management (AAPM) capabilities but supports command filtering and detailed session monitoring and alerting capabilities.

SecureCube Access Check also provides access control and monitoring of file transfers and database sessions to Oracle RDBMS.

With majority of its customers in Japan, SecureCube Access Check makes a good fit for East Asian organizations looking for regional integration support and detailed privileged session auditing and monitoring capabilities.

## 6.6 ObserveIT

ObserveIT provides a comprehensive agent based PSM platform that is deployable and scalable across a variety of IT systems. Offers detailed user behavior analysis and live session response features, ObserveIT is one of a few specialized vendors that originated in the area of Session Recording and Monitoring (SRM) and extended it to include other PSM features. In addition to monitoring and recording of both CLI and GUI type sessions in visual formats that allows creation of detailed user activity log from the recorded data, ObserveIT offers advanced user behavior analytics that detects and alerts anomalous user behavior. Observe IT also offers live session response that allows for interruption of sessions at runtime based on information fed from user behavior analytics or through external products such as SIEM (Security Information and Event Management) tools.

With visual endpoint recording, ObserveIT can capture sessions across a variety of systems, supporting all major protocols such as RDP (Remote Desktop Protocol) including the Citrix variants, SSH, Telnet and direct logins to application consoles. An agent-based approach allows for detailed logging and therefore more meaningful and efficient activity search in contrast to other similar solutions that are primarily proxy or gateway-based.

## 6.7 Saviynt

Saviynt is a US based company founded in 2010 that specializes in IGA and Identity solutions. It has recently entered the PAM market with a new cloud only PAM platform, with HashiCorp vault technology to store secrets – generation of new keys, rotation and check in/check out are

performed within Saviynt Cloud PAM, however. The solution is designed to run on all major cloud platforms including AWS, Google, Azure SAP 4 Hana, Oracle, AWS and Azure. It is also compatible with Workday and Salesforce platforms. While no PAMaaS option is offered directly by the company, in theory it could be deployed as a service by third party managed service providers (MSPs) or as an option within large enterprises.

Within the product itself are a discovery tool, session recording and session management as well as more advanced features such as risk analytics, access reviews and a risk and controls library. PAM for DevOps will appear in a later release. The product will also connect to other applications running on all major cloud platforms and it claims its IGA experience with existing identity products should reduce the risk of privilege accounts sitting on a cloud service and applications.

## 6.8 Venafi

US based Venafi offers TrustAuthority, a machine identity protection platform that also offers extensive SSH key management for securing privileged access gained through SSH keys across organizations of all sizes and verticals. SSH keys are used for privileged operations in a Unix environment and pose significant threats to security as most organizations don't have a policy pertaining to management and rotation of SSH keys. Venafi TrustAuthority offers continuous discovery, inventory and monitoring of SSH keys across the IT infrastructure and enables automated key rotation.

Venafi TrustAuthority delivers centralized SSH key management and provides enterprise-wide visibility into SSH key inventories and SSH trust relationships. Venafi also offers automation of SSH key lifecycle from key provisioning to decommissioning, thereby securing and controlling all SSH keys to minimize the risk of unauthorized access to critical systems.

Venafi isn’t categorized as a pure-play PAM vendor by KuppingerCole as it doesn’t provide basic common features required to be qualified as a PAM vendor. While several vendors offer SSH key management support as part of their SAPM, Venafi provides most advanced SSH key management capability in the market. Venafi appeals to organizations that have a critical security requirement to gain visibility and control over unmanaged SSH keys and other credentials used for privileged access.

# 7 Related Research

Advisory Note: Trends in Privileged Access Management for the Digital Enterprise –71273Architecture Blueprint: Access Governance and Privilege Management – 79045
Blog: PAM Can Reduce Risk of Compliance Failure but is Part of a Bigger Picture
Blog: Privileged Access Management Can Take on AI-Powered Malware to Protect
Blog: Taking One Step Back: The Road to Real IDaaS and What IAM is Really About
Executive View: BeyondTrust Password Safe – 80067Executive View: CyberArk Privilege Cloud – 80122
Executive View: Devolutions PAM Solution – 80070
Executive View: One Identity Safeguard Suite – 80074
Executive View: Thycotic Privilege Manager – 80004
Executive View: Wallix Bastion – 79053
Executive View: Xton Technologies Access Manager – 80128
Leadership Brief: Privileged Account Management Considerations – 72016
Leadership Compass: Identity Provisioning – 70949
Leadership Compass: Identity Governance & Administration – 71135
Leadership Compass: Privilege Management - 72330
Whitepaper: AI, Machine Learning and Privilege Access Management – 80120
Whitepaper: Privileged Access Requirements for Small to Medium Size Businesses (SMB) – 80123
Whitepaper: Understanding Privilege Access Management – 80302

# Methodology

### About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

### Types of Leadership

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- **Market Leaders**: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders**: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders**: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- **Challengers**: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers**: This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even the best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in a given market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

**Product rating**

KuppingerCole as an analyst company regularly conducts evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- **Security**
- **Functionality**
- **Integration**
- **Interoperability**
- **Usability**

**Security** – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such

issues and the way a vendor deals with them.

**Functionality** – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

**Integration** – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

**Interoperability** – interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

**Usability** – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user

interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

**Vendor rating**

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

**Innovativeness** – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

**Market position** – measures the position the vendor has in the market or the relevant market

segments. This is an average rating overall markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

**Financial strength** – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.

**Ecosystem** – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor

**Rating scale for products and vendors**

For vendors and product feature areas, we use – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

**Strong positive**
Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

**Positive**
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

**Neutral**
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.

**Weak**
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

**Critical**
Major weaknesses in various areas. This rating most commonly applies to company ratings for

market position or financial strength, indicating that vendors are very small and have a very low number of customers.

### Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- **Lack of information supply**: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview of vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

# Content of Figures

# Copyright


**KuppingerCole Analysts** support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

**KuppingerCole**, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.
For further information, please contact clients@kuppingercole.com.