KuppingerCole Report

LEADERSHIP COMPASS

By Paul Fisher
August 31, 2021

Privileged Access Management

Privileged Access Management (PAM) is an essential component in protecting organizations against cyber-attacks, ransomware, malware, phishing, and data leaks. No longer only for protecting admin accounts, privilege management now extends across the entire organization -from on-premises and cloud infrastructures to every user, no matter where they are working from, or what they are accessing.

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

Content

1 Introduction

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

1.1 Highlights

- In depth ratings and reviews of 26 leading PAM products, fully updated for 2021
- PAM vendors have responded well to the privilege remote access challenges of the pandemic period with EPM and RPA capability improvements.
- More vendors are now offering automation and improved UX design to reduce the PAM admin burden, and make access easier.
- Several previous Challengers are now taking their place among the Leaders after a year of significant capability additions and enhancements. The market remains highly competitive.
- A small but growing trend is for IDP and IAM vendors to put their toes in the PAM waters, and some existing PAM vendors openly talking about Privileged Identity and Identity Security as part of their pitch.
- More general trends include the increased availability of PAMaaS, and PAM platforms designed specifically for SMBs and cloud native deployment
- Ease of Use is no longer a "nice to have" but increasingly seen as essential to cope with the growing demands on PAM.
- More use of consumer like Wizard tools to ease set up and deployment, and PAM architecture provided out of the box
- The Product Leaders are Arcon, BeyondTrust, Centrify, CyberArk, Hitachi ID, One Identity, Senhasegura, SSH.COM, Broadcom (Symantec), Thycotic, WALLIX and Xton (acquired by Imprivata in July 2021).
- The Innovation Leaders are Arcon, BeyondTrust, Centrify, CyberArk, Hitachi ID, ManageEngine, Remediant, Saviynt, Senhasegura, SSH.COM, Stealthbits, Thycotic, WALLIX and Xton.

- The Market Leaders are BeyondTrust, Centrify, CyberArk, Hitachi ID, Micro Focus, One Identity, Saviynt, Senhasegura, Stealthbits, Broadcom (Symantec), Thycotic and WALLIX

1.2 Market Segment

Privileged Access Management (PAM) platforms are critical cybersecurity controls that address the security risks associated with privileged access in organizations and companies. It is reckoned that most successful cyber-attacks involve the misuse of privileged accounts. And misuse is enabled by poor management of privileged access using old or inadequate PAM software, policies, or in-house processes. A 2020 RSA Conference report[1] states that potentially malicious privileged access from an unknown host accounted for 74% of all privileged access anomaly behaviour detections. The message is clear: hackers are actively targeting privileged accounts as the best way to get inside an organization.

While PAM platforms have been around for around 20 years, the demands of digital transformation and wholesale structural changes to IT architecture have intensified interest in Privileged Access Management software and applications -- across all market sectors.

Vendors, both traditional and new have been responding to the demand and critical need for advanced PAM that can meet the challenges of the modern computing era. Among key negative activities that PAM must control are abuse of shared credentials, misuse of elevated privileges by unauthorized users, theft of privileged credentials by cyber-criminals and abuse of privileges on cloud infrastructure.

KuppingerCole research shows that the PAM market is responding and growing because of these challenges and is in a vigorous period of innovation. Part of this is flexibility in purchasing options with growth in subscription models and SaaS options, although licensing and maintenance deals still dominate the sector. We believe that as PAM moves from a static to a more dynamic operating model to deal with equally dynamic IT architecture; SaaS and flexible purchasing options will become more popular with customers not wanting to be tied into technology that is not evolving fast enough for their changing demands. For PAM futures, flexibility will be key in purchasing, delivery, deployment and usage.

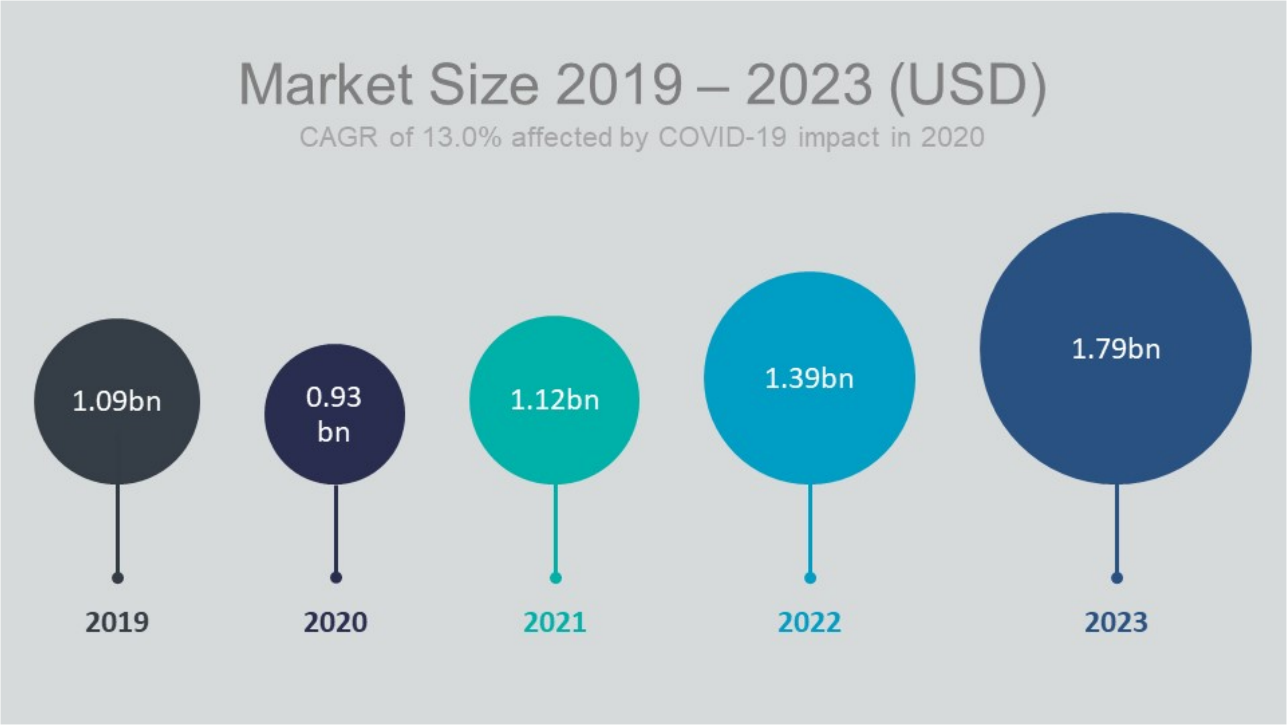


Figure 1: Projected market growth of global PAM market by 2023 (KuppingerCole)

Trends in the market

In the past 12 months we have seen some changes in the vendor landscape with mergers and acquisitions affecting some of the bigger independent players, while those PAM vendors that became part of global IT providers have seen a rebranding and refocus of their product lines, considering trends such as PAM for DevOps and EPM. When two players join forces in the same market there is always some uncertainty for new and existing customers as mergers take time to bed down. In previous times we have seen vendors struggle to manage product overlap, differing marketing strategies, and customer groups. Even those mergers seen as symbiotic rather than simply acquisitive can pose some teething troubles for both parties.

Another small but growing trend is for IDP and IAM vendors to put their toes in the PAM waters, and some existing PAM vendors now openly talking about Privileged Identity and Identity Security as part of their pitch. While Identity is increasingly taking a central role in IT security and access management, it is too early to detect a fundamental shift in this market. But vendors and analysts alike are looking at how Identity, Risk and Task controls may play a central role in governing and managing Privileged Access in the future -- particularly in sprawling cloud infrastructures.

The term Zero Standing Privilege (ZSP) is also gaining traction. In short, the theory is that no person or entity should ever hold standing privileges and all PAM be based on a Just in Time or ephemeral footing. If it is fast enough - this could potentially be one future for PAM but there are likely to be many organizations that continue to rely on standing privileges, passwords, and vaults for operational and legacy reasons and would find it hard to transfer to ZSP (and by extension, they do not trust putting passwords and vaults in the cloud).

Zero Trust is an extension of this approach, but it should be remembered that for PAM to work efficiently, a level of trust must still be priced into operations. The future may well be a mixture of all approaches, based around Identity and Risk to ensure that trust can be maintained for many users and accounts. Finally micro-PAM features are starting to appear in Data Governance and IRM platforms and cloud providers continue to add forms of secrets management to their offerings -- but these are a sideshow currently to the concerns of this Leadership Compass.

More general trends include the growing availability of PAMaaS, and PAM platforms designed specifically for SMBs and cloud native deployment. Ease of Use is no longer a "nice to have" but increasingly seen as essential to cope with the growing demands on PAM. We are seeing more use of consumer like Wizard tools to ease set up and deployment.

1.3 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.

1.4 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 infrastructures. A core PAM solution will provide an organization with the basic defences needed to protect privileged accounts, but the PAM market is adapting to provide different levels of service and capabilities to meet with newer capabilities being offered. Digital transformation and infrastructure changes mean that organizations would benefit from many of the advanced capabilities offered as part of PAM suites from leading vendors in the market.

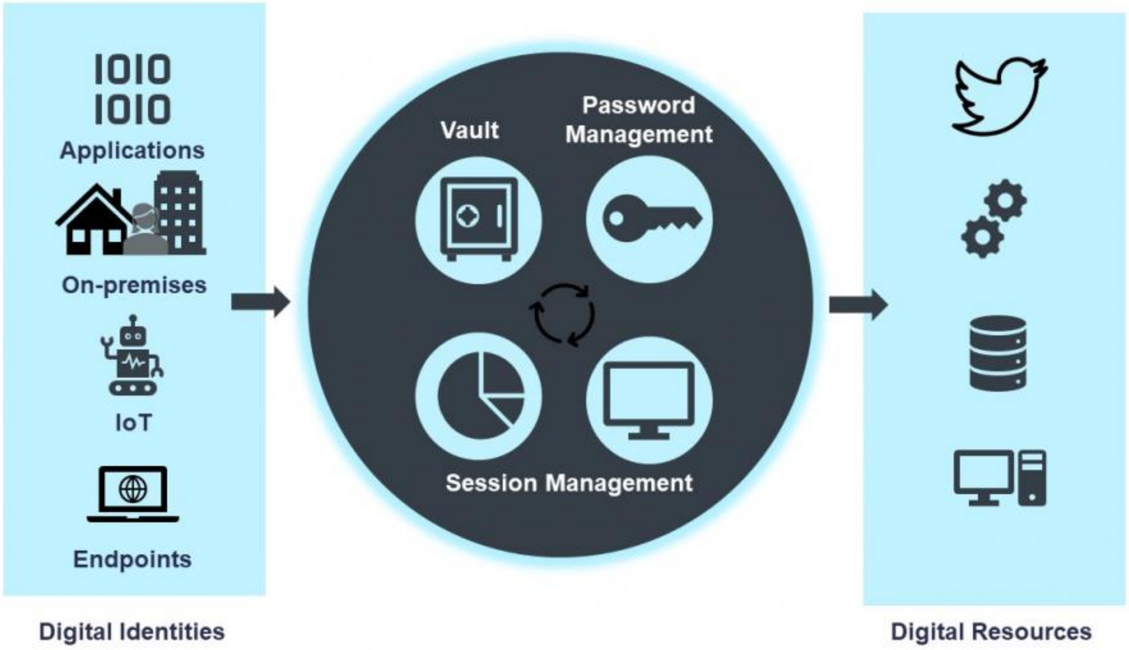


Figure 2: The core capabilities of PAM should provide secure access for all digital identities and locations (Source: KuppingerCole).

1.4.1 Classical PAM capabilities

While the market continues to offer more capabilities to PAM platforms to meet the privileged access demands of large and more complex organizations, classical PAM capabilities are outlined below.

Password Management

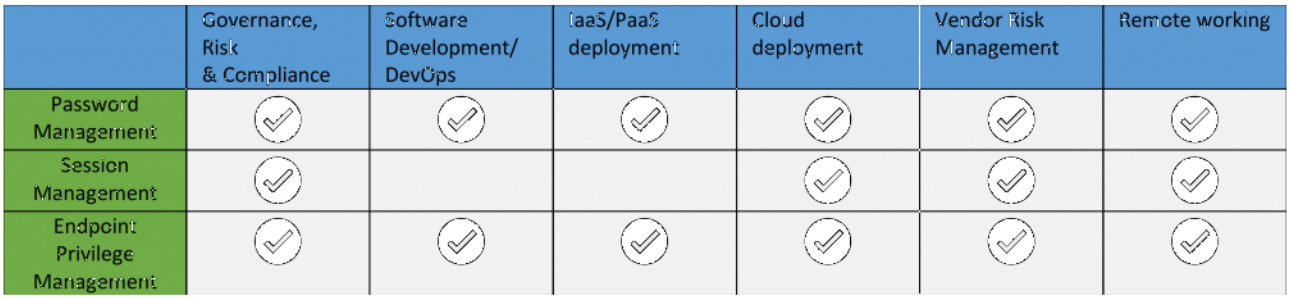
Although not ideal, many organizations will share passwords and keys to privileged accounts. To counter this, Password Management controls access to shared accounts and ideally provides alerts to unauthorised usage of accounts. It is a fundamental tool that usually includes a Vault to store encrypted keys, passwords, or other relevant secrets.

Session Management

Session Management offers basic auditing and monitoring of privileged activities. Session Management tools can also offer authentication and Single Sign-On (SSO) to target systems.

Endpoint Privilege Management (EPM)

Managing privileged access to endpoints is important and is often combined with specific capabilities such as black or whitelisting of applications. In the new era of much increased working from home we are also seeing privileged access authenticated directly ***from*** endpoints.



	Governance, Risk & Compliance	Software Development/ DevOps	IaaS/PaaS deployment	Cloud deployment	Vendor Risk Management	Remote working
Password Management	✓	✓	✓	✓	✓	✓
Session Management	✓			✓	✓	✓
Endpoint Privilege Management	✓	✓	✓	✓	✓	✓

Figure 3: The three classical PAM capabilities can cover most core business IT use cases.

1.4.2 Desired capabilities in addition to the classical components

As demands develop across the market, the choice for PAM has become wider but also more fragmented with the result that one solution may not fulfil all requirements. For some organizations, some modules will be more important than others depending on enterprise architecture. A good example of a new challenge for PAM vendors has been the rise on remote working which calls for privileged access from the endpoint. Elsewhere, right across organizations we have seen further penetration of DevOps, CI/CD, IaaS, and multi cloud environments which also call for extra capabilities in PAM, but again not all customers will desire or need all of them.

The more complex operating environments means that customers can take advantage of the wide choice of PAM capabilities now available to them across the vendor spectrum. There is not always a need for a specialized PAM for DevOps, but for a PAM solution that supports the hybrid reality of your business including DevOps and agile computing -- but also any legacy architecture that is in place.

Step back and rethink your PAM needs before making decisions. It starts with the use cases: what do you need to protect and where? Which are the capabilities you need? And which can you really handle -- do you have the capacity and need for full session monitoring and analytics for example?

The optional capabilities to consider are as follows:

Privileged Account Data Lifecycle Management (PADLM)

The usage of privileged accounts must be governed as well as secured. PADLM serves as a tool to monitor the usage of privilege accounts over time to comply with compliance regulations as well as internal auditing processes.

Application to Application Password Management (AAPM)

Part of digital transformation is the ongoing 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.

Controlled Privilege Elevation and Delegation Management (CPEDM)

As the name suggests CPEDM 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.

Remote Privileged Access (RPA)

Since the Covid 19 pandemic, the prevalence of working from home has soared and some PAM vendors have responded by adding capabilities allowing privileged access directly from endpoints such as laptops.

Just in Time (JIT)

Implementing JIT within PAM can ensure that identities have only 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.

Single Sign-On (SSO)

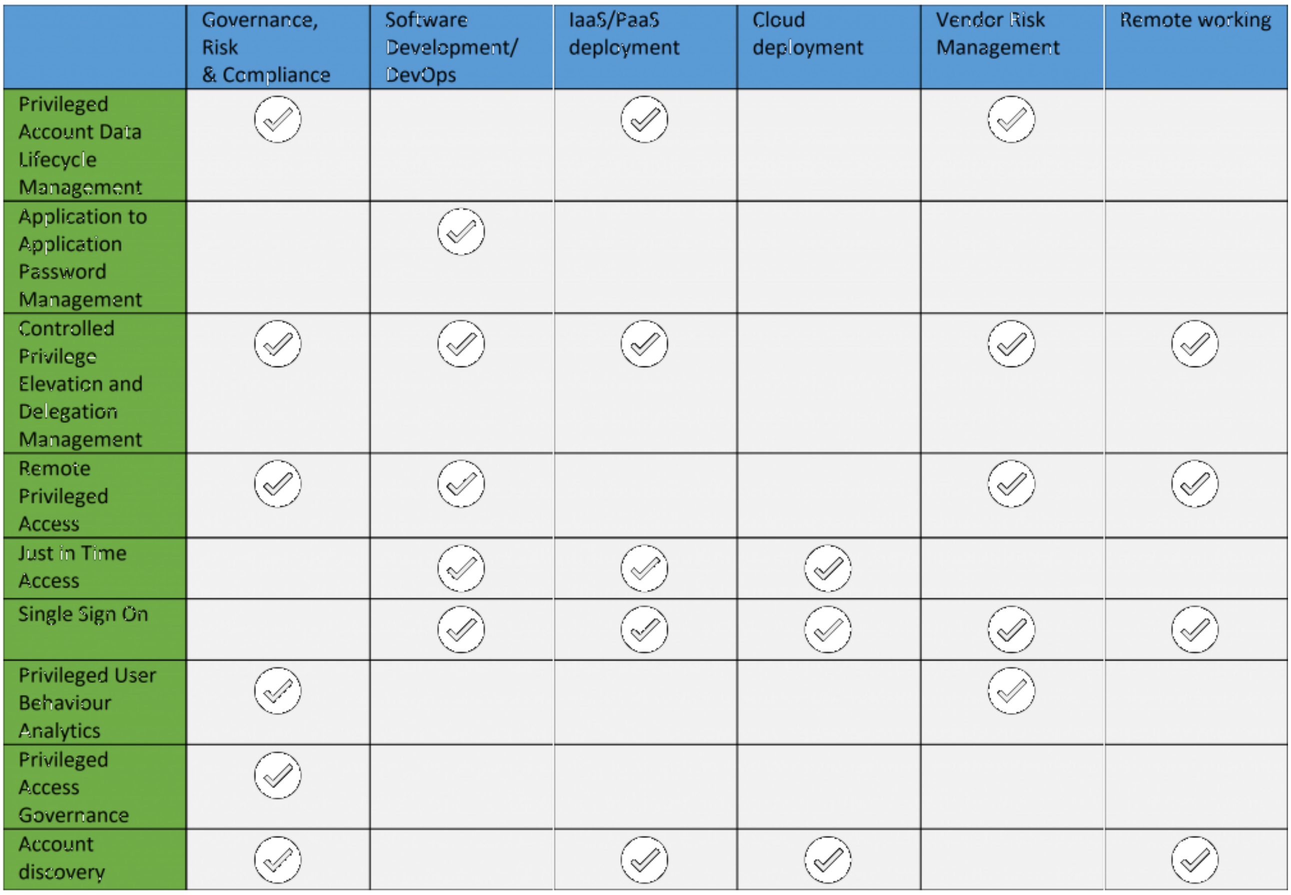
Single sign-on is a user authentication system that permits a user to apply one set of login credentials (i.e., username and password) to access multiple applications. Therefore, PAM solutions are increasingly supporting integration with leading SSO vendors to add convenience to PAM.

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.

Account Discovery

Some vendors offer modules that scan networks and endpoints to discover privileged accounts in use to enable better security and compliance.



	Governance, Risk & Compliance	Software Development/ DevOps	IaaS/PaaS deployment	Cloud deployment	Vendor Risk Management	Remote working
Privileged Account Data Lifecycle Management	✓		✓		✓	
Application to Application Password Management		✓				
Controlled Privilege Elevation and Delegation Management	✓	✓	✓		✓	✓
Remote Privileged Access	✓	✓			✓	✓
Just in Time Access		✓	✓	✓		
Single Sign On		✓	✓	✓	✓	✓
Privileged User Behaviour Analytics	✓				✓	
Privileged Access Governance	✓					
Account discovery	✓		✓	✓		✓

Figure 4: Optional PAM capabilities and the business IT use cases they can assist with.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Compass. The Compass provides a comparison based on standardized criteria and can help identifying vendors to be further evaluated. KuppingerCole recommends a comprehensive selection includes a subsequent detailed analysis and a Proof of Concept or pilot phase, based on the specific criteria of the customer.

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

- Product
- Innovation
- Market

2.1 Overall Leadership

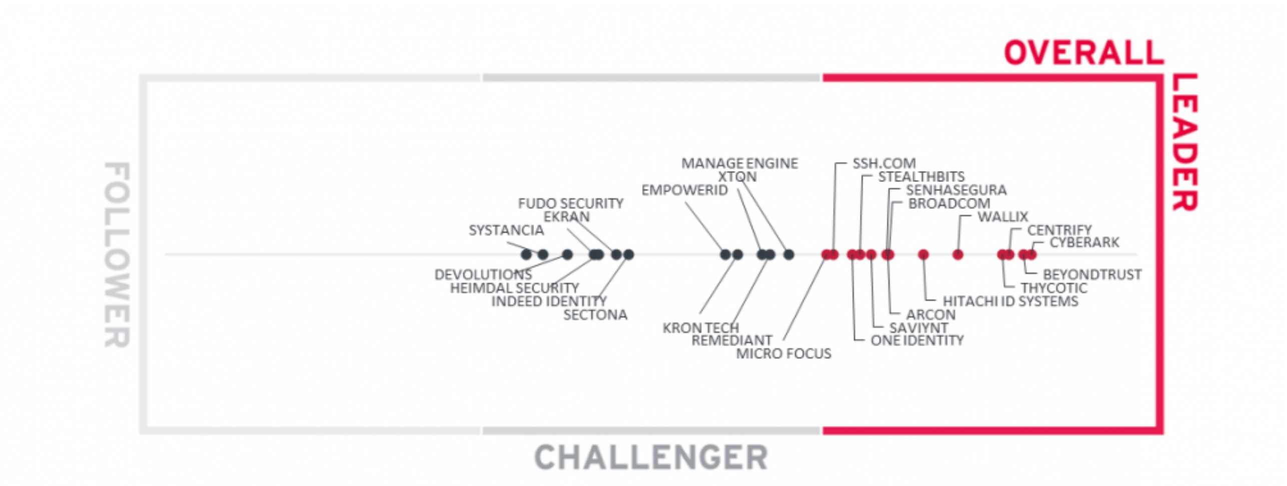


Figure 5: The Overall Leaders in Privileged Access Management.

When looking at the Leader segment in the Overall Leadership rating we can see that the number of overall vendors remains high at 26, with a couple of new vendors not seen in the 2020 Leadership Compass: Ekran and Heimdal. How much longer the market will support 26 vendors is an open question and the recent merger of Centrify and Thycotic will have ramifications for both those companies and their customers. For the purposes of this Leadership Compass the newly merged business asked that we consider both product suites separately, but the final post-merger entity will mean that the current "Big Four" -- CyberArk, BeyondTrust, Thycotic, Centrify will become the "Big Three" and the newly named ThycoticCentrify will have a responsibility to existing and new customers to offer a better product from the merger and compete effectively.

Of course, one of those in the chasing pack can close that gap significantly which currently includes WALLIX, Hitachi ID, Senhasegura, Broadcom (Symantec), Arcon, Saviynt, Stealthbits, One Identity, SSH.COM and Micro Focus. Certainly, some of those such as Senhasegura and Arcon have upped their game significantly in terms of capabilities and functionality -so little room for complacency among the Leaders.

The Challengers now comprise two distinct groups; the first - closer to the leaders - includes Manage Engine, Remediant, Xton, Kron Tech and EmpowerID who all offer a good mix of basic and some advanced PAM capabilities.

Then we see a close packed group of secondary Challengers which includes Sectona, Fudo Security, Indeed Identity, Ekran, Heimdal Security, Systancia and Devolutions. There are no Followers in the 2021 Leadership Compass suggesting a maturing of the market and capabilities with all now offering most basic capabilities but in well-designed packages that will find homes in organizations looking for simpler tools.

The Overall Leaders are (in alphabetical order):

- Arcon
- BeyondTrust
- Centrify
- CyberArk
- Hitachi ID
- Micro Focus
- One Identity
- Saviynt
- Senhasegura
- SSH.COM
- Stealthbits

- Broadcom (Symantec)
- Thycotic
- WALLIX

2.2 Product Leadership

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

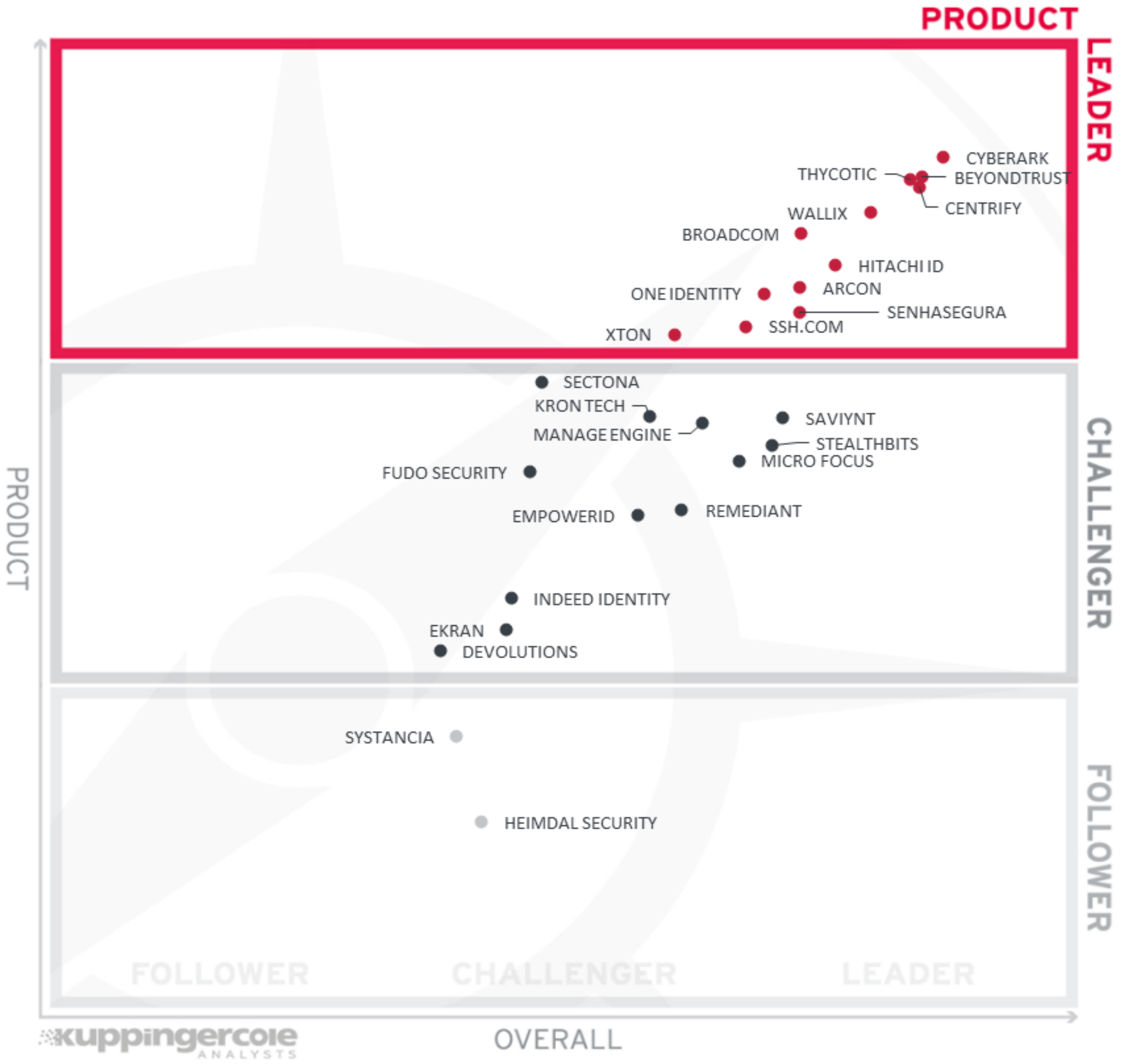


Figure 6: The Product Leaders in Privileged Access Management.

As mentioned in Chapter 2, *Required Capabilities,* the PAM market is still made up of a heterogenous mix of vendors that offer different capability levels with some of the leading platforms offering comprehensive levels of functionality through a modular approach while others offer the three basic capabilities which will still serve PAM to around 90% of most business IT tasks. However, there are also those vendors that offer basic capabilities but may well find a place in organizations looking for a specific PAM task in a discrete part of the IT architecture.

The overall trend remains for the leading PAM providers to add more specialist capabilities, especially in Analytics or DevOps deployments. One advantage of the modular approach is that buyers can buy into a vendor and add modular capability as and when scale demands extra PAM leverage. While there has been some consolidation (Thycotic and Centrify) the product choice remains wide in this sector. The market fluidity allows smaller players such as SSH.Com and Xton score as Leaders thanks to innovative approaches that fulfil more than basic capabilities with a lean code approach.

In the top tier of Product Leadership, we find CyberArk, BeyondTrust, Thycotic and Centrify but these are now more closely followed by WALLIX and Broadcom (Symantec) who have both improved product capability. Then we have the rest of the Leaders; Hitachi ID, Arcon, One Identity, Senhasegura, SSH.COM and Xton.

The Challengers are led by Saviynt, Stealthbits and Micro Focus followed by Sectona, Kron Tech, Manage Engine, Fudo Security, EmpowerID Remediant and then a group comprising Indeed Security, Ekran and Devolutions. Finally, the Followers are Systancia and Heimdall which have limited product capabilities but can still serve useful PAM functions to organizations.

The Product Leaders (in alphabetical order) are:

- Arcon
- BeyondTrust
- Centrify
- CyberArk
- Hitachi ID
- One Identity
- Senhasegura
- SSH.COM
- Broadcom (Symantec)
- Thycotic
- WALLIX
- Xton

2.3 Innovation Leadership

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 and other cutting-edge features, while maintaining compatibility with previous versions.

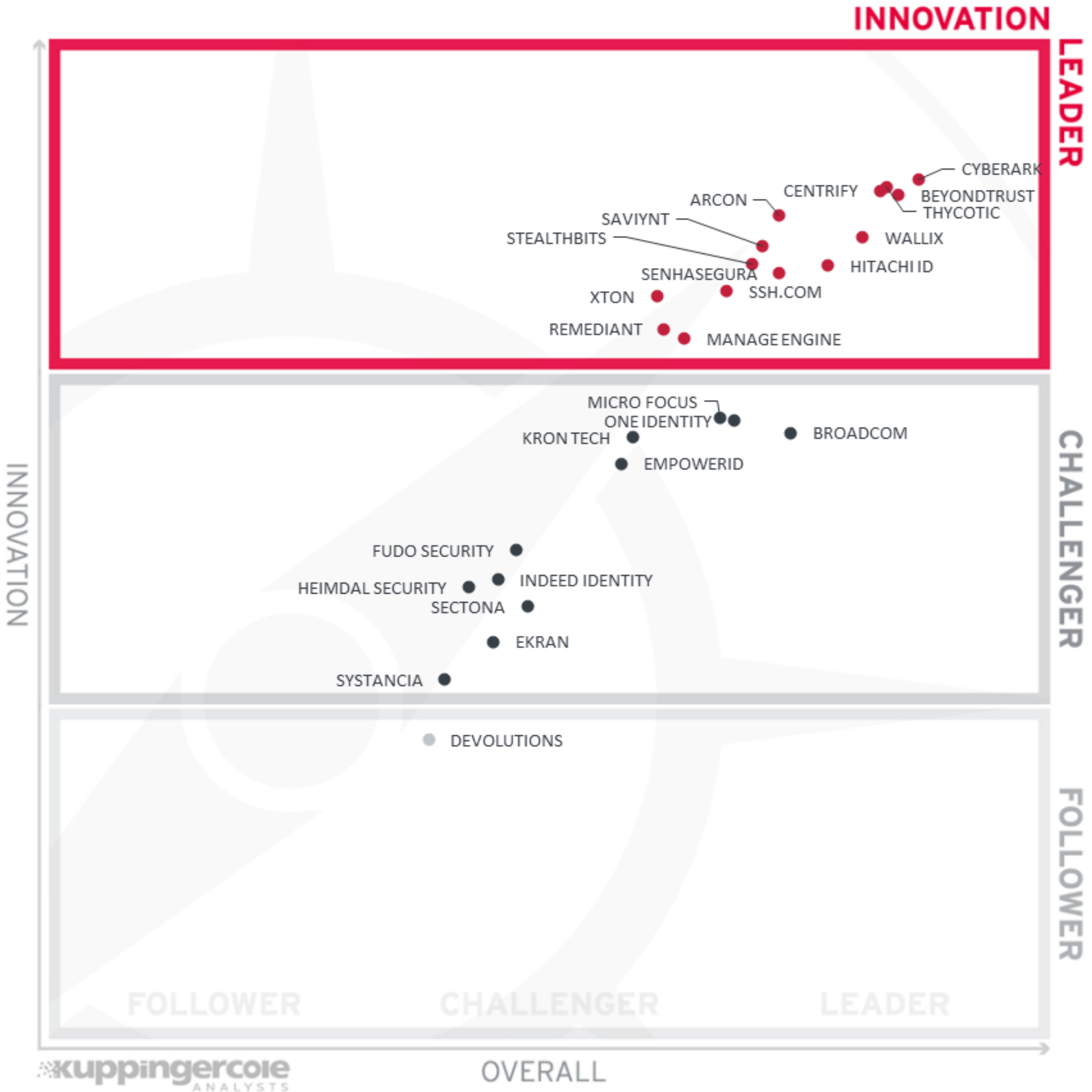


Figure 7: The Innovation Leaders in Privileged Access Management.

Innovation has been relatively strong in the PAM market in the last two years with vendors large and small adding to capabilities and making use of AI and Machine Learning in certain areas. We have also seen the entry of so-called lean PAM solutions, cloud-native PAM and vault-less/password-less solutions designed to shift PAM to a fully JIT model with Zero Standing Privileges (ZSP). At the same time, while these technology-forward solutions will find deployments, there remains plenty more conventional options that have also been enhanced by vendors in terms of performance and suitability for the widest number of business IT use cases.

For this reason, we still see the quartet of CyberArk, BeyondTrust, Thycotic and Centrify as Innovation Leaders as they strive to stay ahead of the pack and provide innovation and wide capability scope. CyberArk has also had something of a strategic shift with a new focus on Identity at the core of its product suite -- partly in response, we think, to the interest of Identity Providers into the PAM market.

Close to the leading quartet we see WALLIX, Hitachi ID, Stealthbits, Arcon, Saviynt, Senhasegura, SSH.COM, Xton, Remediant and ManageEngine, all of which have either improved capabilities or already benefit from innovation.

We have some Challengers split into two groups; the first comprises Micro Focus, One Identity, Broadcom (Symantec) and EmpowerID while the second also includes two newcomers to the Leadership Compass; Fudo Security, Indeed Identity plus Heimdal Security, Sectona, Ekran and Systancia. Devolutions remains as the solitary Follower in this grouping. There is innovation to be found here but it does not yet translate into a level that can support a wide mix of business IT functions.

The Innovation Leaders are (in alphabetical order):

- Arcon
- BeyondTrust
- Centrify
- CyberArk
- Hitachi ID
- ManageEngine
- Remediant
- Saviynt
- Senhasegura
- SSH.COM
- Stealthbits
- Thycotic
- WALLIX
- Xton

2.4 Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, 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.

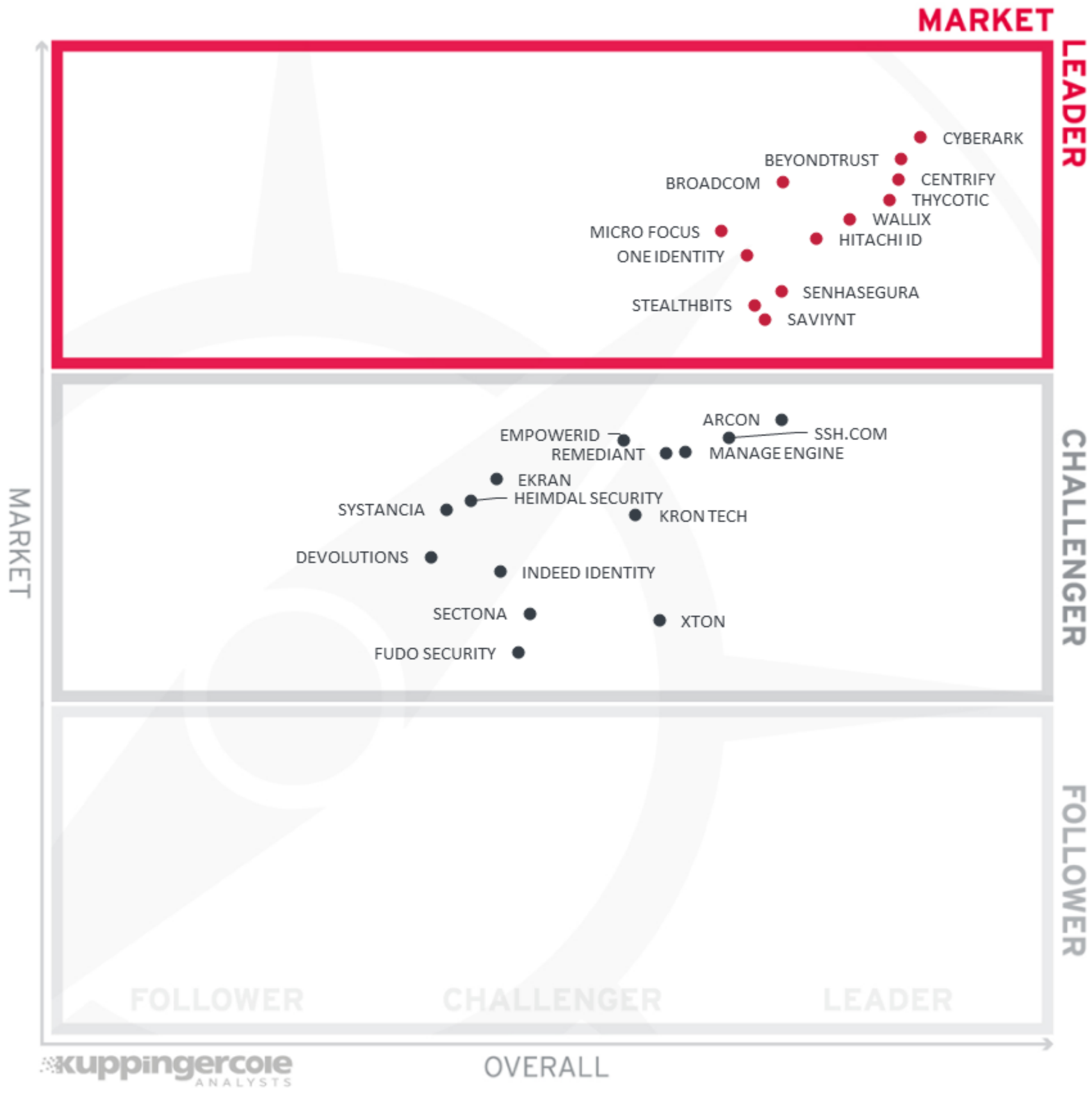


Figure 8: The Market Leaders in Privileged Access Management

There are no real surprises when it comes to Market Leadership with vendors with the largest customer base and market reach dominating the top right of the Leaders section. These are CyberArk, BeyondTrust, Centrify, Thycotic, WALLIX, Broadcom (Symantec), Hitachi ID and Micro Focus. Not all these are the most innovative or feature rich but they are backed by the financial resources of multinational tech businesses; Hitachi ID, Broadcom (Symantec) and Micro Focus come into this category, making them a safe buy that should benefit from future investment. There is another group of Leaders just below these which comprise One Identity, Senhasegura, Stealthbits and Saviynt.

After that we have an evenly bunched group of vendors that make up our Challengers. These are Arcon, SSH.COM, EmpowerID, ManageEngine, Remediant, Ekran, Heimdal Security, Systancia, Kron Tech, Devolutions, Indeed Identity, Sectona, Xton and Fudo Security. There are no Followers.

The Market Leaders are (in alphabetical order):

- BeyondTrust
- Centrify
- CyberArk
- Hitachi ID
- Micro Focus
- One Identity
- Saviynt
- Senhasegura
- Stealthbits
- Broadcom (Symantec)
- 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.

The first of these correlated views contrasts Product Leadership and Market Leadership.

3.1 The Market/Product Matrix

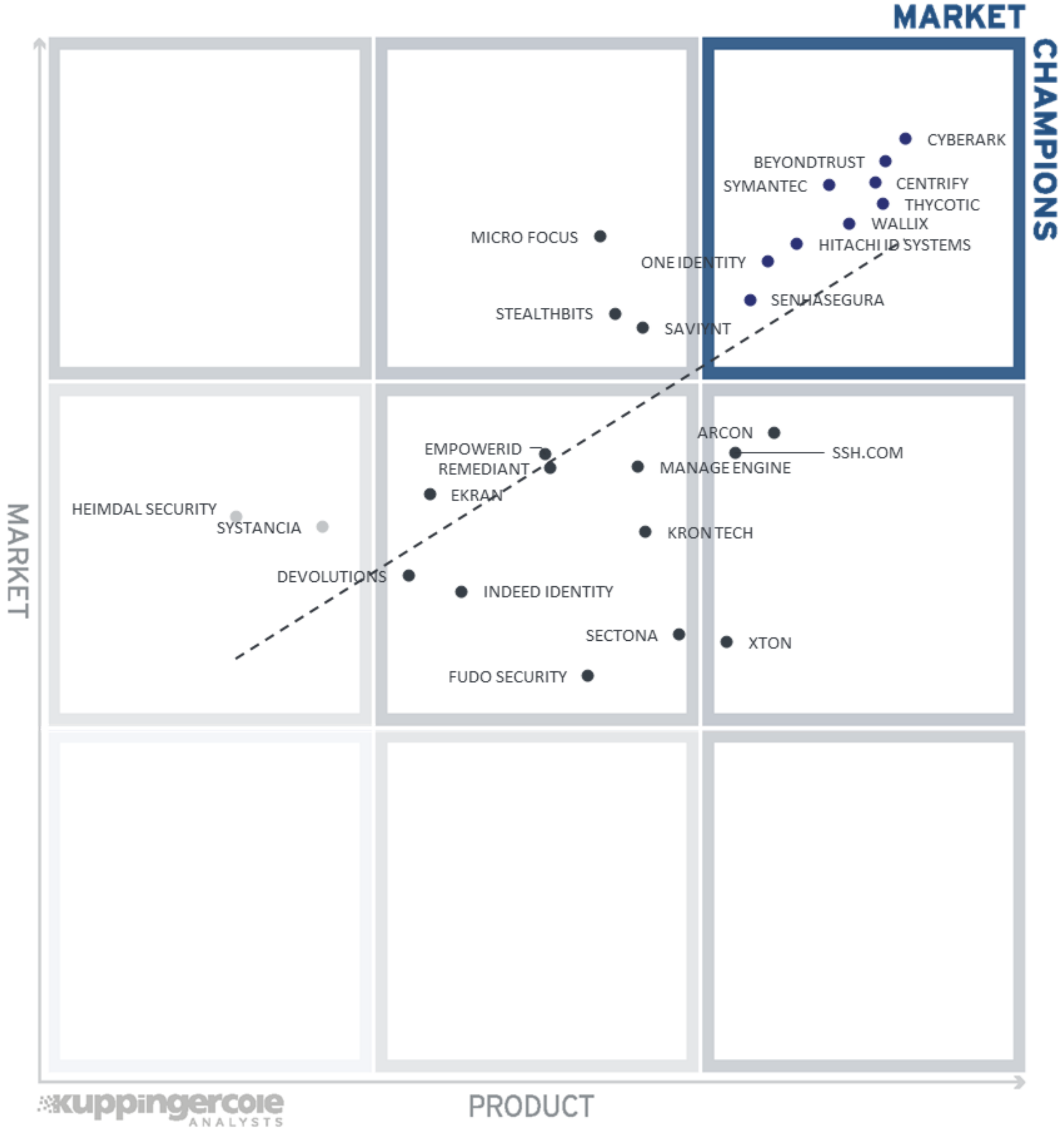


Figure 9: The Market/Product Matrix for Privileged Access Management.

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.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The Market Champions here are CyberArk, BeyondTrust, Broadcom (Symantec), Centrify, Thycotic, Hitachi ID, WALLIX, Senhasegura and One Identity. They are closely followed by the trio of MicroFocus, Stealthbits and Saviynt. All can offer a good range of capabilities along with market solidity making them a safe investment bet for many organizations.

The next group of vendors; EmpowerID, Ekran, Heimdal Security, Systancia - all offer more limited sets of capabilities but represent a good choice for certain organizations and IT environments. Finally, the group that consists of Arcon, SSH.COM., ManageEngine, Kron, Indeed Identity, Sectona, Xton and Fudo Security also have some great capabilities which we feel could benefit from more effective marketing to compete better (Xton may benefit from its recent acquisition in this area).

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. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

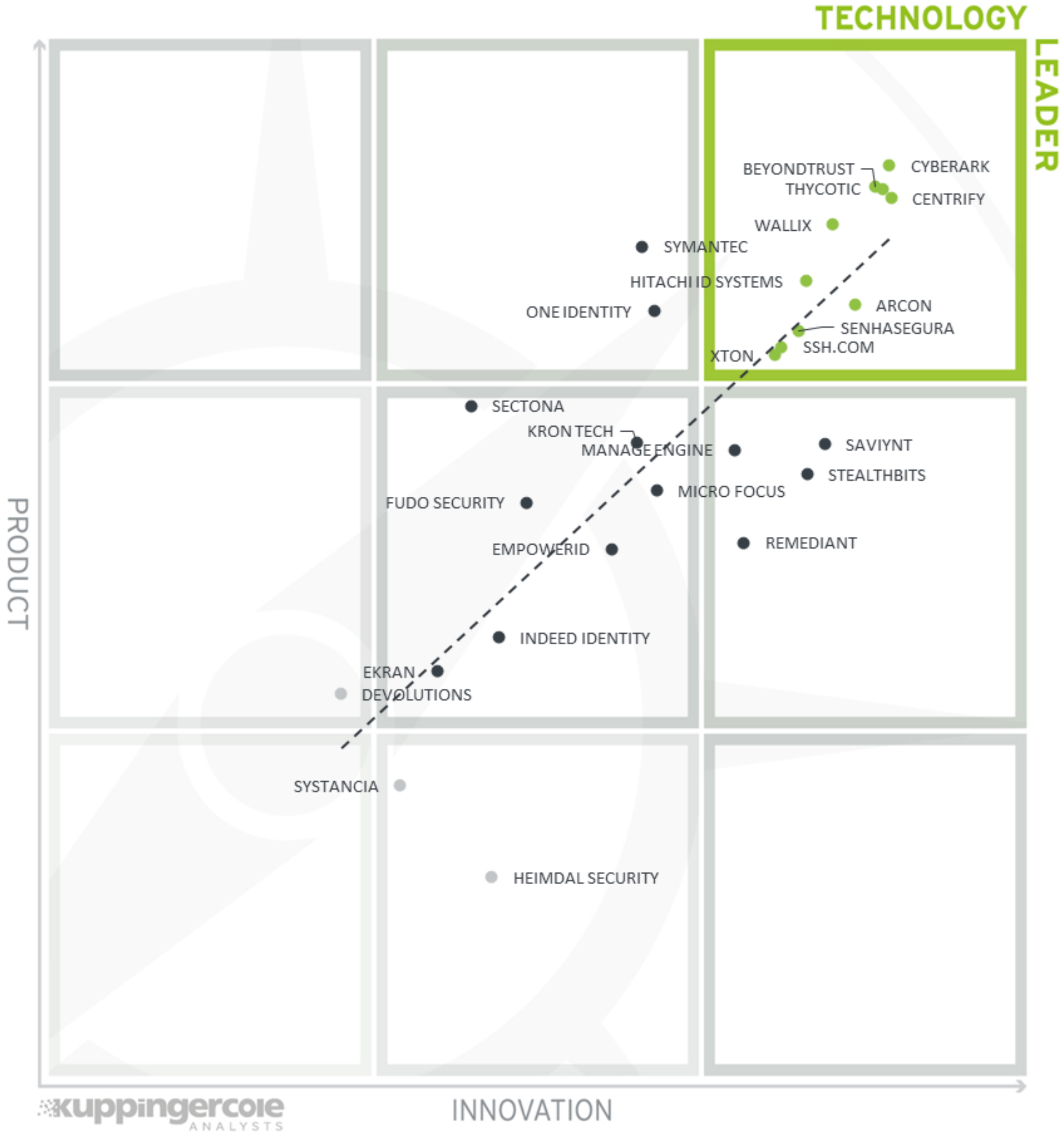


Figure 10: The Product/Innovation Matrix for Privileged Access Management.

Innovation is important in this market given its core role in reducing the risk involved in matching identities to tasks. The Leaders are no real surprises here and include CyberArk, BeyondTrust, Thycotic, Centrify, WALLIX, Hitachi ID but also some smaller but innovative players such as Arcon, Senhasegura, SSH.Com and Xton -- who are driving innovation through more nimble product architectures.

Broadcom (Symantec) and One Identity are found in the top centre box with strong product offerings but not quite among the leaders. In the center box we see a cluster of vendors close to the line; Kron, Micro Focus, EmpowerID, Indeed identity and Ekram. With only a couple of outliers we see that most vendors are performing well in terms of product and innovation, and size is no impediment to innovation or specialization.

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 who 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.

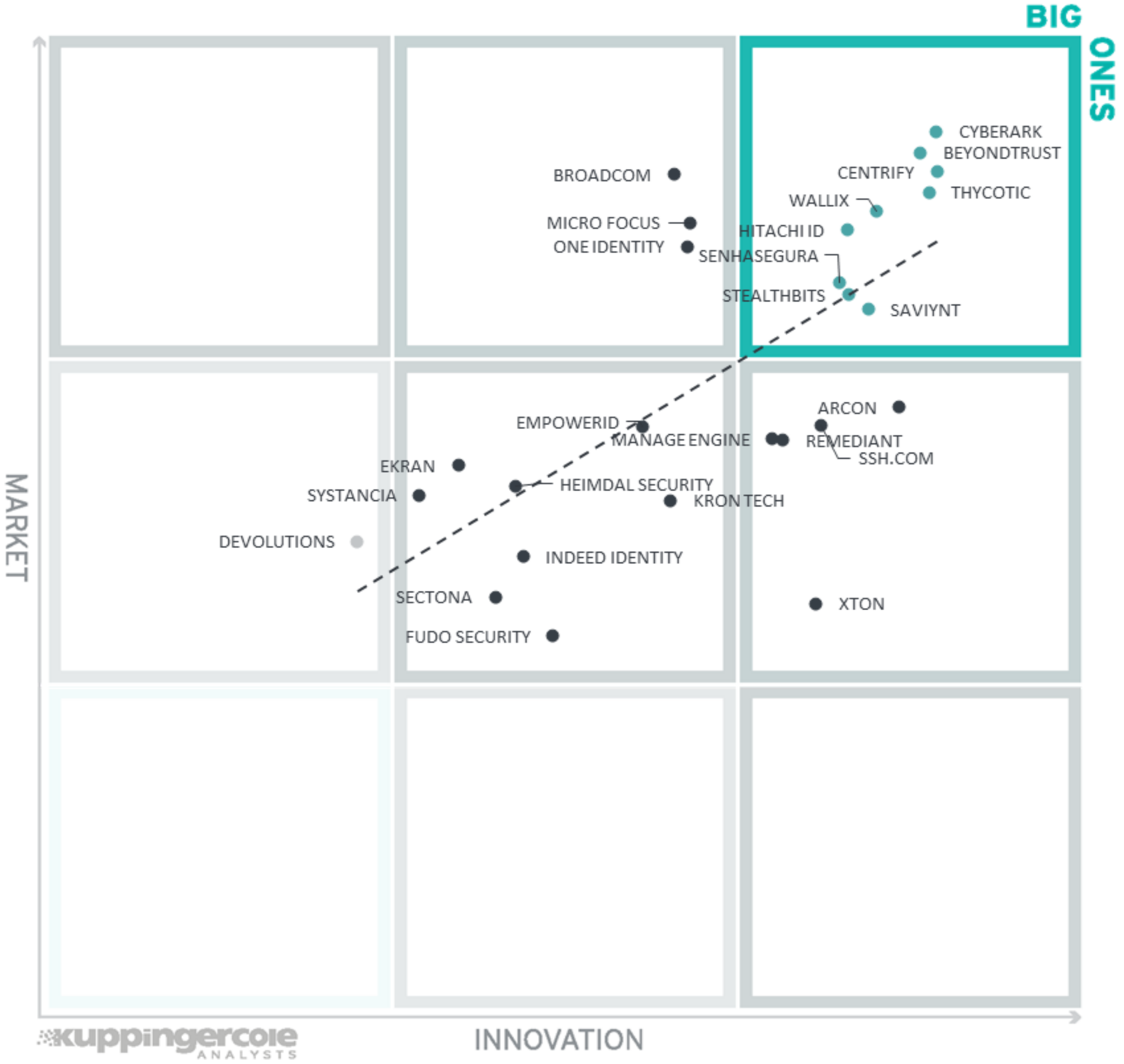


Figure 11: The Innovation/Matrix for Privileged Access Management.

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

In the final matrix we see the Big Ones as CyberArk, BeyondTrust, Centrify, Thycotic, WALLIX, Hitachi ID, Senhasegura, Stealthbits and Saviynt who are benefitting from established or greatly improved market positions which impacts on their capabilities and innovation strengths. In the top centre box we find Broadcom (Symantec), Micro Focus and One Identity who are slightly under performing in innovation relative to their strong market position.

In the centre right box, we see Arcon, Remediant, SSH.COM and Xton who we believe have enough innovation in their products to fuel further growth. The middle of the matrix is taken up by a cluster of vendors who include EmpowerID, ManageEngine, Ekran, Heimdal Security, Kron Systancia, Sectona and Fudo Security representing a midrange performance of innovation relative to market strength.

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. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. 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.

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 PAM	●	○	○	●	○
BeyondTrust Universal Privilege Management	●	●	○	●	●
Broadcom Symantec PAM	●	●	●	○	○
Centrify PAM Platform	●	●	●	●	●
CyberArk Identity Security Platform	●	●	●	●	●
Devolutions Server and Password Hub	○	🟡	🟠	🟠	🟡
Ekran System Lightweight PAM	○	🟡	🟡	🟡	🟡
EmpowerID Privileged Session Management	○	🟡	🟡	○	🟡
FUDO Security PAM	○	🟡	🟡	○	○
Heimdal Privileged Access Manager	🟡	🟠	🟠	○	🟡
Hitachi ID Bravura Privilege	●	○	○	●	●
Indeed Identity Privileged Access Manager	○	🟡	🟡	🟡	🟡
Krontech Ironsphere	○	○	○	○	○
ManageEngine PAM360	○	○	○	○	🟡
Micro Focus NetIQ Privileged Account Manager	●	●	●	○	🟡
One Identity Safeguard	●	○	○	●	○
Remediant SecureOne	○	🟡	○	●	○
Saviynt Cloud PAM	●	○	○	○	○
Sectona Security Platform	●	○	○	○	○
Senhasegura PAM	●	○	○	○	○
SSH.COM PrivX Lean PAM	●	○	○	●	●
Stealthbits SbPAM	●	○	○	○	○
Systancia Cleanroom	●	🟡	🟡	○	🟡
Thycotic Secret Server	●	●	●	●	●
WALLIX Bastion	●	●	○	●	○

Product	Security	Functionality	Interoperability	Usability	Deployment
Xton Access Manager (XTAM)	●	🟢	🟢	🟢	🟢
Legend	🔴 critical	🟠 weak	🟡 neutral	🟢 positive	● strong positive

Table 1: Comparative overview of the ratings for the product capabilities.

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	🟢	🟡	🟡	🟢
BeyondTrust	🟢	🟢	🟢	🟢
Broadcom Inc.	🟩	🟢	🟢	🟢
Centrify	🟢	🟢	🟢	🟢
CyberArk	🟢	🟢	🟢	🟢
Devolutions	🔴	🟡	🟡	🟡
Ekran	🟠	🟡	🟡	🟩
EmpowerID	🟡	🟩	🟩	🟩
Fudo Security	🟠	🟡	🟠	🟠
Heimdal Security	🟠	🟡	🟩	🟡
Hitachi ID Systems	🟩	🟢	🟢	🟢
Indeed Identity	🟠	🟡	🟢	🟠
Krontech	🟡	🟡	🟡	🟡
ManageEngine	🟩	🟩	🟩	🟡
Micro Focus	🟡	🟢	🟢	🟩
One Identity	🟡	🟩	🟩	🟢
Remediant	🟩	🟡	🟡	🟩
Saviynt	🟢	🟩	🟩	🟩
Sectona	🟢	🟡	🟡	🟡
Senhasegura	🟢	🟩	🟩	🟢
SSH Communications Security	🟩	🟩	🟩	🟡
STEALTHbits Technologies	🟢	🟢	🟢	🟡
Systancia	🟡	🟩	🟡	🟡
Thycotic	🟢	🟢	🟢	🟢
WALLIX	🟩	🟢	🟢	🟢
Xton Technologies	🟩	🟡	🟡	🟡
Legend	🔴 critical	🟠 weak 🟡 neutral	🟩 positive	🟢 strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor 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 the LC PAM, we look at the following eight categories:

- Endpoint Privilege Management
- High Availability
- Dashboard Tools
- Analytics & Reporting
- Account Discovery
- Machine Access
- Just in Time Access
- Architecture

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, and is offered in software, virtual and physical appliances and a PAM as a Service (PAMaaS) option.

Taking a fully integrated browser approach to PAM controls, and APIs to connect to component parts, ARCON now has one of the more comprehensive PAM offering on the market, putting it in close contention with the established leaders. ARCON has made further good use of its browser-based approach. During session management, for example, Admins can open multiple sessions as tabs, and open another while waiting for approval in another -- saving time and resources.

The Session monitoring dashboard offers standard and more advanced analytics. Users can also run multiple video logs at the same time -- good for live interactive analytics. ARCON also provides its proprietary Knight Analytics software which delivers an aggregate risk score to access and usage anomalies and can initiate threat detection.

There is Smart Session Monitoring. Authentication is by SSH key and not passwords and authentication takes place on the login page to ARCON. There is auto-onboarding that can be integrated with Active Directory and AWS for service onboarding. The OnBoard Server can identify groups in AD. The interface mixes the best of consumer tech design with touches such as "My Apps" for Admins. The ARCON EPM module can control what users do at the endpoint and is now based on JIT processes.

ACON has made an impressive number of improvements to its platform since 2020. A new Robotics Connector Platform helps to automate mundane tasks and users can customize steps for any SSO Connector or Password Connector. Integrated tasks now include application password management when previously only available via GUI. The Global Remote Access Solution allows remote users to establish a connection to their assigned desktop/machines from when on the road.

My Vault is now offered as a discrete solution (with or without PAM). The solution is based on a microservices framework and is built for the cloud (it can also be installed on-premise for PAM customers). The solution has advanced features like onboarding user groups, tagging businesses, workflow, Just-in-Time access to Secrets, Keys, Certificates, Files, etc. Further, users can deploy role-based access for sharing, downloading, viewing, or transferring files and secrets.

ARCON Digital PAM is a PAM solution for Non-Human Identities, leveraging native application attributes and role-based access controls to authenticate applications and containers. It can manage and pass credentials securely to validated containers and clusters when required.

Finally, PAM lite is a multi-tenancy solution that offers only key PAM features including: SSO, Session Monitoring, Password Vault and Reports. This solution is very useful for SMEs as it is simple to deploy and use, hosted in either AWS or Azure.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○

arcon

Strengths

- Design works well with strong focus on compliance
- Strong, dedicated analytics come as part of the package
- Dashboard and interface make this easy to learn and to use
- Good understanding of the needs of EPM and RPA in the era of hybrid working
- Ease of deployment and administration
- Readily integrable with standard SIEM and help-desk tools
- Incremental improvements show vendor is listening to the market

Challenges

- Interface still not quite up to the current best standards but is based on easily improved HTML5 foundation
- ARCON need to improve its marketing of what is now a highly competitive PAM platform
- The platform would benefit from further DevOps native integration

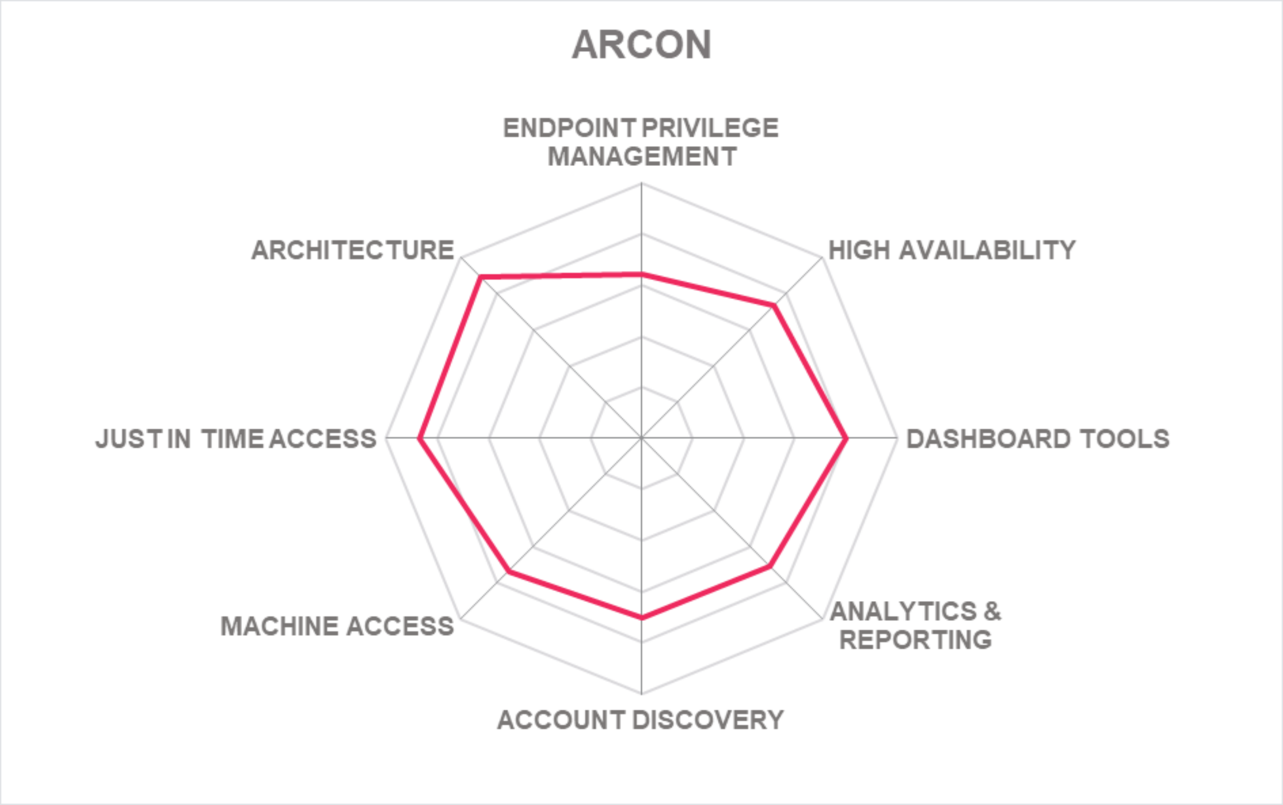
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


ARCON
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.2 BeyondTrust

BeyondTrust has continued to refine its portfolio of PAM products which now includes the Password Safe and DevOps Secrets Safe products, Endpoint Privileged Management (EPM) tools (for Windows, Mac, Unix and Linux), the Remote Support and Privileged Remote Access products, and the new Cloud Privilege Broker product. There is also BeyondInsight, a separately available analytics package. All now benefit from an upgraded and consistent UI -- in line with market trends.

This collection makes it one of the most comprehensive on the market, covering all the recognized functionalities of a PAM suite and takes account of the global interest in securing Privileged Access for home working. BeyondTrust PAM can be deployed on cloud, as hybrid and on-premises. A SaaS option is available for Password Safe, Endpoint Privilege Management and Remote Support products.

Since our last Leadership Compass, BeyondTrust has added new capabilities across the board. These include Azure AD support and a new web policy editor in Privilege Management, plus YubiKey support. DevOps Secret Safe now benefits from Dynamic Account Generation and full Kubernetes & Ansible Integrations. Endpoint Privilege Management sees Streamlined Vendor Onboarding & Linux Jump Points while Remote Support sees the arrival of Chatbot APIs, Android & Mac compatibility, Chrome Screen Sharing, & Zebra Technology Support Deployment, again reflecting the focus on secure remote working.

BeyondTrust has also introduced new Cloud/SaaS deployment options for Password Safe and Privilege Management for Windows & Mac and each offers feature parity to the on-premises versions. There is now increased support for 3rd-party integrations via an expanded API set, with SCIM support added to the Secure Remote Access products and a new integration with ServiceNow Customer Service Management module.

A small but important change is the removal of FLASH support from Password Safe which is now fully HTML5 compliant. BeyondTrust says it has boosted R&D investment 40% YoY and of interest is the foundation of a new Ransomware/Malware Research Lab which to lead further development. Given the serious threat that Ransomware now poses to global business this is a welcome move by the company.

Finally, the new Cloud Privilege Broker (CPB) is architected on a next-generation platform for managing cloud access risk and governance of entitlements in hybrid and multi cloud environments. Overall, a busy and highly productive year of product development for one of the market leaders.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

BeyondTrust

Strengths

- BeyondTrust has built on existing strengths and added sensible and needed capabilities in line with market needs
- Proven enterprise-class solution that is scalable and available on-premises or in the cloud
- 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

- Vendor website can still be a little confusing in presenting the features of PAM products, making selection harder for some buyers
- If Identity focused PAM platforms gain traction, BeyondTrust may find itself behind the curve despite its undoubted capability breadth
- Some further product integrations may be useful, and it is likely we will see that in the next 12 months

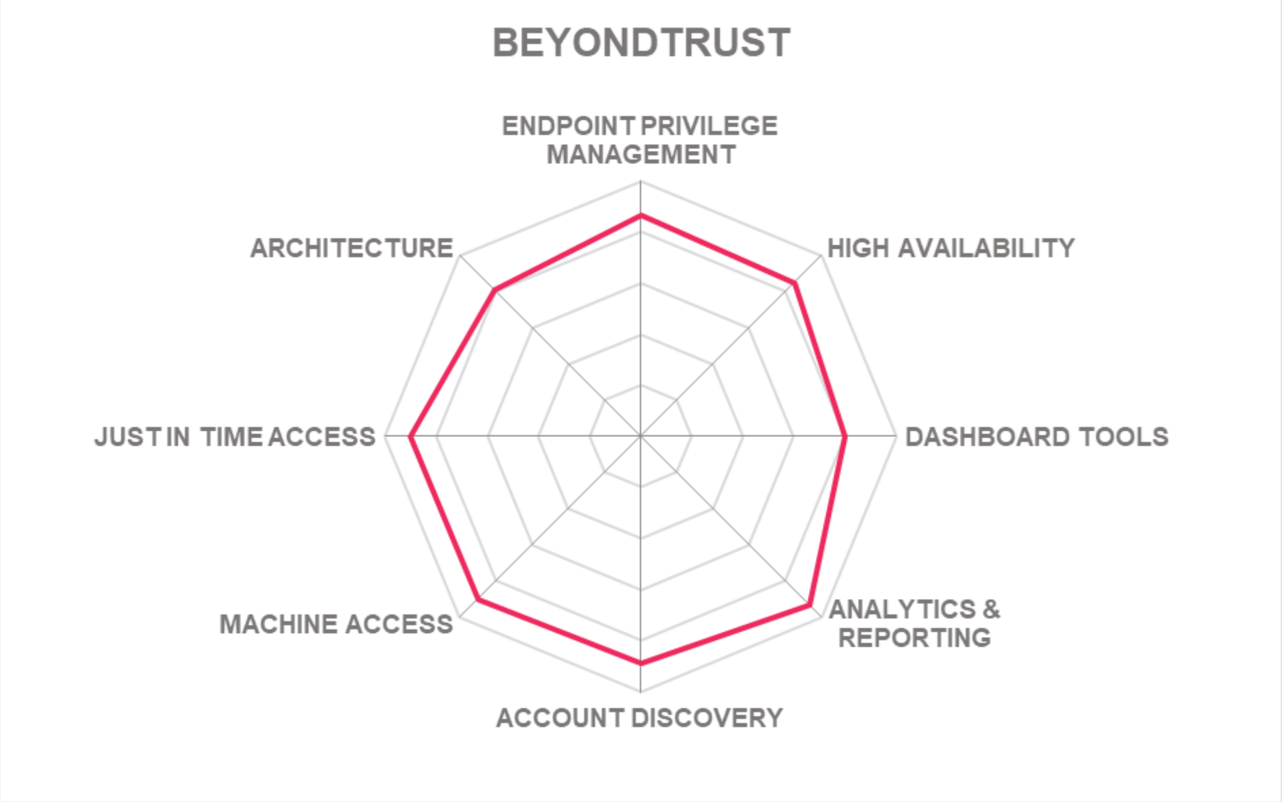
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


BEYONDTRUST
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.3 Broadcom Inc.

Broadcom has now rationalized all its identity products into the Identity Management Security Division of Broadcom Software, including this PAM platform marketed as Symantec PAM. In addition, Broadcom has beefed up marketing with a new digital sales team for its around 15,000 accounts.

There have been more significant technical developments, however, as Broadcom has now fully consolidated the PAM suite it inherited from CA. This puts all key components, Vault, Access Manager, PAM Server Control and Analytics under the control of one appliance. A new and improved console benefits from an improved UX, and single pane of glass access but still lags some of the leaders in advanced usability design for PAM.

The PAM Server Control offers an agent-based architecture to intercept control and restrict commands at OS Kernel level. It is notable for its fine-grained access control able to block Root access to a file or give one specific account access to a file or service. Policies can be upgraded through the central console. The Threat Analytics engine delivers advanced threat analytics leveraging machine learning techniques for automated detection of risky privileged behaviour.

The solution is designed well for hybrid environments with AWS and Azure support and Broadcom 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. Yet, there is not a SaaS version or fully native DevOps module or components and these would enhance Symantec PAM further.

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 if so desired. The flipside is that for many organizations, Broadcom offers a tried and tested PAM one stop solution that offers 100% of the desired capability options -- if not yet a technology leader in all of them.

The affinity with CA's former IAM products remains and Symantec's customer history shows that this PAM platform can scale to multiples of 100k of devices and users and is at home in hybrid IT environments. A solid choice and one that may now flourish under the Symantec Enterprise Security umbrella if further IAM integration plans come to fruition -- as with other vendors, marrying IAM and PAM is seen as the next step forward.

BROADCOM®

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

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

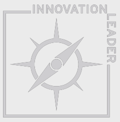
Challenges

- Support for DevOps is present but needs finessing
- Having committed to the brand and product, Symantec's parent needs to invest further to place its platform among the top Leaders
- Remains a lack of focus on mid-market segments and SaaS options

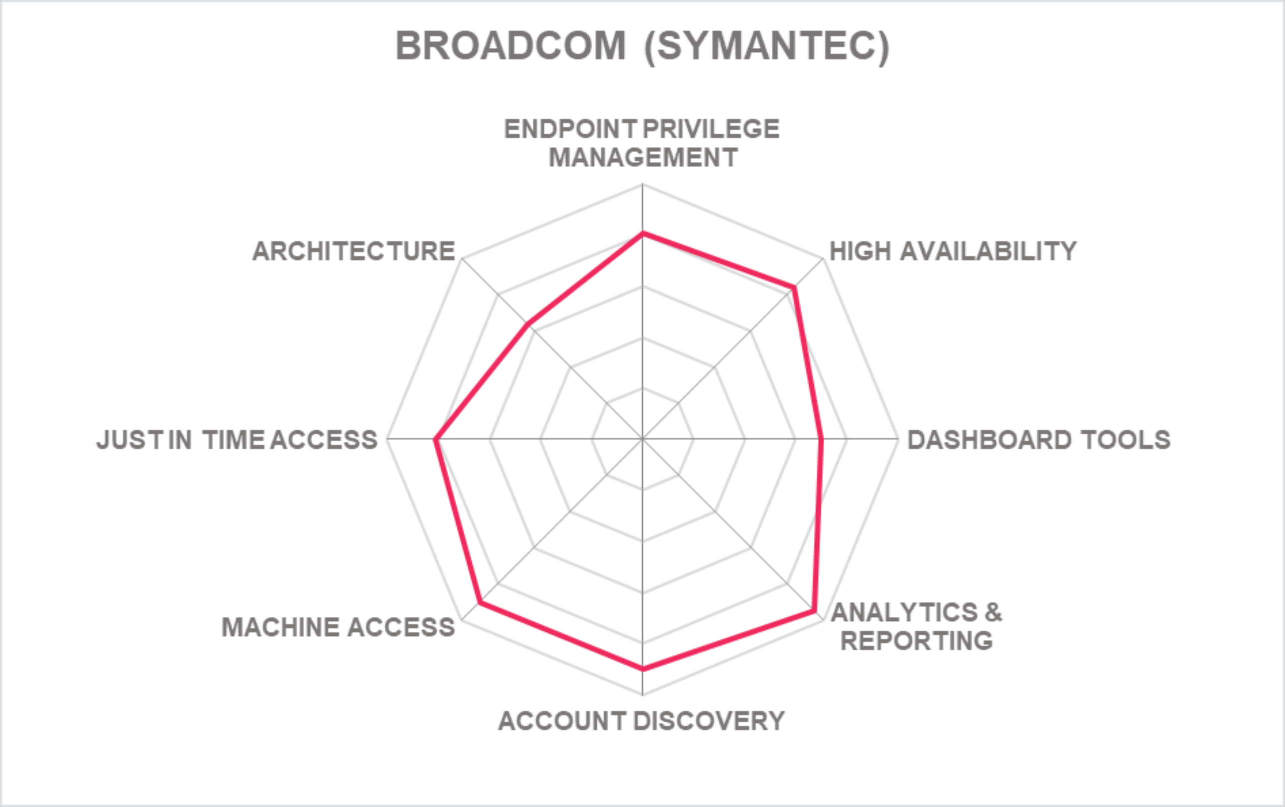
Leader in

OVERALL
LEADER

PRODUCT
LEADER



MARKET
LEADER


BROADCOM (SYMANTEC)
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.4 Centrify

Based in the US, Centrify offers several PAM modules as part of an overall suite which includes credential and secrets vaulting, privilege access, authentication, privilege elevation, auditing, and analytics. Privileged Access Service (PAS) is Centrify's PAMaaS solution. The company recently merged with Thycotic but for now the product continues to be sold and supported separately.

Compatible modules include Centrify Authentication Service, Centrify Privilege Elevation Service, Centrify Threat Analytics Service and Centrify Audit & Monitoring Service (compatible with Micro Focus, ArcSight, IBM QRadar, and Splunk SIEM tools).

The Centrify Privileged Access Service (PAS) provides password vaulting, offering SAPM, secure administrative access via a distributed local jump box and includes secure remote access for privileged users to target systems .

Centrify Authentication Service authenticates Privileged credentials against Active Directory (AD), LDAP, or a cloud directory such as Google Cloud Directory or Centrify Directory, depending on customer choice. It also offers adaptive MFA and identity consolidation in addition to UNIX/Linux -Active Directory (AD) bridging.

Centrify Privilege Elevation Service provides Just-in-Time (JIT) privileged across Windows, Linux, and UNIX and centralized policy management from Active Directory (AD). Administrators can set Privileged Elevation Service to control access based on roles and job functions.

The Centrify Platform provides shared services to all Centrify PAM products. It includes typical PAM services (such as discovery, MFA, and workflow) as well as brokered identity, Delegated Machine Credentials, client-based password reconciliation, and a secure token service.

A strength of Centrify's suite is its Threat Analytics Service which uses machine learning to identify anomalous behaviour in real time. This then activates set policies for users who are accessing the Centrify vault, initiating a privileged session, or checking out a password.

Dynamically enforced access policies grant the user access, prompt for a second factor of authentication (MFA), or block access completely, based on a risk score derived from the user's context and previous behaviour.

Centrify Privileged Access Service supports DevOps with its vault being able to store IP addresses, API keys, SSH credentials and AWS IAM credentials and the Delegated Machine Credentials solution can incorporate PAM into DevOps using the Centrify Vault. There is enhanced management for application secrets though the new Secrets Workflow tool found in PAS.

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 system usage free of charge.

Since 2020, Centrify has added the following core enhancements: Delegated Machine Credentials, Client-based Password reconciliation, SSH key management and discovery using an SSH key Windows UAC elevation using a cloud user credentials, ability to launch RDP connections without visiting the Privileged Access Service portal and automatically manage discovered accounts. There is also local Windows Workstation administrator vaulting and Password reconciliation for local accounts on Windows workstations.

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
- Centrify Privilege Threat Analytics Service uses machine learning to identify anomalous behaviour in real time

Challenges

- Merger with Thycotic may now lead to period of uncertainty and loss of momentum in the market as product lines must rationalise
- Still lacks fully comprehensive Endpoint Privilege Management capabilities
- Centrify’s product positioning and delineation remains confusing to buyers, but merger may improve this

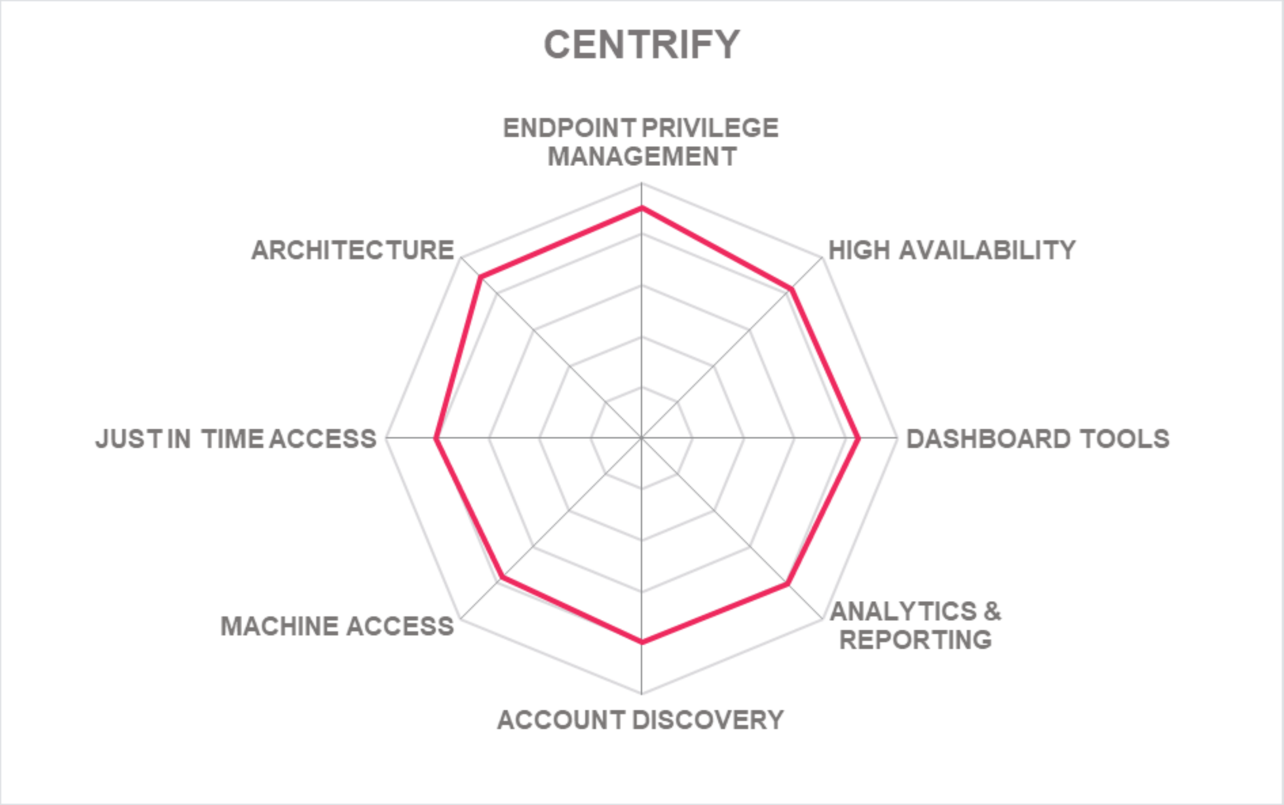
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


CENTRIFY
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.5 CyberArk

Headquartered in Israel and the US, CyberArk is a highly mature PAM provider 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.

The full CyberArk portfolio includes CyberArk Privileged Access Manager available as self-hosted or as PAMaaS (CyberArk Privilege Cloud); its PAM for DevOps product, Conjur Secrets Manager; CyberArk Remote Access for vendors, third parties and privileged employees from remote locations; and CyberArk Endpoint Privilege Manager (EPM). CyberArk EPM removes local administrator rights from endpoints and offers temporarily elevated privileges for specific tasks in real-time. As an example of proactive defence, it also protects against the SolarWinds Orion-style credential theft.

Within those products are pretty much all the key technical capabilities for managing PAM in modern IT environments that KuppingerCole recommends as part of an IAM blueprint. Since the acquisition of Idaptive in May 2020, the company has worked hard to integrate the acquired Access Management technology with existing in-house developed offerings.

More boldly perhaps, CyberArk has started to rebrand the business around this enhanced product portfolio as an Identity Security vendor, encompassing IAM, PAM and Cloud management. This messaging may take some ironing out but get it right and it will be a canny move to stay ahead of growing interest in the PAM market from IAM vendors. It also dovetails well with KuppingerCole's Identity Fabric model for organizations.

CyberArk has made numerous other enhancements across its suite in the last 12 months, consolidating its leadership in 2020. In Conjur, its DevOps product, segregation of data between different environments using the same vault is now possible by synching different secrets to different Conjur Enterprise instances. There is also now native authentication support for Azure and Google Cloud Platforms. Cloud Entitlements Manager, a new SaaS offering introduced in November 2020, uses AI-powered detection and remediation of hidden, misconfigured, and unused permissions across an organization's cloud environments.

Also, Linux administrators can now connect to multiple target servers through Privileged Session Manager for SSH for either interactive sessions, remote commands execution or files transfer, while being required to perform MFA only once in a short, configurable period. Nice.

A new unified inbox for EPM consolidates three key modules: Privilege Management, Application Control and Privileged Threat Protection and a new Event Management interface delivers an improved view of all important events running in the environment. CyberArk continues to keep pace with current UX and UI deign languages.

CyberArk also offers in depth analytics, session management, elevation management and AAPM technologies across its suite of products. The products on offer here remain the benchmark in integrating new capabilities with tried and tested technology while keeping up with new challenges such as remote access, DevOps, cloud and identity management integration.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

CYBERARK®

Strengths

- One of the widest support levels for platforms and deployments
- Has continued to add features in the last year to maintain leadership
- CyberArk is an independent 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 unfavourable for certain deployments
- Complete solution may be overkill for some smaller PAM deployments, but PAMaaS is a step forward here
- With two of its major rivals embroiled in a merger, the only danger could be complacency, but we don’t think that will happen

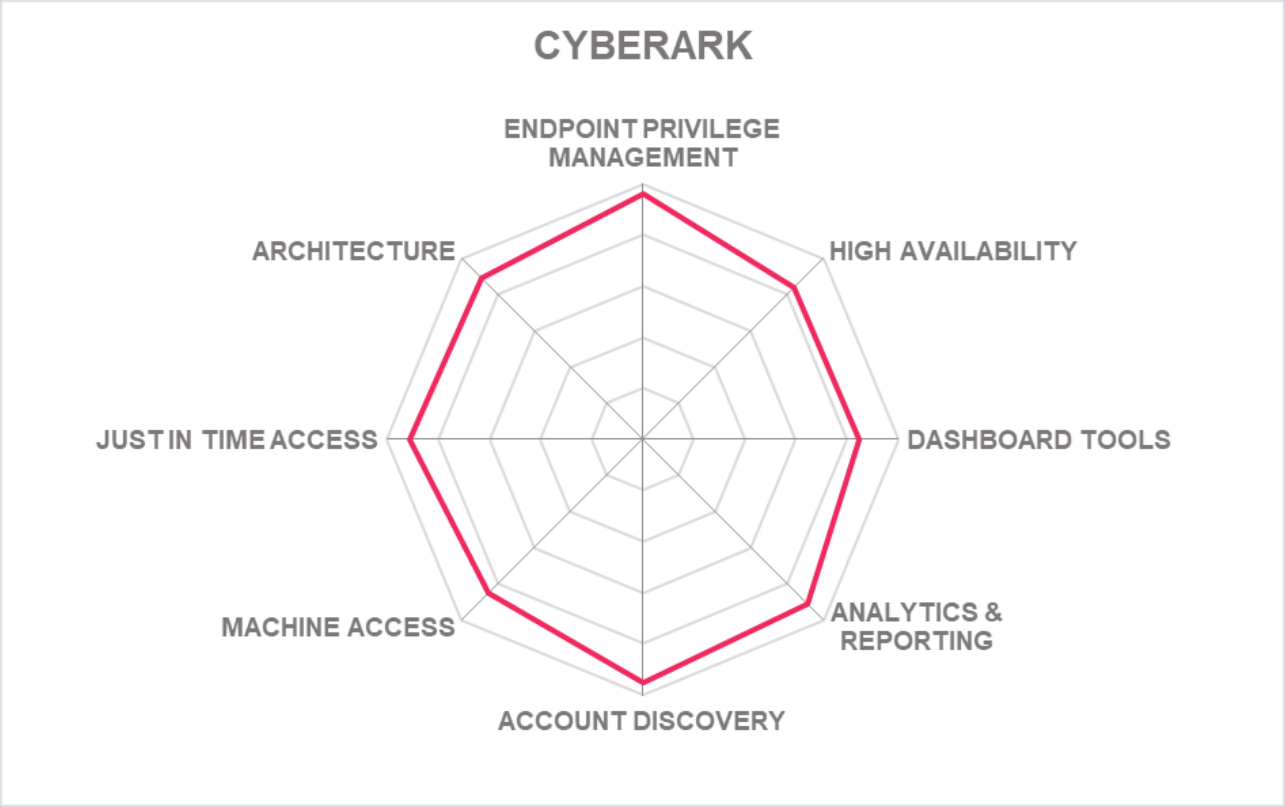
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


CYBERARK
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.6 Devolutions

Founded in 2010, Canadian firm Devolutions started with its Remote Desktop Manager aimed at SMBs. It has since added PAM solutions to its portfolio with Devolutions Server and Password Hub, also aimed at smaller businesses.

The two PAM products offer essential capabilities such as a central password and credentials vault which can integrate with Microsoft Active Directory. It also offers account discovery and secure remote access. But for a package that is created with SMBs in mind it has several enterprise capabilities including session recording and playback, automated password check in/check out and SSO. It lacks others however: privileged escalation, privileged task management and JIT authorization.

It remains strong on account discovery focusing on identifying privileged (and specifically, shared) accounts across 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 relatively 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 discovery capabilities, 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.

While still very much an entry level/SMB PAM platform, deployment has been simplified in the last 12 months and the base products can be integrated with more advanced elements from the Thycotic, CyberArk, Centrify and BeyondTrust suites. However, there is still no cloud or SaaS option of the Server product with only Password Hub hosted by a third-party cloud provider of the customer's choosing. This is a major oversight in 2021.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ○ ○ ○
Usability	● ● ○ ○ ○
Deployment	● ● ● ○ ○

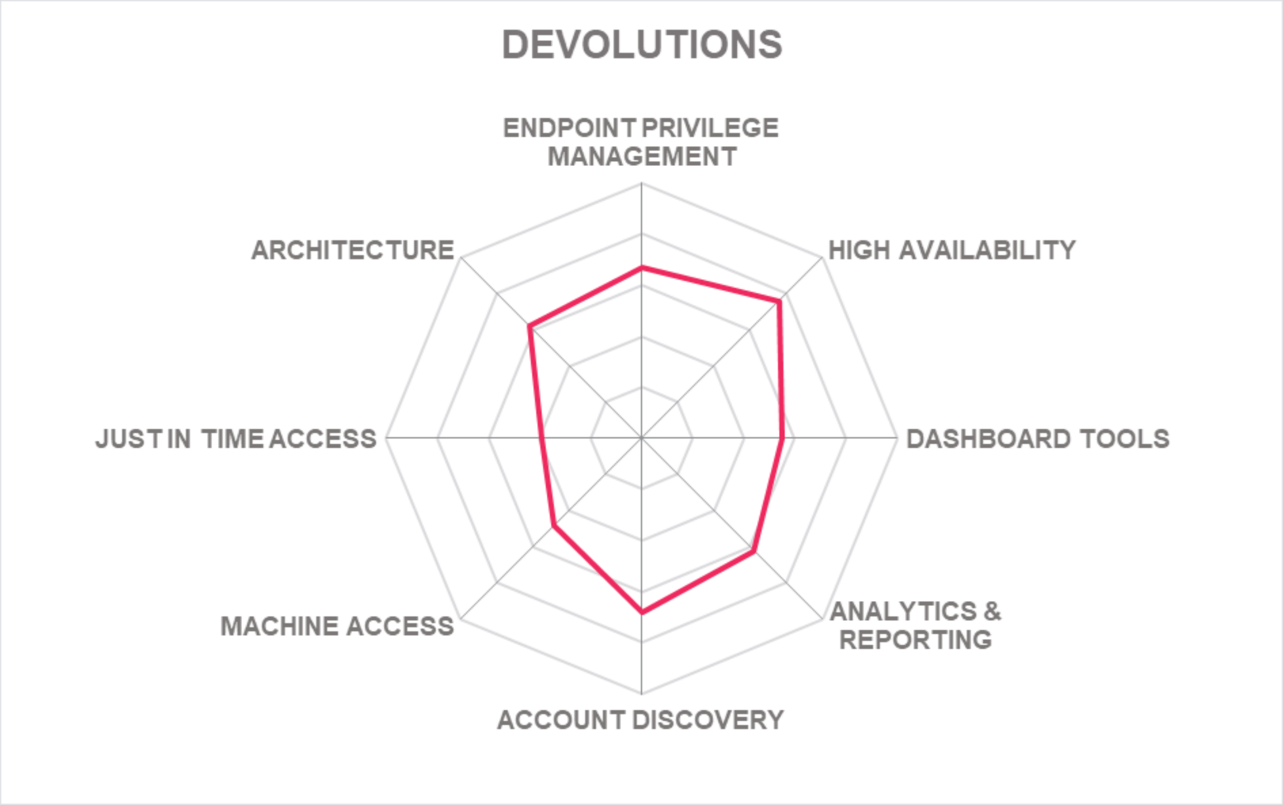
Devolutions

Strengths

- Good solid PAM solution for SMBs, that understands that sector's needs
- Ease of use and ease of delivery is a positive for SMBs
- 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 relies on third-party PAM products to scale
- On-premises only, no cloud version currently available for modules apart from Password Server
- Limited functionality may restrict market growth into larger enterprise sectors – but also for more complex SMB environments


DEVOLUTIONS
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.7 Ekran

New to the KuppingerCole PAM Leadership Compass this year is Ekran System. Founded in 2013 and based in Newport Beach, California it specializes in User and Identity Management solutions.

Ekran System also provides a PAM solution within a single endpoint agent. This includes privileged access and session management via a jump box, password management, request access workflow and two-factor authentication. It supports both cloud and on-premises deployments.

In terms of capabilities, Ekran has ticked many of those from our High-Level Checklist but there are some notable absentees: automated password check in/out, rule based privileged escalation, privileged task management and API authentication, for example.

For development and integration purposes there is some API support including application credential brokerage, ticketing system integration, and provision of monitored information via API; more API support would be welcome if Ekran System is to compete against the leaders in integration.

Session monitoring and recording is well taken care of. Video recordings are indexed with multilayer metadata including names of active applications, titles of active windows, websites (URLs) visited, keystrokes typed, commands and scripts executed, and devices connected. A single Ekran System Terminal Server Client can be installed on a jump server to monitor all sessions that come through it. The trigger rules for alerts can be set and modified by the customer.

There are some elements of Artificial Intelligence (AI) in play. The Ekran User and Entity Behaviour Analytics (UEBA) engine can detect a hacker with stolen credentials through self-learning techniques. The working hours of a genuine user are scanned, and a formal baseline created from which to compare anomalous or unusual behaviour. The company has plans to develop this with new behavioural factors for baselining. We look forward to more development in this exciting area.

The platform is now available on Microsoft Azure Marketplace and will support the Azure payment system. A solid, if yet unremarkable package in the crowded mid-market that can only benefit from further development in the coming years.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ○ ○
Deployment	● ● ● ○ ○

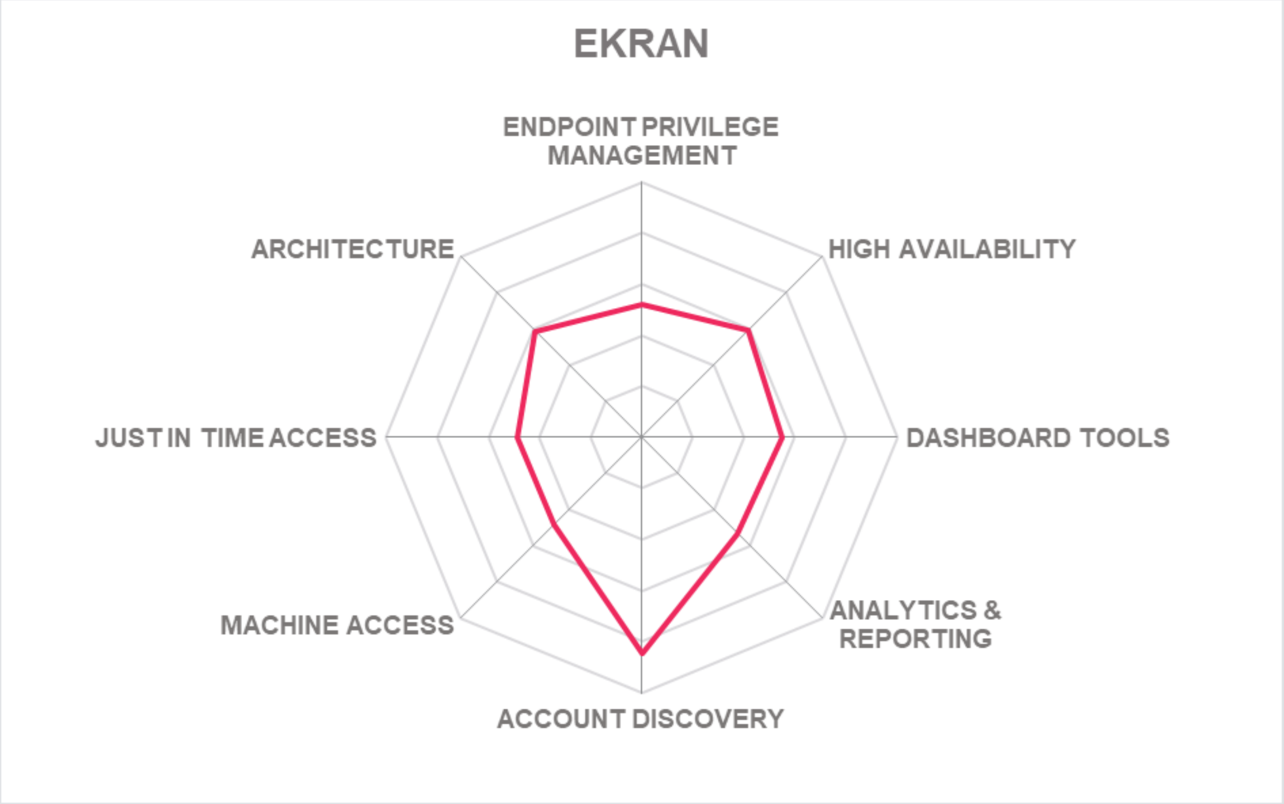
EKRAN

Strengths

- Effective use of AI to detect hackers and unauthorized users in UEBA capability
- API driven integrations are a good start and foundation for future scalability
- Solid session monitoring tools
- Available to run from AWS
- Ekran System’s experience in IAM should give confidence to potential PAM buyers

Challenges

- Lacks some of the key PAM capabilities such as task management and privilege escalation
- Some, but still limited DevOps capabilities that need development
- Needs more investment and innovation to compete with the best


EKRAN
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.8 EmpowerID

Based in Ohio (US), EmpowerID offers several products within its broader IAM portfolio, of which EmpowerID Privileged Access Management (PAM) is targeted at managing privileged shared access, session recording and auditing for common access protocols.

Largely built on top of Microsoft technology, EmpowerID offers integration and performance benefits for Microsoft-centric organizations, particularly for existing customers of its user provisioning and identity governance products.

The product is completely workflow based. A set of 1000 ready-made workflows ship with the product to get started, and more can be added through simple drag and drop creation. It uses conventional vault technology which hides passwords from users via RDP, SSH or web browser SSO. MFA support is through YubiKey Universal 2nd Factor Authentication, Duo Push, knowledge-based authentication (Q&A), and an OATH token server for issuing one-time password tokens.

EmpowerID has added an Eligibility Policy Engine which manages what users may see and request and which roles and resources in the enterprise can again access. Eligibility policies can be applied to users by query, role, group, or other criteria, to target who receives which policies.

A new microservice called My Tasks provides a consumer grade UX for request and to do item tracking. My Tasks was designed to work with EmpowerID's new Business Request approval flow engine which supports multi-level approvals.

As promised, EmpowerID has extended integrations through workflows, APIs and microservices. A SCIM (System for Cross-Domain Identity Management) Microservice connector model allows customers to develop new connectors without requiring knowledge of EmpowerID or SCIM. EmpowerID\'s IGA connectors can perform role-based escalation of existing user accounts or alternatively JIT provisioning of a privileged account. EmpowerID also supports SAML session-based JIT elevation

The interface remains a highlight, with an e-commerce like structure which enables end users to add access requests to a shopping cart icon. There is also a unique chat bot for help which is a nice touch. As a complete PAM solution, it lacks PUBA and native DevOps support. This is a surprise given its progressive architecture that allows for components to be containerized and orchestrated on Kubernetes.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

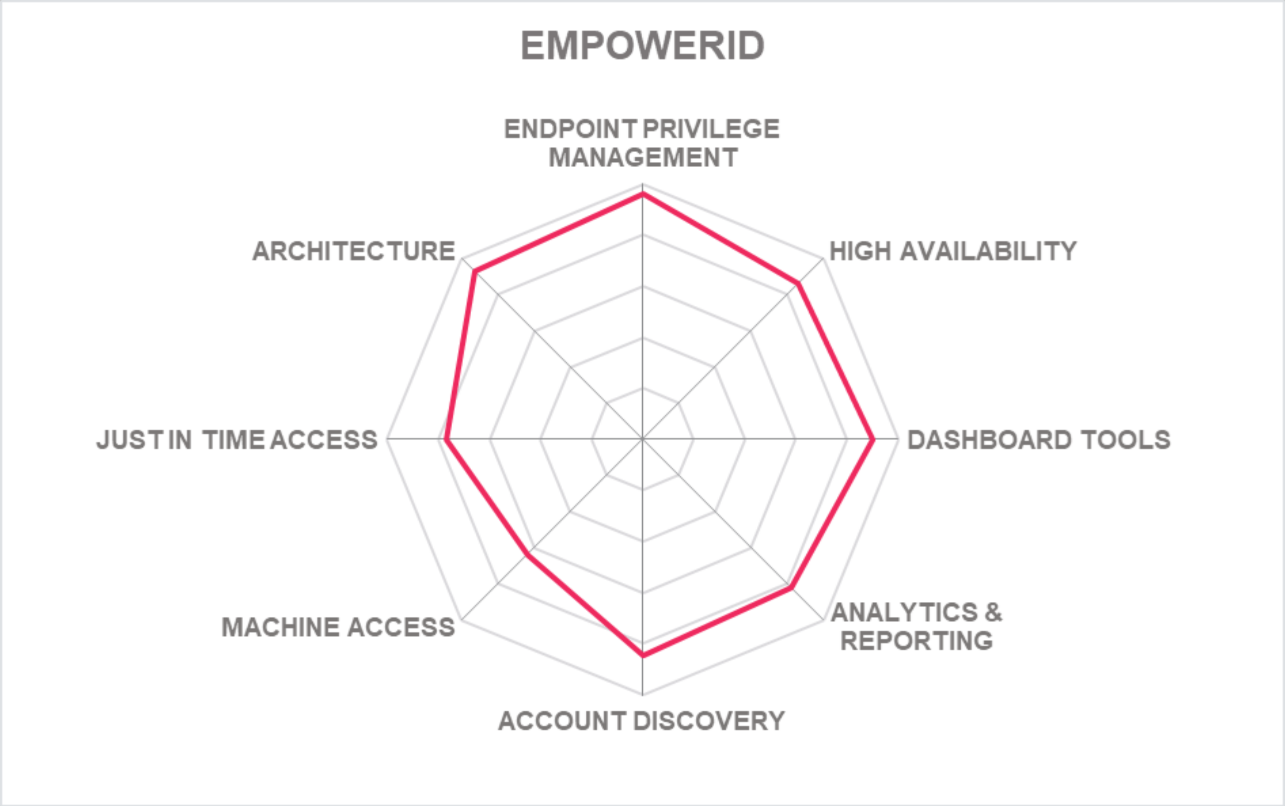
empowerID

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 YubiKey
- Admins can access session data from mobile devices
- Good reporting tools with real time alerts
- Strong API support and SCIM identity management
- Open architecture, scalability and interoperability

Challenges

- Needs to expand EPM and PRA support for the era of home working
- We would like to see PUBA and other advanced capabilities added to make this a more rounded option
- Limited DevOps support, behind leaders in native support which we hope will be addressed in the roadmap


EMPOWERID
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.9 Fudo Security

FUDO Security, with offices in California and Poland was founded in 2004. It offers FUDO PAM as its primary PAM product in the market. FUDO Security is used across the North America, Europe and Middle East markets.

Fudo PAM has a modern and crisp interface and allows customization with drag and drop resizable tiles available. The same customization can be used for data presentation, useful for reporting and behaviour pattern management.

For end users, the User Access Gateway portal provides easy access to servers -- the user is presented with a list of servers in one place, and a privileged session start can be initiated by pressing the "play" button - a thoughtful touch and one that adds greater efficiency to PAM in digital environments.

In the last year Fudo Security has evolved its PAM from session management with a password manager with other capabilities including JIT Access, Auto-Discovery with quarantine and graphical web session recording.

The session manager remains competent; it supports HTTPS recording of user's interaction with web services as well as RDP, VNC. The password and session recording tools of Fudo are up there with some of the best in class

There have been several incremental improvements since 2020. Logins are now automated for command line credentials and RDP plus support for credentials injection for One Time Password (OTP) and multi-page authentication in HTTP session. More fundamentally, the platform now supports HTML5 and an Auto Discovery Mode.

Fudo Security has used AI used to detect biometric anomalies such as unusual mouse or typing movements within the CLI or dashboard components. The use of Machine Learning has been enhanced further with new PUBA capabilities. Fudo\'s latest release enables existing systems to build users and system usage profiles based on continuous analysis of behaviour patterns and anomalies . Password Management offers password changes through pre-defined scripts and in-house plug-ins can be used to automate password management.

Fudo PAM supports SIEM including ArcSight and Splunk platforms. Its well thought out interface and AI tools that can detect unusual behavior will appeal to smaller organizations. We would like to see more development in terms of capabilities and native support for cloud and DevOps.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

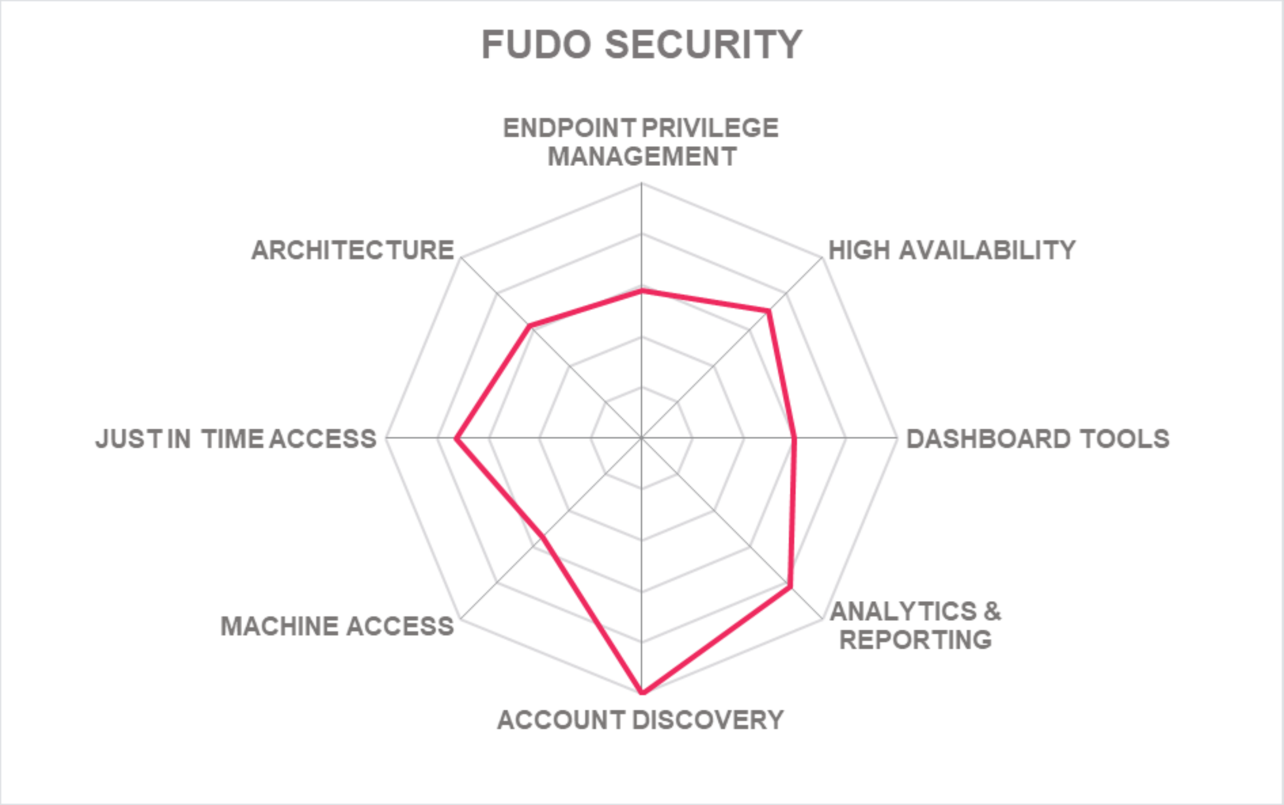
FUDO SECURITY

Strengths

- Crisp design, drag and drop customizable interface is refreshing
- Strong SRM and PSM functions with full data capture
- May appeal to many organizations looking for compact solution that does the basics well or as part of hybrid PAM environment
- Appliance and agent less based delivery offers much faster deployment and configuration than many PAM solutions
- Feels modern and should lend itself well to future development

Challenges

- Being built to support more capabilities so now needs bigger marketing push
- Current lack of support for cloud platforms and DevOps not yet addressed
- Opportunity to further integrations with IAM tools


FUDO SECURITY
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.10 Heimdal Security

Heimdal is a security vendor based in Copenhagen, Denmark. It sells various security software products including a stripped-down PAM tool which focuses on endpoint privileged session management and escalation. It has two cloud-based components, Heimdal Dashboard and Heimdal Agent both compatible with Azure.

But this is limited platform lacking a vault, session recording and monitoring, analytics and many other capabilities standard to other basic PAM packages in this Leadership Compass. This software really works best when integrated with Heimdal's other Application Control, Endpoint Protection and Vulnerability Management tools. Heimdal offers a bundle of its PAM tool with Application Control, to add application white/blacklisting on top of access management at the endpoint, which will have appeal to some buyers or department heads.

The password less approach to authentication is assisted by automation built into the admin dashboard. The Heimdal dashboard give admins the ability to block requests that come from compromised endpoints, or authorise for escalation at the endpoint, enable Passive Mode for system indexing; Auto-approval flow with rules defined and automatic de-escalation on threat. Admins can also define and apply a rule-based system and define individual rights within an AD group. The ability to revoke privilege escalation rights is based on DNS or AV detections of anomalous activity.

Some interesting capabilities have been added to the mix. A "PAM Compliance" view available from a tab gives some insight into user behaviour such as elevations (a kind of micro PUBA) and groups the user belongs to. There is also automatic blocking of revoked Admins and an API linking PAM directly to ServiceNow to process privileged service requests. To protect against Ransomware and other attacks, a Zero Trust module can block malicious file execution and users not in whitelisted groups are automatically blocked.

While this is specialist and limited PAM product, in the new era of remote and home working Heimdal may find willing customers, especially if it continues to add more PAM capabilities. All organizations, even those with existing PAM portfolios may benefit from a dedicated, easy to use cloud-based tool that simplifies controls and monitors Remote Privileged Access (RPA) requests for rapid elevated access.

Security	● ● ● ○ ○
Functionality	● ● ○ ○ ○
Interoperability	● ● ○ ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

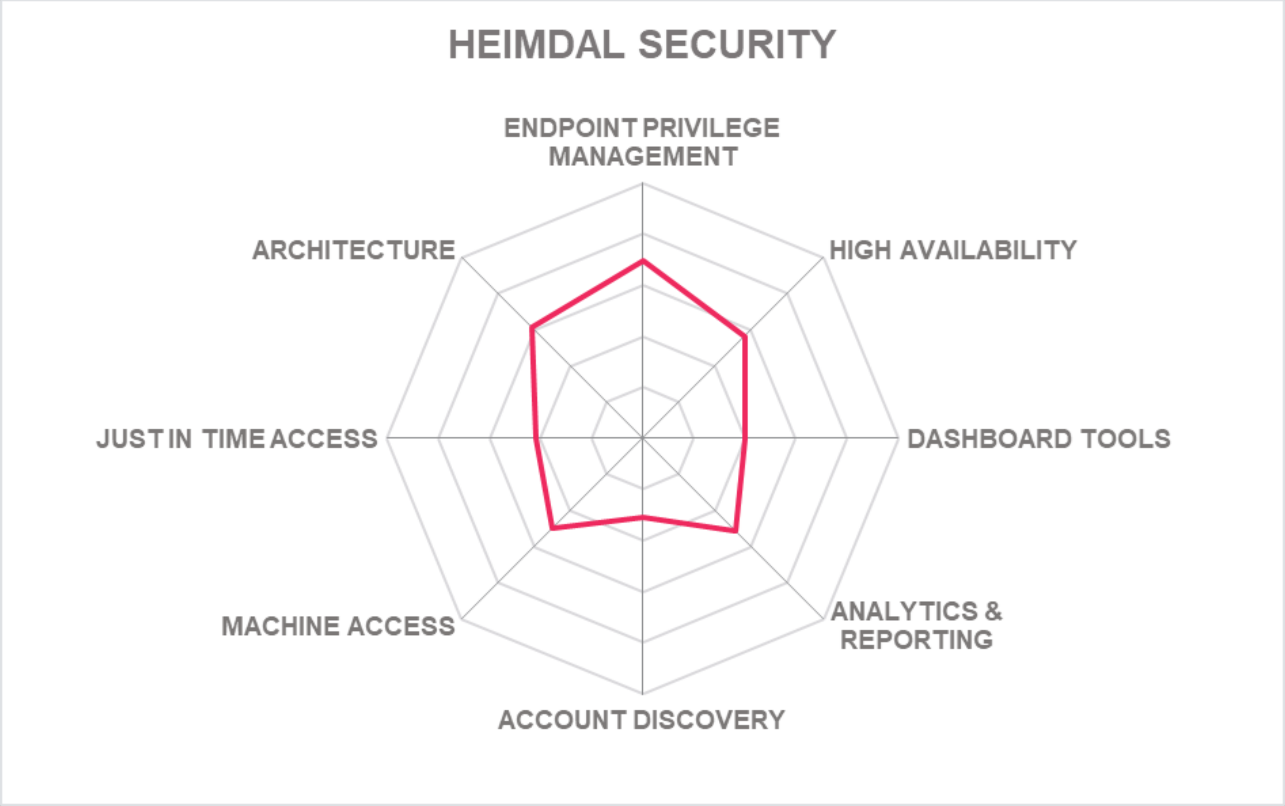
HEIMDAL SECURITY

Strengths

- Easy to use dashboard for admins making approval and blocking efficient at endpoints.
- Auto approval mode and automatic removal of privileges on threat detection
- Works best as a dedicated, easy to set up PRA tool for known users
- Fully compatible with Heimdal's other VM and Endpoint Protection products
- May appeal to smaller and mid-size organizations (or departments) looking for a simple to manage tool to control privilege access for remote workers

Challenges

- Limited as a traditional PAM tool that lacks many desired capabilities
- Agent based tool may cause some deployment issues in larger organizations, agentless would be preferable – lessen reliance on Agent
- Would prefer to see the Blacklisting/Whitelisting integrated fully with the RPA software as standard
- Great potential to develop into a full agentless/password-less/vault-less JIT PAM platform


HEIMDAL SECURITY
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.11 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. Following a restructure and rebranding, the company now offers Bravura Privilege for PAM. Hitachi is also taking more interest in its security subsidiary, and Bravura Privilege has replaced a PAM incumbent at sister data business Hitachi Vantara.

The product consists of three core modules: an identity manager, password manager and an access manager. It has 2FA and federated access built into the password manager. For 2021 Hitachi ID introduced Bravura Discover which despite its name, is not a simple account discovery tool. Instead, it is an enterprise PAM (and IAM) threat and risk assessment service designed to discover accounts, groups, entitlements, and associated metadata to discover hidden vulnerabilities.

While not essentially a part of key PAM functionality it nevertheless adds a new level of risk assessment that will play well into the subsequent controls of Bravura Privilege and policies for customers. For this, the development should be welcomed and represents some welcome ambition on the part of Hitachi ID. The company has also made some improvements to the UX and ease of use of the core PAM products, with workflows simplified and reduced steps to complete tasks. 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 for analysis.

Hitachi ID Bravura Privilege supports either direct connection to endpoints or via a proxy while users' access to the solution is via a direct UI, web proxy or via HTML5. Endpoints are connected behind the walled garden of Hitachi ID Bravura Privilege and mobile users can download and iOS or Android app and access via proxy service.

Session recording allows confidential information such as social security numbers to be redacted -- good for GDPR. There are 2 levels of authorization for viewing -- not all vendors consider the compliance aspects of session recording and monitoring like this. Single Sign On is supported and admins can check out multiple accounts in one request.

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 Bravura also offers multiple copies of the vault and option to store files in those vaults. After years in the doldrums, it feels like Hitachi ID is getting the support it needs to compete with what is fundamentally a good and secure PAM product.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

Hitachi ID

Strengths

- Strong contextual support for API/ service authentication
- Hitachi ID in the process of consolidating its suite with a focus on Identity
- 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
- Improvements to marketing and messaging still needed to compete better
- OOB connectors for cloud applications are limited but growing
- Limited partner ecosystem impacts market outreach and growth

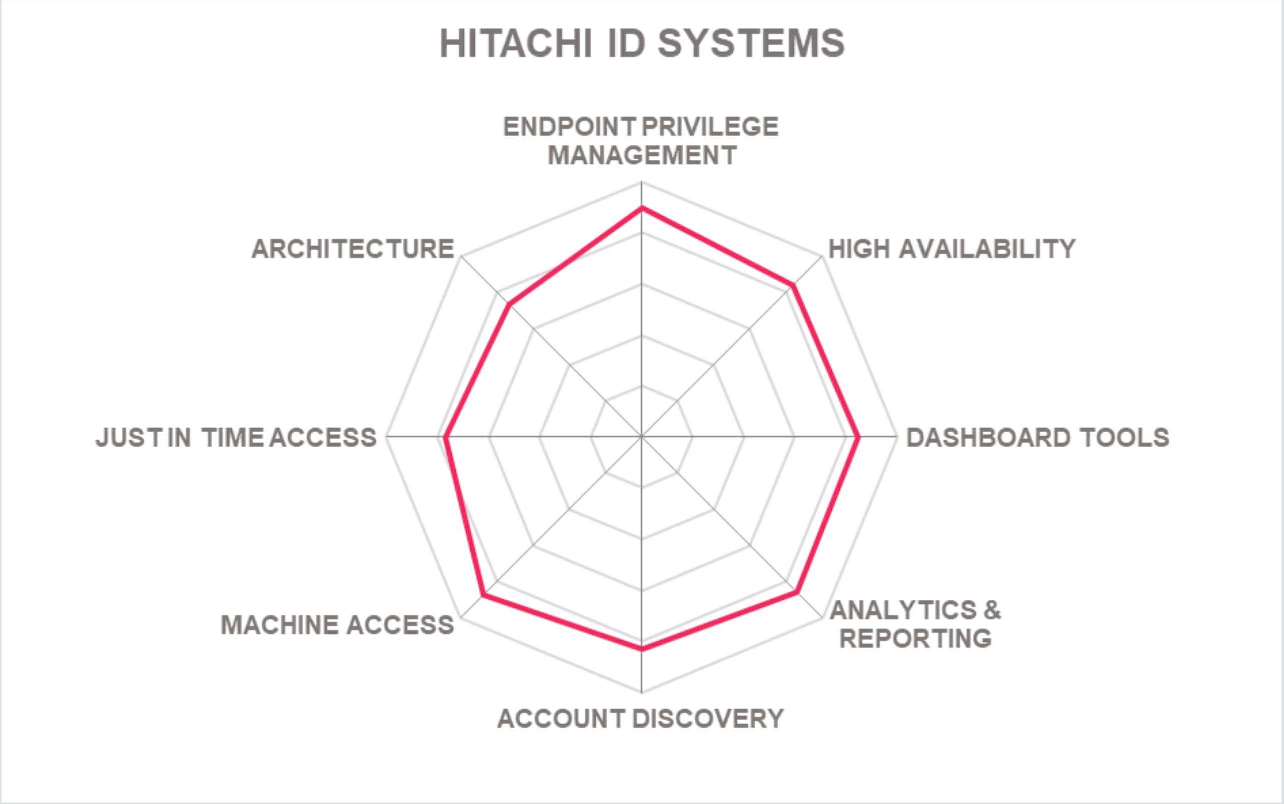
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


HITACHI ID SYSTEMS
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.12 Indeed Identity

Indeed Identity is a Lithuanian IAM vendor founded in 2011. It has now branched out into PAM, reflecting a recent trend in the industry of IAM and PAM technologies coming closer together. Currently the platform runs as software on-premises only with no cloud or SaaS options -- although this is on the company's two-year roadmap.

Despite current deployment limitations, the platform is well featured for basic PAM capabilities, including vaulting, session recording, and shared account management. Also on the plus side is a thoroughly modern interface and UX which older rivals in the market could learn from.

Capabilities that stand out are an SSO module that connects to any client application plus 2FA supported out of the box without any third-party applications needed. The base code of Indeed Identity's PAM server is lean and designed for easy integration into legacy and new architecture. The company also designed the platform to be configured on privileged and security policies such as approved SSH commands and the policies and rules around session recording.

A good basic package that ticks many of the boxes but has some notable omissions that would be essential for many buyers. These include Cloud support, EPM, PUBA, Privilege Elevation, JIT and DevOps support. It makes Indeed Identity's proposition in the market a difficult one to recommend. IT does basic PAM stuff well and is very well designed but without its omissions and shortcoming being addressed soon, it is difficult to see Indeed Identity becoming truly competitive in the PAM space.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ○ ○
Deployment	● ● ● ○ ○

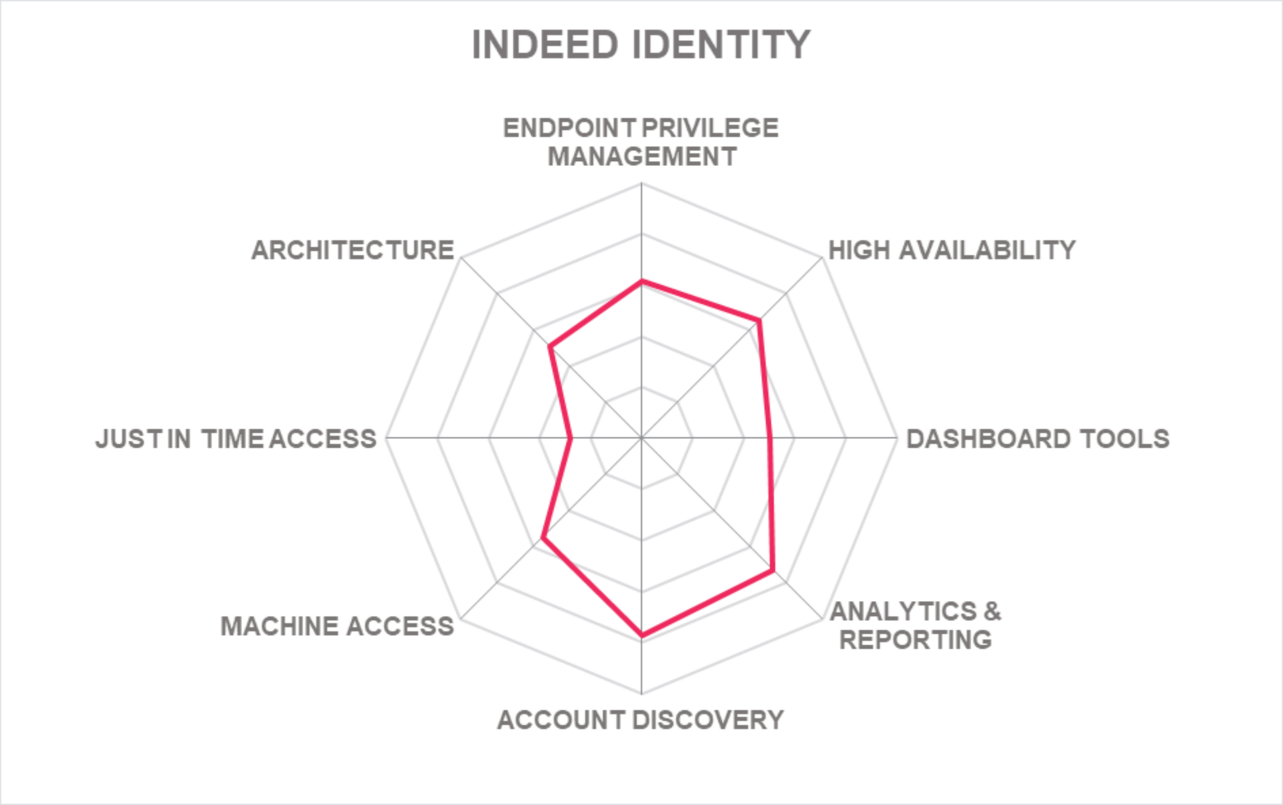
INDEED ID

Strengths

- Possesses just enough of the PAM basic capability to make it viable thanks to SSO and 2FA out of the box
- Bang up to date UX and dashboard design among the best
- Can be configured around existing security policies and for session recording
- Company has good knowledge of IAM technologies which will be useful for future development

Challenges

- Currently lacks far too many capabilities such as DevOps support, PUBA, JIT and others to be a credible enterprise or even larger SMB solution
- Would benefit from a SaaS version sooner rather than later
- Indeed Identity needs to decide on a product development strategy if it wants to meet the demands of more buyer personas.


INDEED IDENTITY
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.13 Krontech

Based in Turkey, Krontech is the technology arm of Kron, a telco firm publicly listed on the Istanbul stock exchange. Krontech offers its Ironsphere PAM suite that comprises several modules aimed at managing privileged access.

In addition to a rebranding, Krontech has made some notable improvements to its suite. It features a "bottom-up" strategy for secrets onboarding. This translates as a visual hierarchical tree structure to manage secrets and more flexible policies for password generation (length, numbers, letters, special characters, alpha numeric characters). There is now out of the box support for 60+ enterprise applications and systems.

The PUBA component has been enhanced with adaptive intelligence techniques, able to act according to risk scores and imminent security threats related to privileged accounts/access. Risk score calculations are made in 3 different dimensions: users, servers, sessions. Reports of all threat activity are also available for download. Ironsphere has also responded to our view that its interface was outdated and improved its web-based GUI, with new UX as well as new Desktop Client Application for Windows

Automation can be applied to recurring privileged tasks such as network port updates, DNS maintenance, router configuration, CMDB update automation (pre check, validation, and post check mechanism), as now supports integration with any ITSM system before running any task.

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.

There is support for CPEDM, PUBA and PADLM which should be expected at this level of PAM solution. Supported third parties applications include Duo and Okta and management of access to cloud applications is supported on AWS, Azure and Google. Unusually, Single Connect has a built-in MFA manager called the Unified Access Manager which also includes support for SSO.

With easy-to-use SAPM and PSM capabilities, Krontech Ironsphere may appeal to small and mid-size businesses (SMBs) with manual routine PAM tasks eliminated by useful privileged task automation, thereby accelerating leaner privileged operations. This undoubtedly is a package worth further investigation that has become further enhanced over the last 12 months.

Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

Krontech™

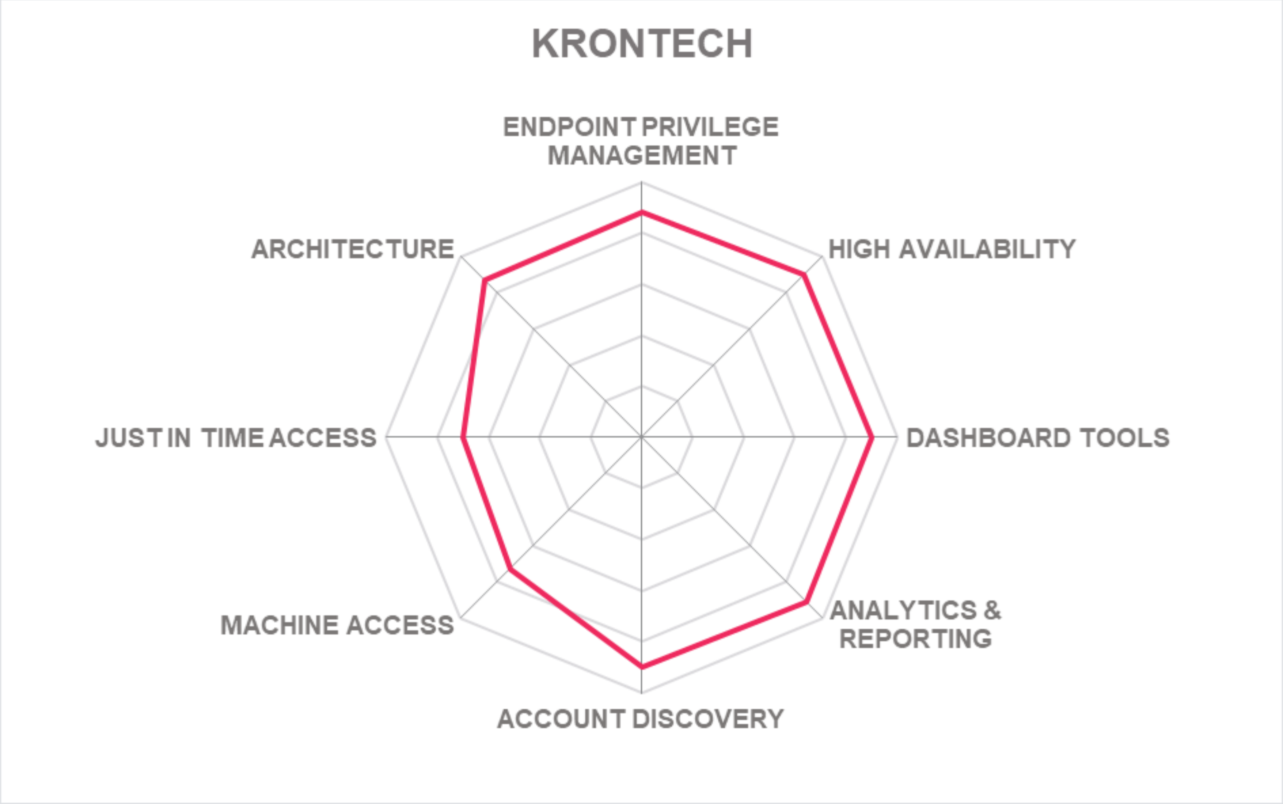
Protect What You Connect™

Strengths

- Separate modules for distinct PAM functions, integrated under a common PAM platform
- Has made constructive improvements to capabilities in the past year
- 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 most commonplace IaaS platforms

Challenges

- Still missing some advanced features such as native DevOps support
- It now has a more competitive product which should be marketed to attract more buyers outside core markets
- Corporate telco background tends to favour telco customers currently


KRONTECH
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.14 ManageEngine

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

The product promotes key management over more traditional password management but still supports traditional password rotation with a proprietary vault technology. Privileged Account discovery works across Windows, Linux, Network devices and databases. Session management masks passwords from users when launching RDP, VNC, SSH and SQL sessions. All sessions can be recorded and PAM360 comprises tools for PAG, PUBA, SSL and SSH key management and workflow automation.

Admins are well catered for in the User Management Area which has been improved with enhanced support for MFA and the ability to add custom roles -- essential for adding contractors or other third parties. Onboarding of users can be done directly from LDAP or AD and is assisted by the easy-to-understand UX, and password control and configuration is highly efficient.

PAM 360 benefits from machine learning capabilities in 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. We would have liked to have seen more capability development: native DevOps, cloud and PAMaaS are still missing but this remains one of the best platforms outside the Leaders.

ManageEngine

Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

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
- A lack of significant product development since 2020 is a surprise
- Lack of integration with IGA tools
- Lack of connector support for cloud applications and cloud-based delivery

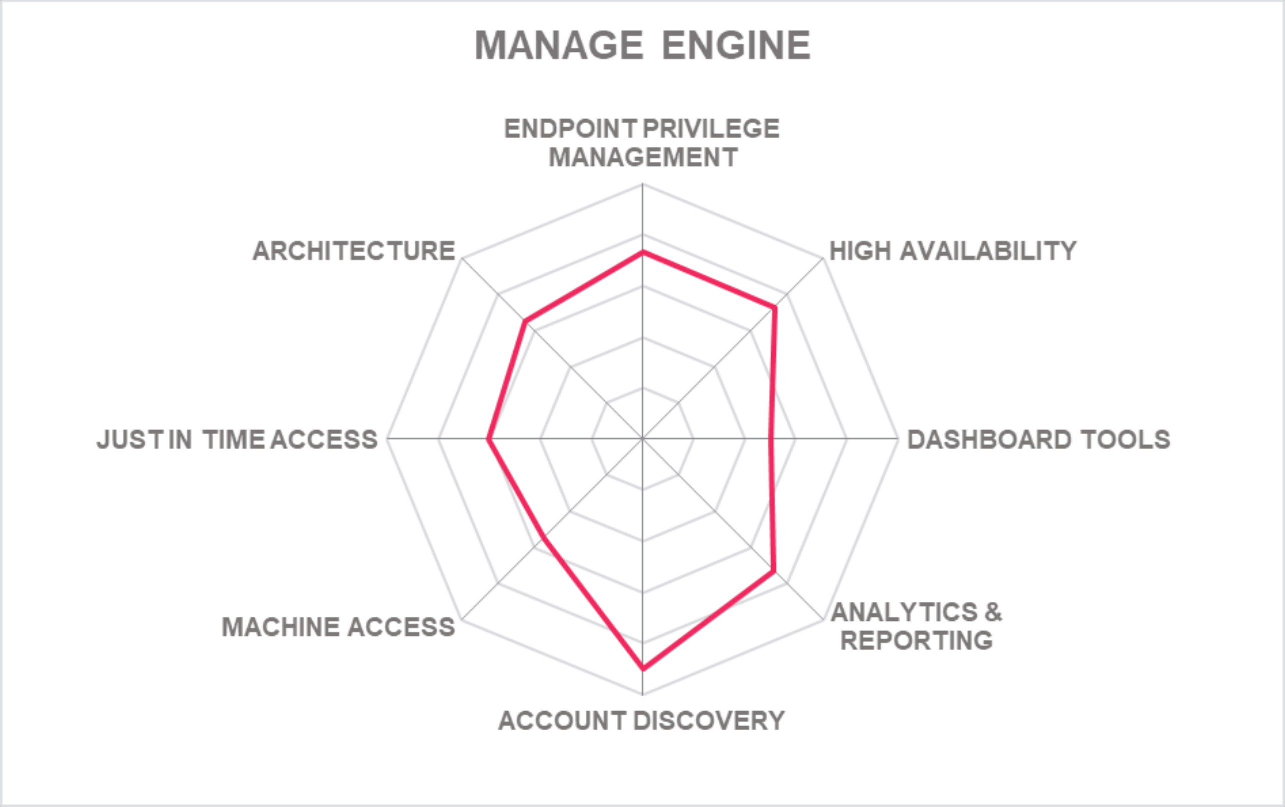
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


MANAGE ENGINE
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.15 Micro Focus

UK based software vendor Micro Focus, founded in 1976, has many solutions for organizations looking to transform operations and infrastructures. It markets its PAM platform under the NetIQ brand, a former acquisition, and now part of the company's CyberRes security portfolio. Micro Focus has made effort to add functionality to its platform where it matters utilizing technical strengths and user experiences from other Micro Focus properties. A good example is the integration of Net IQ Privileged Account Manager with Micro Focus Interset, its proprietary UEBA solution. A good move and one that will help facilitate further integration with NetIQ IAM and IGA products -- as is the plan, along with a full SaaS option.

Micro Focus Interset can calculate risk scores based on user behaviour anomalies, such as unusual applications accessed, time of day, geographical location, device used and other metrics. NetIQ Privileged Account Manager then uses this information in its decision-making process to provide a privileged session based on the user\'s risk score.

Elsewhere, new agentless capabilities for both Windows and Linux deployments should speed time-to-value requiring fewer components to be installed (and be vulnerable). The platform now provides real-time session streaming, for improved monitoring and control of privileged sessions. This allows a secondary user to audit a privileged session in real-time and make decisions based on detected risky behaviour and terminate the session if desired. Improvements have also been made to user interfaces across the platform and a new console allows quick toggling between multiple privileged sessions.

Support for DevOps processes remains limited, but Ansible scripts are now available for developer processes for PAM component deployment, upgrades, and other common use cases in those specialised environments.

NetIQ Privileged Account Manager is now much more of a contender in the Leadership stakes. The solid PAM tools at its core: discovery, vault, session management and recording, AAPM, EPM and SIEM are now boosted by solid improvements to Monitoring, Analytics and Risk Management. It also offers 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. Looks like Micro Focus is getting back on track with its PAM play.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

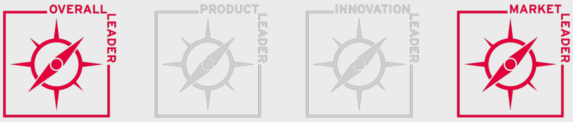
Strengths

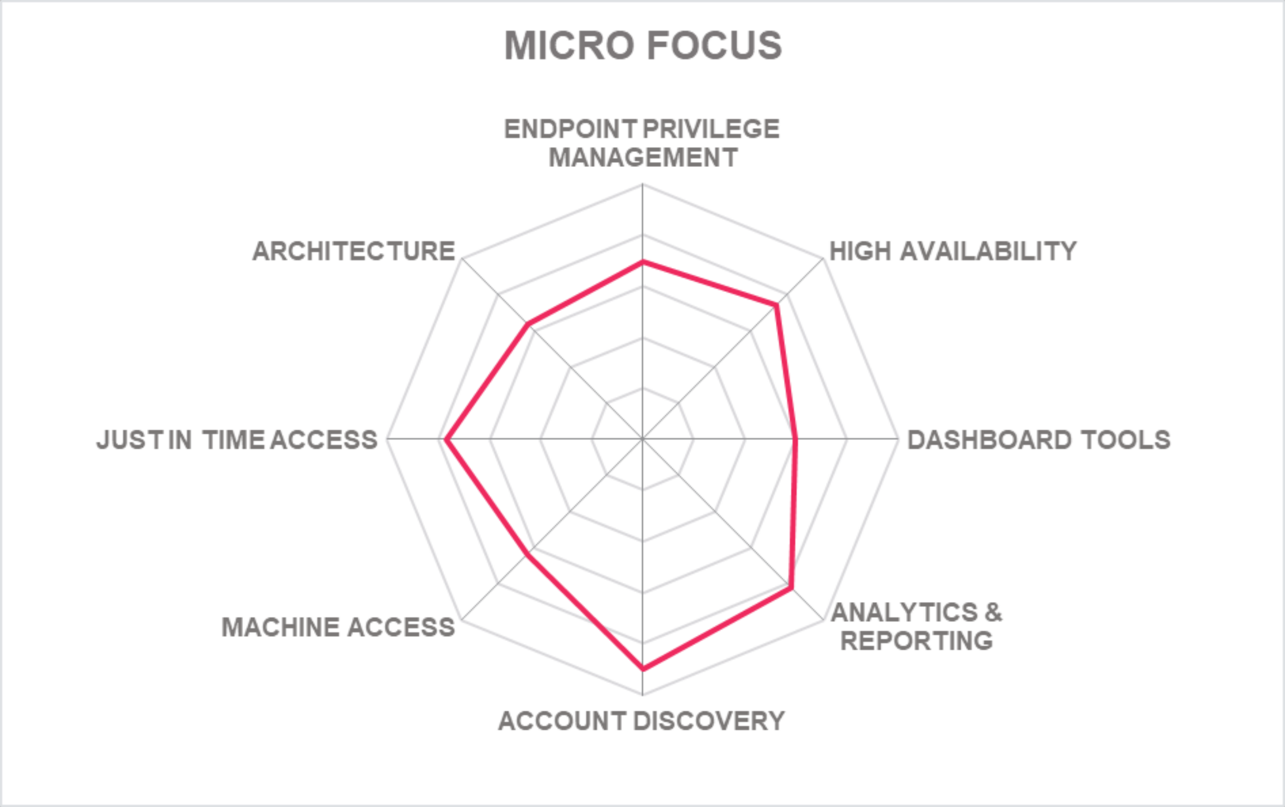
- Good for organizations that already adopt other NetIQ IAM products especially with new family integrations
- Real-time session recoding now standard
- Support for SAP and other major database platforms
- Reliable and trusted solution for its basic capabilities
- Retains a good interface with user friendliness to the fore
- Financially backed by a large enterprise software vendor

Challenges

- The product would now benefit from more comprehensive DevOps and other digital capabilities as the next positive step
- Micro Focus website remains confusing to buyers and dual branding is confusing
- The platform is now being given technical and marketing attention, but now the next level push is required

Leader in




MICRO FOCUS
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.16 One Identity

California-based One Identity, a Quest Software business, specializes in IAM solutions and offers a range of products that fulfill the fundamentals of PAM. 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. 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 protected by two-factor authentication.

Safeguard for Privileged Sessions can record all privileged sessions and content is indexed to simplify searching for events and reporting. Safeguard for Privilege Analytics tracks user activity in real time and compares activity to session data collected from the wider IT environment. New additions include a SaaS solution, SafeGuard On Demand and a Remote Privileged Access tool, SafeGuard Remote Access, that flesh out the portfolio.

In a more specialized and welcome move, the Safeguard DevOps Service tool has been added which is a fully containerized service that brings a native level of connectivity from the Safeguard Vault to DevOps tools and environments. There is also Starling Connect for Passwords that allows customers to quickly subscribe to credential connectors for password rotation and discovery of cloud targets.

One Identity has improved its JIT provisioning for Safeguard which now allows privileges to be assigned at the exact time of credential check-out. Accounts in Active Directory that require privileges to perform a function can be added to the appropriate group(s) when the account is approved for check out, then removed.

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 also offers CPEDM and AD Bridge products as installable client packages. Safeguard for UNIX/Linux is a comprehensive suite delivering Unix-AD bridging, authentication, root delegation (SUDO enhancement) and centralized management of policies across Unix-based systems.

Privilege Manager for Windows offers CPEDM capabilities for Windows-based platforms. 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, Yubikey, Okta, Duo and RADIUS. Finally, Safeguard now supports Sudo 1.9 which brings new security safeguards against user error, and furthers JIT capability.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○

ONE IDENTITY™

Strengths

- Much improved capability for DevOps environments with native Kubernetes support
- Fully featured PAM platform that now addresses the SaaS market in latest release
- Easy to understand interface shared across all modules with support for both CLI and GUI
- Good reputation for enabling smooth deployment, integration and scale for many organizations
- Simple integration with One Identity IAM products will appeal to organizations already invested in the ecosystem

Challenges

- Some products are complementary tools from parent Quest Software
- Despite addition of new capabilities there is a feeling of filling the gaps rather than fully innovating to challenge the top players

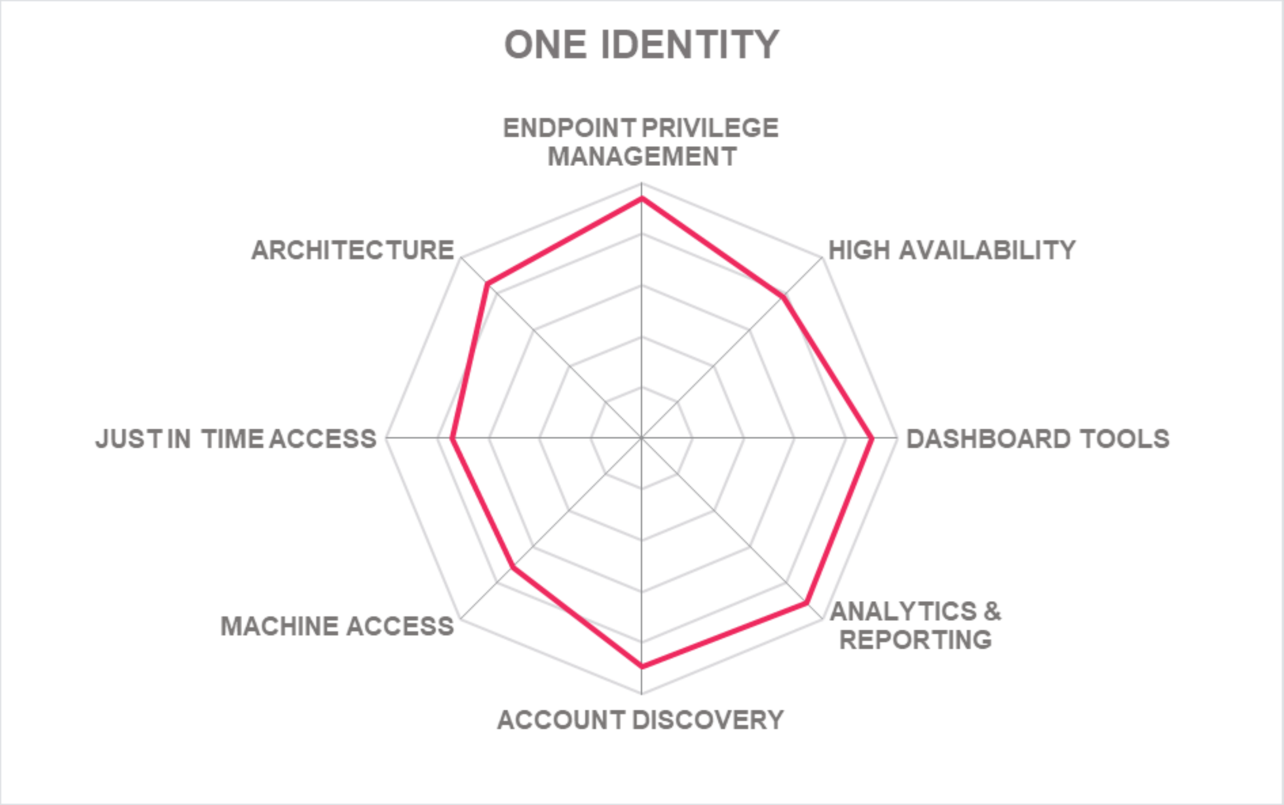
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


ONE IDENTITY
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.17 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 PAM platform. Remediant has created a PAM solution that provides JIT access for ALL privileged accounts, abolishes shared accounts and stores no credentials at all -- a bold approach and one that has benefitted from tandem development of interoperability and functionality.

SecureONE now integrates with security platforms from Axonious (Cyber Asset Management), Carbon Black (EDR), CrowdStrike (EDR) and broader SIEM support. In terms of functionality the EDR integration permits session recording, associating relevant data with privileged access sessions. Basic IGA capability is now available with deeper IGA integration, specific to SailPoint, trialled in several customer environments.

OAM (Offline Access Management) now provides break-glass and scheduled on-demand rotation of local account credentials in case JIT access is not working due to the target system being offline. Remediant has also expanded its API endpoint integration count by 22% to further assist customer driven integrations.

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 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.

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 lightweight directory bridging for Linux systems. As for High Availability SecureONE supports HA, DR and HA+DR configurations. It can support HA configurations with up to 4 node fault tolerance. SecureONE also supports integration with several SIEM systems.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○

Remediant

Strengths

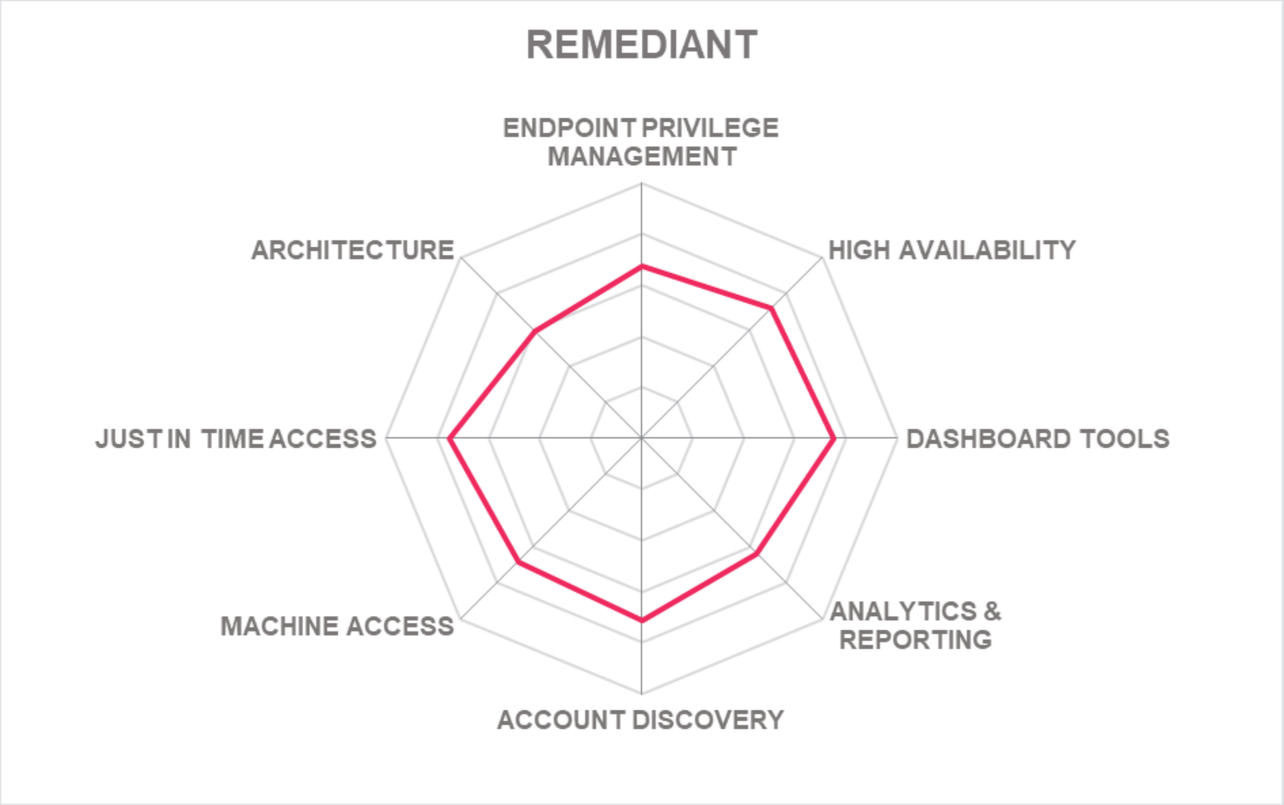
- Theory of agent less and vault less operation makes sense and will appeal to some organizations
- Simple to install with modern interface
- Basic solution that does a good job of access control and management
- Role-based access control
- Potentially the basis of a future leading PAM solution

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

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


REMEDIANT
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.18 Saviynt

Saviynt is a US based company founded in 2010 that specializes in IGA and Identity solutions. It fairly recently entered the PAM market with a new as-a-service cloud solution, a Vendor to Watch in 2020. Saviynt does not provide a vault allowing customers to choose their own. The solution is designed to run on all major cloud platforms including Google, AWS and Azure. It is also fully compatible with Workday and Office 365 integrations.

Saviynt's solution comes with built-in Cloud Entitlements Manager (CIEM) features, which is good. In addition, as part of its converged Enterprise Identity Cloud (EIC) platform, Saviynt's cloud PAM comes with built-in IGA features. New stuff for 2021 includes continuous discovery of cloud workloads and entitlements and monitoring of services and workloads for security errors or misconfigurations. A new Risk Exchange tool allows bi-directional data integration with 3rd party solutions such as SIEM and vulnerability management solutions. There is now also Automated Backdoor Entry Protection, able to identify backdoor accounts and automatically disable, delete, based on policies - and alert and mitigate.

Within the product itself are a discovery tool, session recording and session management as well as more advanced features such as Risk Analytics, credential vaulting and a risk and controls library. The guiding principles behind the platform are based on reducing numbers of static privilege accounts in an organization and avoid storing unused credentials in a vault.

The web-based interface is designed to be user -centric and in this the company has succeeded in creating a very clean and simple interface. It is a bold move to create a PAM solution that runs only as a service. While it gives the developers control over iterative development, it also hands them greater responsibility for the integrity of privileged access management for their clients. Overall, this represents a promising addition to the ranks of PAM solutions, taking PAMaaS further but still in need of extra capabilities.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

SAVIYNT

Strengths

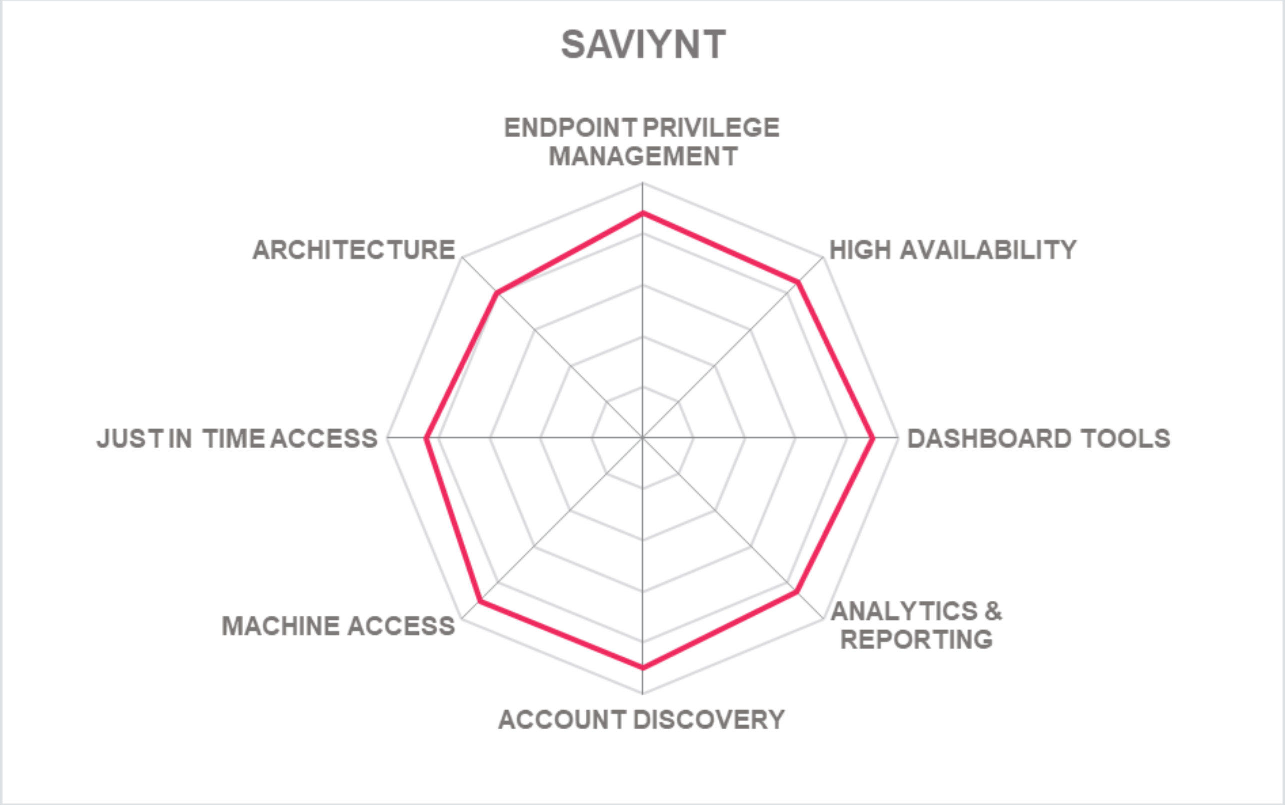
- Integration of functions designed in from the start, takes PAMaaS to a whole new level and is ready for the IaC future
- Saviynt has clearly thought about how cloud apps affect PAM and worked to accommodate that
- A good step towards reducing reliance on passwords
- Good control of redundant IDs and unused passwords
- Unique HR integration capabilities

Challenges

- Saviynt may wish to explore a password less platform in the future
- This is a solid and innovative platform that now needs the effective marketing it deserves to achieve a wider audience
- Next step would be to integrate native DevOps tools and improve Machine Identity capability

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


SAVIYNT
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.19 Sectona

Founded in 2017, Mumbai (India) based Sectona is one of the newest PAM market entrants and offers four modules that cover fundamental PAM, Endpoint Privilege Management (EPM), Privileged Access Governance (PAG) plus DevOps Secrets Management.

Having consolidated its technology into a modular platform it has also enhanced capabilities in the last 12 months. Sectona has improved its JIT capability with Zero Standing Privilege (ZSP) now supported, Privileged Task Management (PTM) now automates SSH and PowerShell commands to automate routine tasks while Privileged Account Lifecycle management is now fully accessible from the Management Console.

Sectona's Common Session Management Framework can leverage sessions across browsers, local machines and jump servers. User access is governed by a unified policy framework & common connector element.

Sectona describes its platform 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.

Sectona 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.

A highlight of the platform is 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 its software aimed at IT service providers wishing to offer managed PAMaaS, which is fairly unique in the market, at present.

It is 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 (AAPM) by using APIs and SSKs for many platforms. It is well positioned then to manage DevOps and containerization demands in the future. Some good development in a platform already built on solid foundations.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

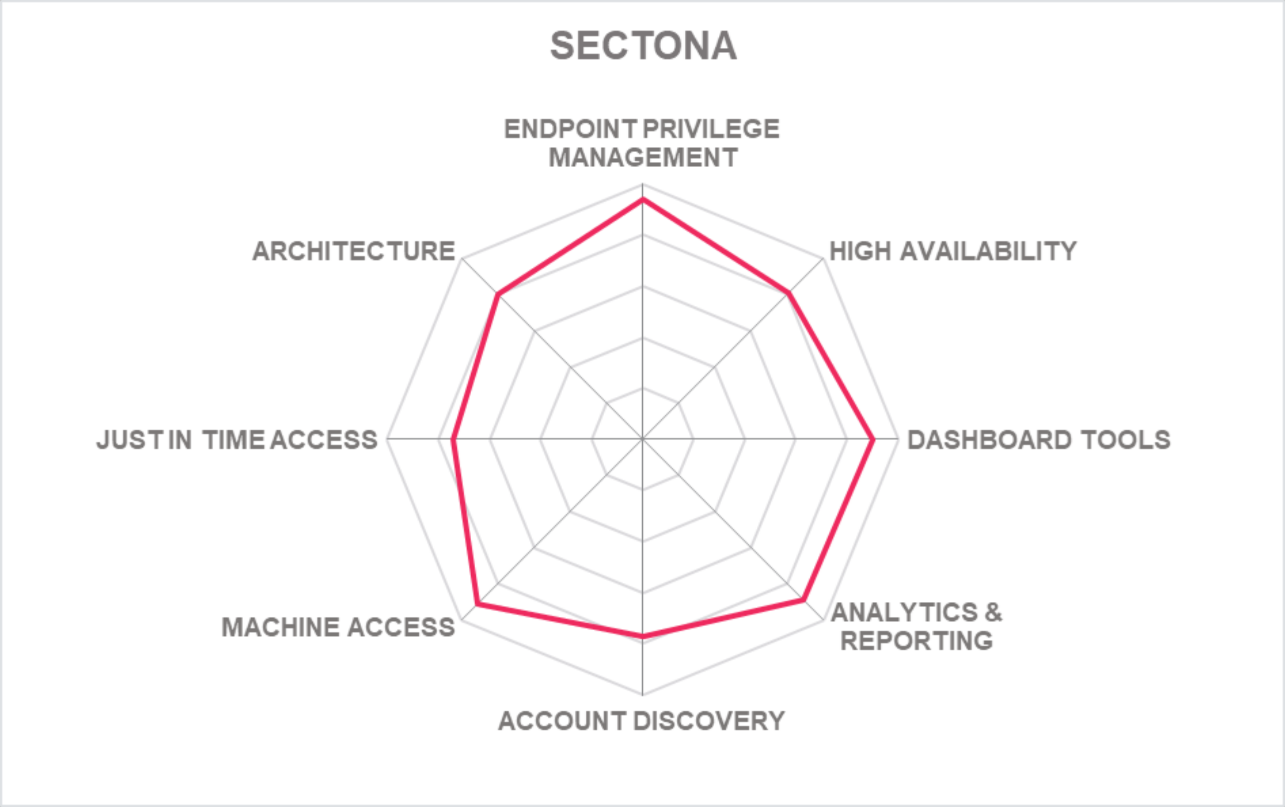
Sectona

Strengths

- Easy to understand and use dashboard
- Managed services option (MSP) will appeal to third parties
- 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 and may suffer in enterprise market, although Sectona has increased in-house resources
- Built in functionality still largely basic and lacks CPEDM for example


SECTONA
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.20 Senhasegura

Based in São Paulo, Brazil, MT4 Tecnologia produces Senhasegura as its flagship PAM product. Comprised of multiple modules, Senhasegura offers comprehensive PAM capabilities. Senhasegura PAM is built over 15 tightly integrated functional components and is available in virtual or hardware appliance delivery formats.

Senhasegura already had a broad level of capability and its ambition to break into wider markets has resulted in solid development of its feature sets. The company has improved its use of biometrics -- already used for MFA, with supporting algorithms designed to identify human keystroke patterns and alert to activity by unauthorised users on endpoints. Related to this is a new module that collates user behaviour data to determine a risk score for all Privileged Users.

The User Security Posture Rating is used to calculate the probability of malicious actions given the history of the user\'s previous behaviour. With each new privileged event executed by the user, the score is updated and dynamically influences password controls for the user.

Developers will appreciate the new support in Task Manager Pro for Red Hat Ansible playbooks to create new privileged tasks. With Ansible it is easier to create complex privileged routines and the tool integrates vendor modules already in its repository.

A new SaaS-based tool delivers Remote Privileged Access (RPA) that is agent-less and VPN-less, using the client cloud as the connection point to the network. The authentication is made via an MFA biometric validation on Senhasegura\'s Mobile App.

MT4 Networks now has a more powerful PAM proposition, with enhanced usability and forward thinking on the needs of developers and how PAM fits into Infrastructure as Code (IaC) environments. 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 built -in infrastructure modules offer high availability, load balancing and advanced monitoring capabilities. Senhasegura should be credited with listening to KuppingerCole's analysts and embarking on a period of enhancement and improvement right across the board.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

senhasegura®

Strengths

- Ease of deployment
- Easy to use, clean interface
- Can be customized by admins and end users
- Good efforts made to address previous 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

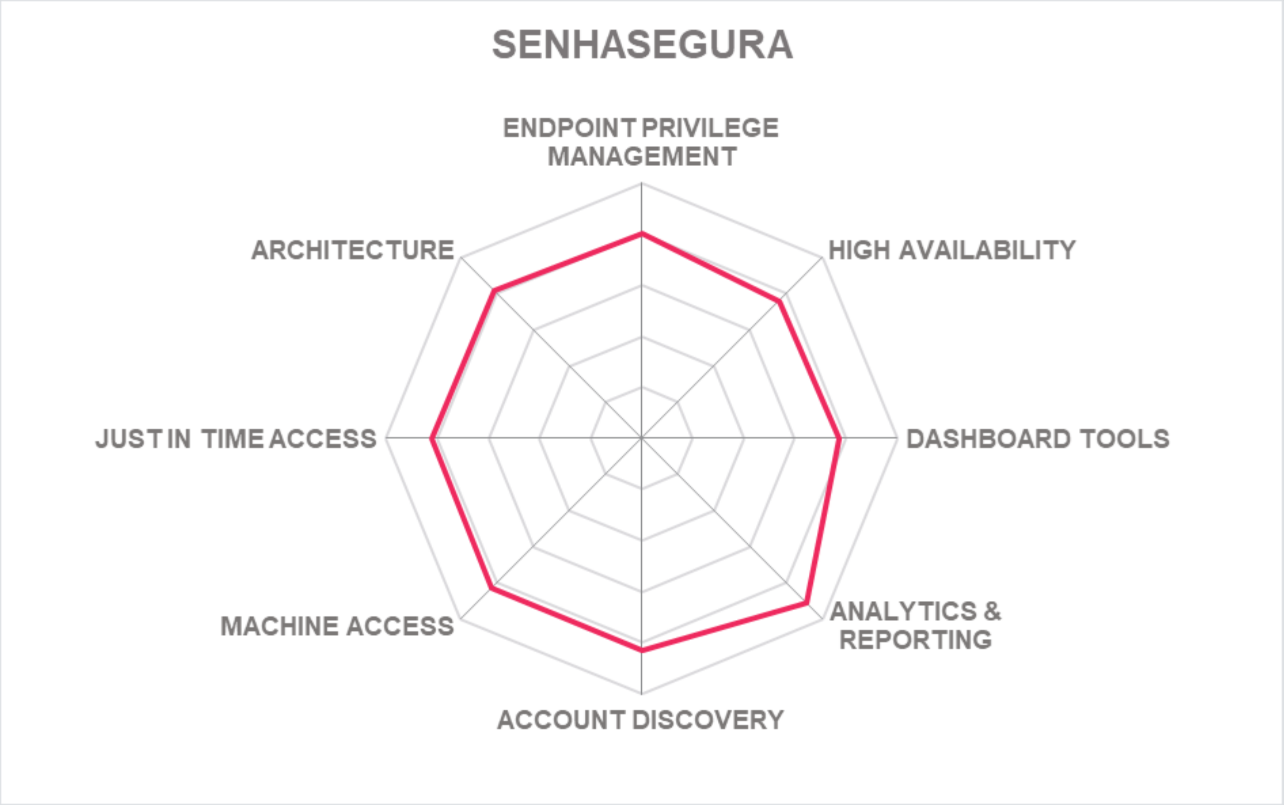
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


SENHASEGURA
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.21 SSH Communications Security

Based in Helsinki, Finland, SSH.COM offers PrivX as its primary product for the PAM market. PrivX offers an alternative to traditional account & password management methodologies. PrivX provides ephemeral (short-lived) certificate based Just-In-Time (JIT) access for SSH and RDP protocol authentication. This approach can reduce the overhead management that typically comes with password vaulting solutions. PrivX does however come equipped with two vaults (user exposed & PrivX admin only access) providing the best of both worlds. In addition to the already existing key vault for admins, the new PrivX Secrets Vault allows for secrets to be stored and retrieved by users from the UI or automated processes.

Newly added functionality for X.509 certificate support further expands the range of targets accessible via certificate-based authentication, including Tectia SSH servers and devices from but not limited to vendors such as Cisco.

It is an innovative approach but one that brings functional and security advantages -- access is faster, onboarding/offboarding of privileged users is quick and for most use cases there are no passwords to expose. Furthermore, credentials or secrets are masked from users when accessing targets using certificate-based authentication or vaulted passwords that are injected into target sessions.

Users can view a list of resources based on role memberships and select targets accordingly. User & Group information is automatically synchronized through seamless IGA/IDM integration capabilities. PrivX currently supports AD, Azure AD, LDAP/s, AWS Cognito, in addition directories from IAM systems using OIDC and SCIM claims are also supported.

While the core product is deliberately lean, it integrates with third parties to add functionality for SIEM, ticketing systems and HSM through APIs. In addition to the UI, Native Clients are supported for SSH and RDP with little to no loss in functionality over the main UI use. All SSH, RDP,HTTPs and VNC sessions are audited, logged and can be recorded for compliance, forensics or training purposes.

PrivX offers accountability of user activities even when shared target accounts are in use, 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.

However, PrivX reduces the need for traditional endpoint security by isolating the user's local machine from the target. When connecting via its UI, target connections take place within a containerized (HTML5) browser session meaning zero exposure to user local machines. This method of access also enables RPA (remote privilege access) without the need to manage external user/3rd party workstations which is ever more prevalent with today's distributed working practices.

The product remains an attractive alternative for many organizations seeking to reduce password management and leverage cloud native capabilities.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

SSH.COM

Strengths

- For a lean product, it still supports many core PAM capabilities and has been recently enhanced
- Rapid access makes 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

Challenges

- Lacking endpoint privilege management keeps the solution lean but may be missed by some
- Agentless approach may deter some buyers
- Would really benefit from an SSH delivered SaaS based version

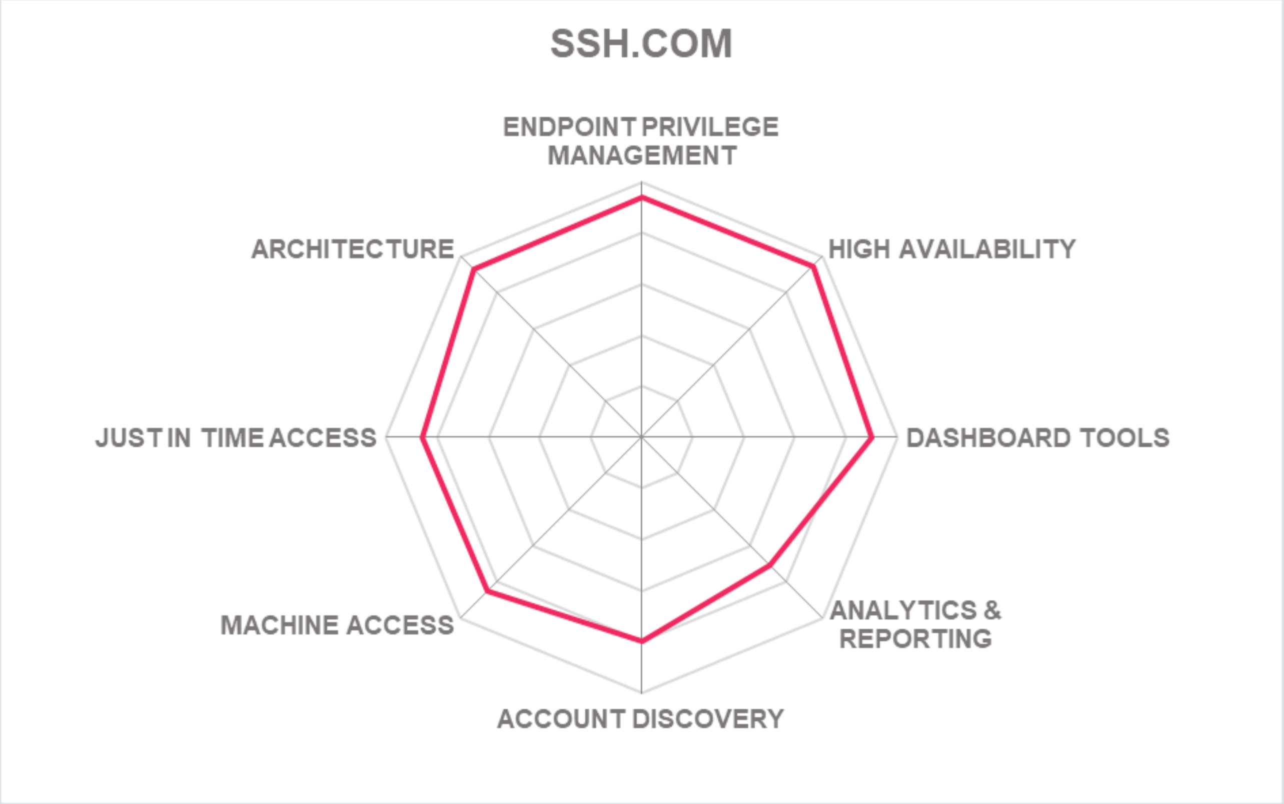
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


SSH.COM
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.22 STEALTHbits Technologies

Founded 2002, 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. Since January 2021, Stealthbits has been part of Data Security vendor Netwrix.

There are four basic functions in the product: access control, session recording, auditing and vaulting. This provides scheduled and on-demand credential rotation capability for all AD, Windows, Linux, Cisco and Azure AD). The design is to simplify PAM as much as possible by providing a fully JIT ephemeral approach to access and provisioning with as little as possible installed in the customer environment. 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 and other 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 via API from several leading PAM providers although 99% of customers choose Microsoft LAPS. Stealthbits built-in vault protects service accounts used for privilege escalation and can manage the passwords for existing 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 run hybrid, on-premises, or in the cloud. Built-in task-based certifications are supported.

On usability, a "My Activities" page displays user activities as cards and a Product Tour feature to help onboard users as they log onto the system for the first time and the navigation menu has been improved. The Service Account management has real-time feedback and 'roll-back' button to undo changes and the Session Lock can send unique messages to a locked user with custom 'what happens after' options.

Fundamentally the product has remained the same but Stealthbits has added a number of capability enhancements that make it more competitive. There are some technical enhancements of note: Security OpenID Connect and SAML2.0 authentication, scheduled password rotation for all supported platforms and a browser extension for Chrome and Edge for improved web session recording. There is also a claimed 10-minute deployment option; as ever such claims need verification in the real world but the simplicity of SbPAM suggests that rapid time to value is achievable. We are promised SSH key management and credential based policies for AAPM in the near future.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

stealthbits

Strengths

- Potentially the future of PAM in terms of ease of use and ephemeral control now with added capabilities
- Highly suitable for DevOps and code driven environments
- Easy to use and administer, potentially highly rapid deployment times for some organizations
- Ephemeral approach means a reduced attack surface
- Would work well with smaller, agile and less legacy incumbered organizations

Challenges

- Larger enterprise organizations may need the back up of existing PAM
- Potential to add capabilities that add data governance to the mix
- Stealthbits need to do more to effectively market this approach to PAM

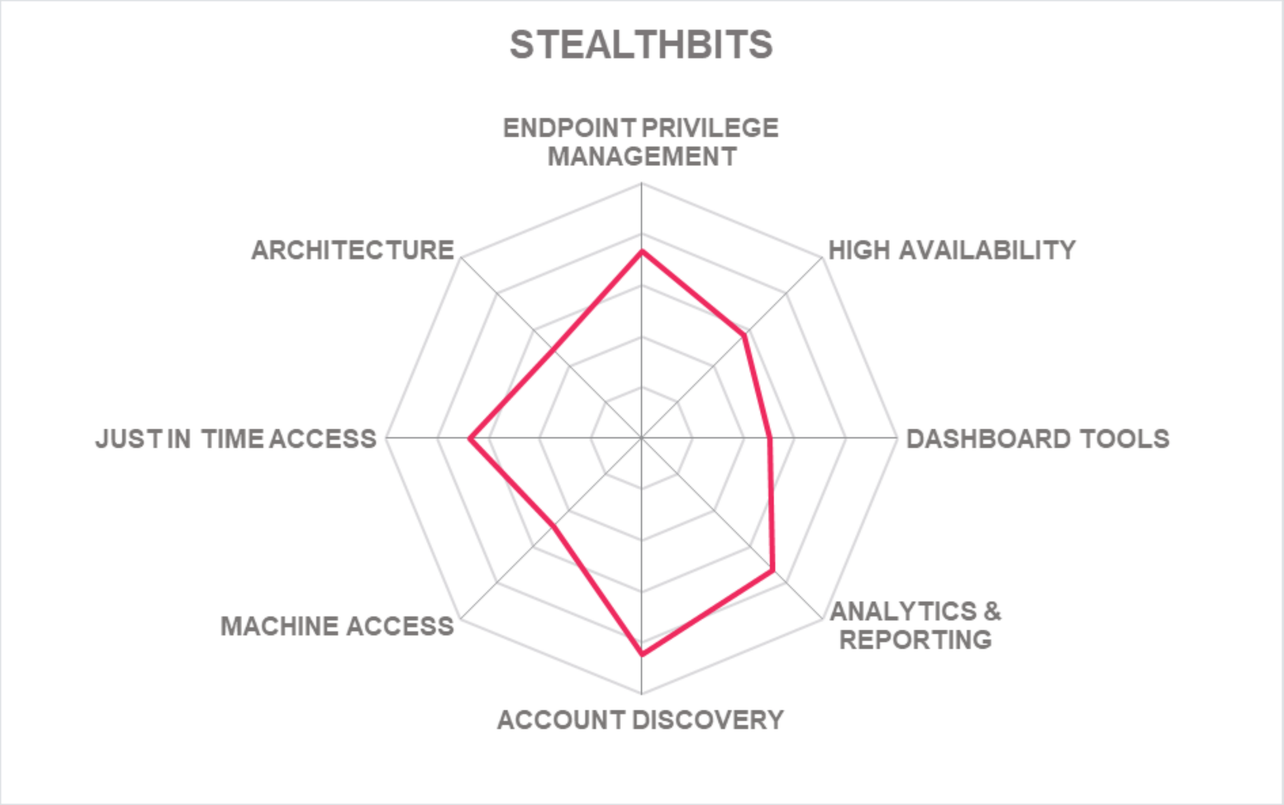
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


STEALTHBITS
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.23 Systancia

France based Systancia has several workplace and application virtualization tools. As part of this it offers the Cleanroom platform, which it developed as a PAM offering to the market. It is available on-premises or as a service in four product lines: Systancia Cleanroom Session, Systancia Cleanroom Desk, Systancia Cleanroom Session Service and Systancia Cleanroom Desk Service

Capabilities include Protocol-based session management and administration of resources (Web, SSH, RDP, VNC) and application-based session management and administration of resources. The platform also has an integrated vault, SSO and password rotation, account discovery and AAPM.

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 native recording of sessions with agentless recording straight from the browser, and videos are fully searchable. The Web Admin Console can access all previous sessions, including all events such as windows opening and closing.

SSO login is available for all admin's resources and applications, and the ability to block suspicious activity in real time. MFA support is available via 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 and probably works best in partnership with that. Overall, we would have liked to have seen greater PAM development for a platform that promises much in usability, automation and Identity integration. This is a fine specialist product with a lot of capabilities for secure workplace delivery, integration with Systancia IAM, and baseline PAM but is less as a full capability PAM product against much of the competition here. There is much room for development however if Systancia wish to build on that.

Security	● ● ● ● ●
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

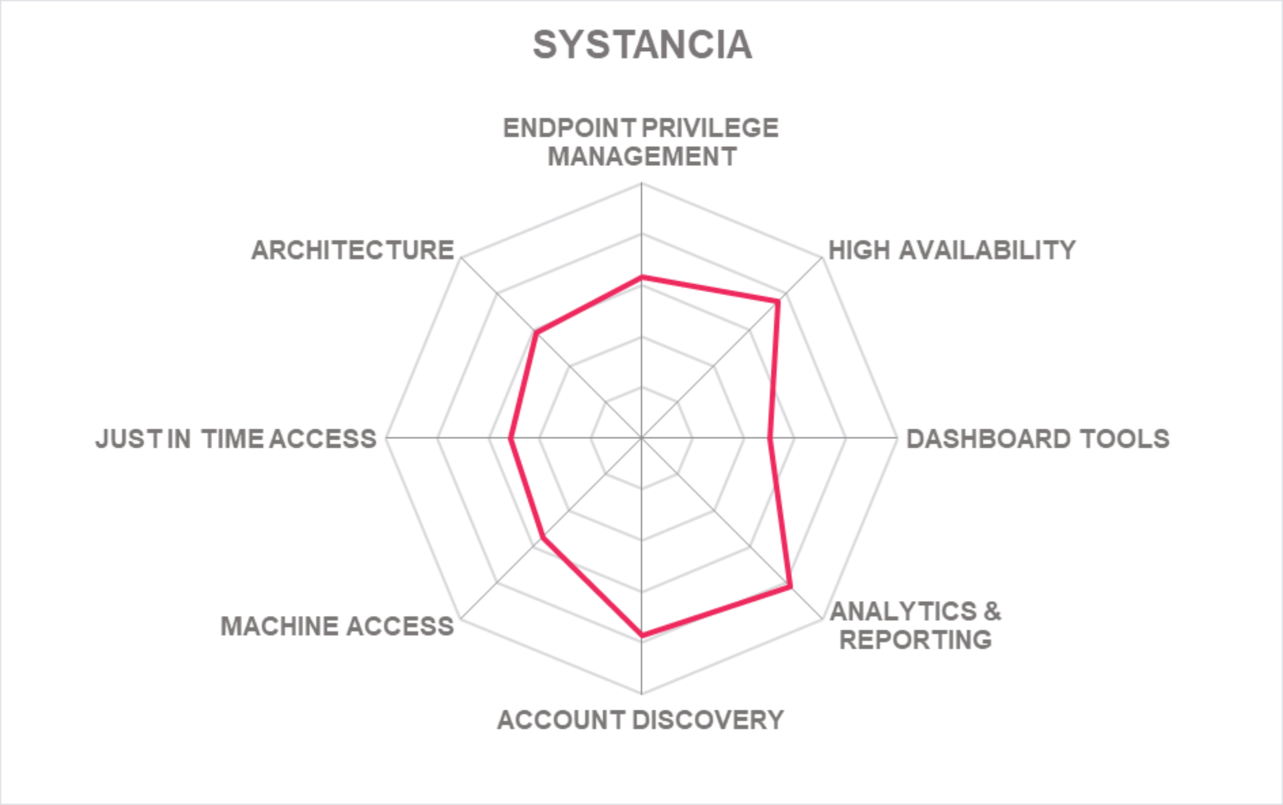
Systancia

Strengths

- Still one off the best user interfaces on the market
- VM works well to isolate sessions and keep secrets secure
- Clever use of automation for login and credential management
- Fully supports in-house IAM suite from Systancia
- Good job of developing product for more advanced applications

Challenges

- Lack some PEDM and DevOps support
- 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 if looking for PAM only


SYSTANCIA
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.24 Thycotic

Based in Washington D.C. (US), Thycotic offers Secret Server as its primary Password Management product and Privilege Manager for Endpoint Privilege Management. The company's product portfolio is known for its comprehensiveness, ease of deployment and configuration. The company recently merged with Centrify but for now the products continue to be sold and supported separately.

Thycotic's portfolio consists of five key modules: Secret Server, Privilege Manager (for workstations and servers), Account Lifecyle Manager, DevOps Secrets Vault plus the Connection Manager to manage remote connections. Secret Server and Privilege Manager are supported by Privileged Behavior Analytics. That is a lot of products in a market that is drifting towards platform consolidation; one of the challenges for Thycotic post-merger will be how to combine these with Centrify's platform.

Privilege Manager is Thycotic's agent based EPM solution for Windows, Mac, and Linux 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.

Thycotic offers some key developments since our last Leadership Compass outing. A new Session Connector provides support for jump hosts and moves session recording away from client endpoint or the target server. A new integration between Secret Server and DevOps Secrets Vault allows usage of the CI/CD pipeline integrations present in DevOps Secrets Vault while using credential management and password rotation in Secret Server. Thycotic also joins the ranks of PAM providers to support iOS and Android devices with Secret Server Mobile. DevOps Secrets Vault can now be integrated with SIEM platforms.

Thycotic Privilege Manager benefits from several UI improvements for policy management and the introduction of a new Wizard tool -- we would like to see more vendors introduce such ease-of-use enhancements. The Connection Manager can now open multiple connections at once, bulk edit capabilities for local connections and customize themes for SSH sessions. There is also an Auto Reconnect to Secret Server after loss of connectivity.

Thycotic has committed to frequent product updates including for DevOps Secrets Vault, and the Account Lifecycle Manager. Thycotic is on the right lines by saying that PAM for DevOps is more about secrets management and development cycles, than just issuing passwords in the traditional sense. To that end, credentials will get embedded into microservices, not a vault, in Thycotic's approach. We expect to see a very different presentation of Thycotic technologies in 2022.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

thycotic

Strengths

- Solid and well-known brand that has mixed product choice with enhanced capabilities
- Ongoing product development and frequent updates show commitment
- Thycotic understands that PAM for DevOps needs to take account of coding environments
- Good new user interface leverages current UX trends for ease of use; Wizards tools now added
- Strong endpoint management capabilities for complex digital environments
- Supports most advanced capabilities

Challenges

- Merger with Centrify may lead to period of uncertainty and loss of momentum in the market
- We would like to see simplification of product choices although merger will undoubtedly affect how this plays out
- May need to convince larger organizations of the need to replace legacy PAM

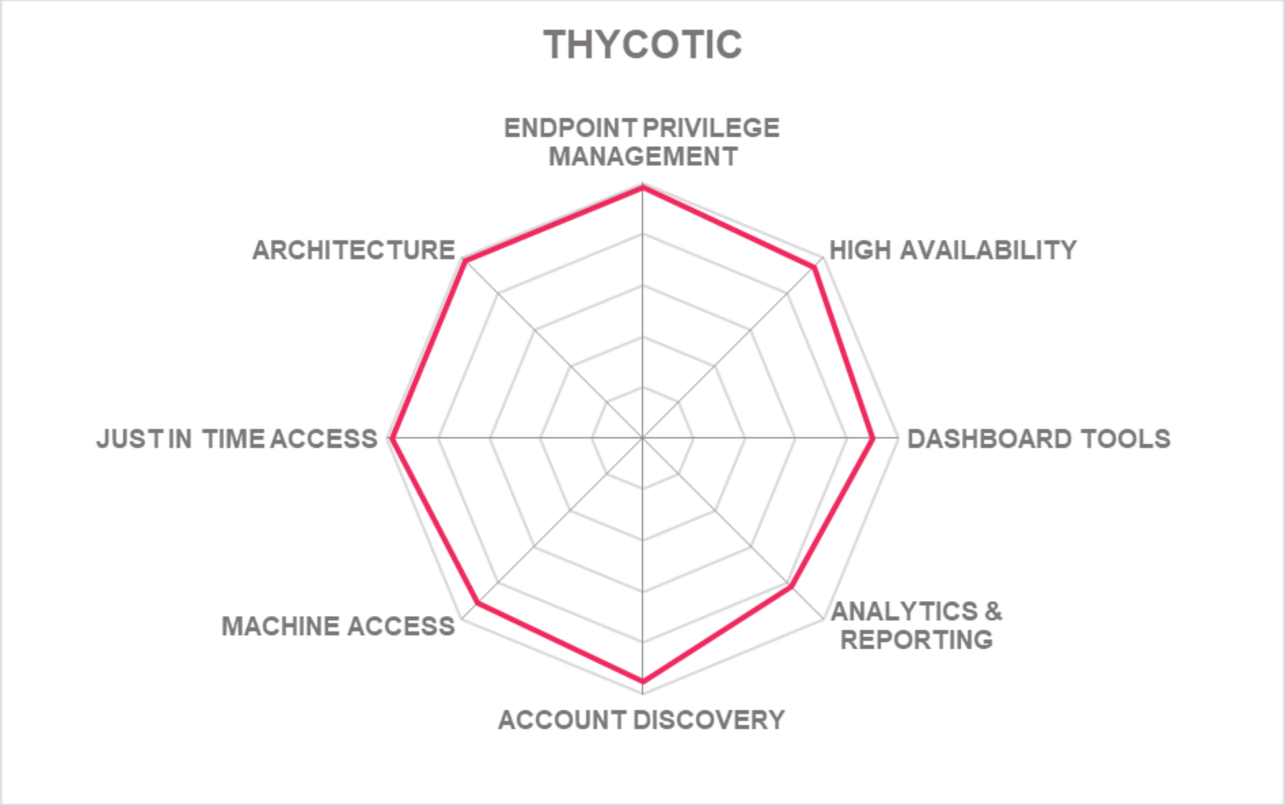
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


THYCOTIC
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.25 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 Bastion consists of five major components that together form a solid foundation for enterprise level PAM: Session Manager, Password Manager (Vault), Access Manager, Privilege Elevation and Delegation Manager (PEDM) and Application to Application Password Manager (AAPM). To complete the picture, WALLIX Bastion is now compatible with WALLIX BestSafe which fills a previous gap in the WALLIX portfolio by providing Endpoint Privilege Management (EPM).

The need for EPM has been brought into sharp relief by the major shift to home working triggered by the COVID-19 epidemic, which is likely to have a lasting impact on business practices. 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 to eliminate hard-coded passwords and provide credentials to DevOps tools.

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.

WALLIX has made improvements to password management; AAPM has capacity to provide virtual filesystem monitoring and replace on the fly placeholders with passwords for applications which rely on passwords being present in a configuration file. Only authorized applications can read this password automatically from the filesystem. New plugins have been released to allow Azure AD password rotation, and new database systems to be managed

WALLIX Bastion now has real time and extendable reporting and dashboarding capacities provided out of the box, based on the profile orientation for auditors and functional administrators. A new Access Manager provides access over native RDP clients.

By building on its existing capabilities for password management and privileged session management (PSM) and adding enhanced EPM, AAPM and better DevOps support, WALLIX now has a highly competitive level of PAM capabilities that should be seriously considered by buyers in all organizations.

BASTION

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○

Strengths

- Well-engineered PAM solution that offers basic and advanced features to a high level of functionality
- Proven in multiple operating environments including OT, industrial and SCADA
- High level of privilege session management and recording capabilities
- Web access gateway and a single administrative console for all Bastion instances
- Strong support for multi-tenancy and HA options
- Non-intrusive, agentless architecture
- Strong execution on a well-thought-out product roadmap

Challenges

- Some admin-focused aspects of platform UX are still behind the curve on current design practice
- WALLIX now needs to expand its presence beyond EMEA with this improved proposition
- DevOps support has solid base in AAPM and Bastion vault, but WALLIX should now develop this further for more native integration

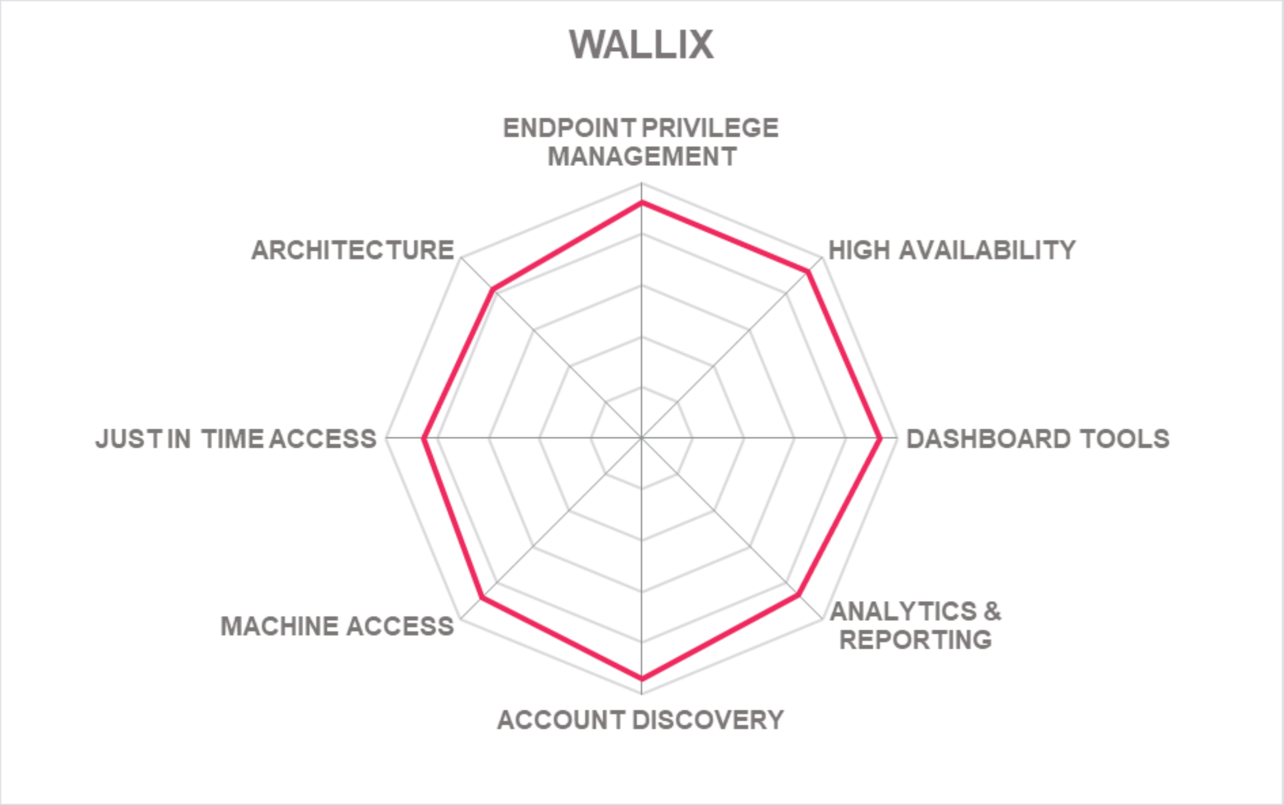
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


WALLIX
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

5.26 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 meet compliance requirements. In July 2021, Xton was acquired by Imprivata, a digital identity company for healthcare and beyond.

Xton claims that its solution was built from the ground up in 2017 and can be installed rapidly. The company says its solution is agentless and has both advanced RDP, SSH and HTTP(s) proxies and HTML 5 that can record sessions, keystrokes, and file transfers.

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, something hard to argue with if update are pushed. Updates are deployed via the GUI and latest improvements include Zero Trust login and session recording for AWS command line and automation tools, access to isolated networks without firewall changes and an improved Administrator Dashboard.

XTAM, provides a web-based password vault with accounts discovery, shared account password management and privileged session management capabilities including password rotation, access request workflows and session and keystroke recording with playback. Credentials never leave the vault and the solution also supports Just-in Time (JIT) provisioning.

While Xton does not provide privilege elevation and delegation management (CPEDM) capabilities, it offers support for elevated script automation for routine privilege escalation tasks, enhancing administrator efficiency.

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.

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 well-known 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. An interesting alternative option, and one to watch -- but needs more capabilities.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

XTON technologies

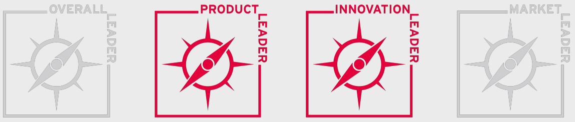
Strengths

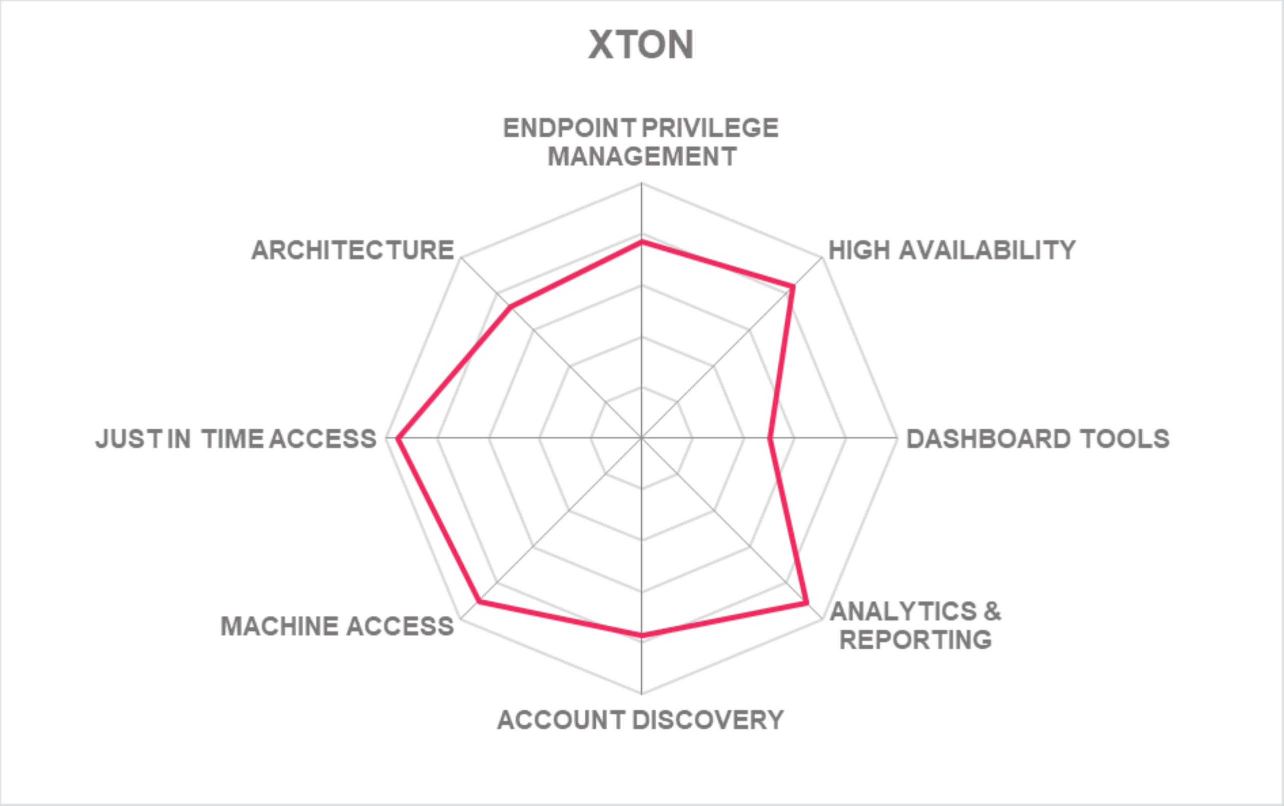
- Solid overall package that supports most of the advanced PAM functions needed for larger organizations
- Sensible incremental improvements have boosted its ratings
- Wide number of options available for 2FA and MFA implementation
- Passwords and key never transmitted to the end user
- Can be offered 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

Leader in




XTON
ENDPOINT PRIVILEGE MANAGEMENT
HIGH AVAILABILITY
DASHBOARD TOOLS
ANALYTICS & REPORTING
ACCOUNT DISCOVERY
MACHINE ACCESS
JUST IN TIME ACCESS
ARCHITECTURE

6 Vendors to Watch

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.

Why worth watching: It appeals to organizations with basic PSM needs along with the requirements of regional delivery and integration support.

6.2 HashiCorp

San Francisco (US) based HashiCorp is a provider of application development and delivery management software for datacentres. 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-datacentres environments such as disaster recovery and replication are only available as part of team and enterprise versions.

While, not a complete PAM platform, HashiCorp offers password vaulting and secure application to application password management capabilities to support enterprise DevOps initiatives.

Why worth watching: While several other PAM vendors are now offering similar capabilities to suit DevOps, HashiCorp offers a good start for organizations looking to onboard PAM within 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.

Why worth watching: 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.

Why worth watching: Iraje's PIM is targeted at 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.

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.

Why worth watching: 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 Session Management platform that is deployable and scalable across a variety of IT systems. ObserveIT is one of a few specialized vendors that originated in Session Recording and Monitoring (SRM) and extended it to include other PSM features. It offers detailed user behaviour analysis and live session response 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 behaviour analytics that detects and alerts anomalous user behaviour. Observe IT also offers live session response that allows for interruption of sessions at runtime based on information fed from user behaviour 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.

Why worth watching: An agent-based approach allows for detailed logging and therefore a more meaningful and efficient activity search in contrast to other similar solutions that are primarily proxy or gateway-based.

6.7 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 one of the most advanced SSH key management platforms in the market.

Why worth watching: 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 -71273
Architecture 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
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

Endnotes

[1] Vectra 2020 RSA Conference Edition of the Attacker Behaviour Industry Report and Spotlight Report on Privilege Access Analytics Report

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

All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, 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 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.