KuppingerCole Report

LEADERSHIP COMPASS

by Anmol Singh | March 2019

Privileged Access Management

Privileged Access Management (PAM), over the last few years, has evolved into a set of crucial technologies that addresses some of the most urgent areas of Cybersecurity today. Continuing the growth trajectory, the PAM market has entered a phase of consolidation characterized by increased price competition and an intensified battle for market share. This Leadership Compass provides a detailed analysis of the PAM market and its key players to help security and IAM leaders find the right product(s) that best fit their cybersecurity needs.

by **Anmol Singh**
asi@kuppingercole.com
March 2019

Leadership Compass
Privileged Access Management
By KuppingerCole

Content

List of Tables

List of Figures

Related Research

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Advisory Note: Secure your Cloud against Industrial Espionage - 70997

Advisory Note: Cloud IAM: More than just Single Sign-On to Cloud Applications - 71031

Advisory Note: The new ABC for IT: Agile Businesses – Connected - 70998

Advisory Note: Connected Enterprise Step-by-step - 70999

Architecture Blueprint: Access Governance and Privilege Management - 79045

Executive View: ARCON Privilege Manager - 70950

Executive View: BeyondTrust PowerBroker for Unix & Linux - 70363

Executive View: CA Privileged Access Management Suite - 79047

Executive View: Centrify Next-Gen Access Platform - 79036

Executive View: Cloud Standards Cross Reference - 71124

Executive View: EmpowerID - 70894

Executive View: EU Guidelines for Cloud Service Level Agreements - 71154

Executive View: Vendor Overview CyberArk - 70280

Executive View: Hitachi ID Privileged Access Manager - 80030

Executive View: i-Sprint AccessMatrix Universal Sign-On - 71064

Executive View: Krontech SingleConnect - 80031

Executive View: ManageEngine Password Manager Pro - 70613

Executive View: Micro Focus Privileged Account Manager - 71314

Executive View: One Identity Safeguard - 79042

Executive View: Osirium: Privileged Access Management - 70836

Executive View: SSH.COM PrivX - 70302

Executive View: Thycotic Privilege Manager - 80004

Executive View: Wallix AdminBastion - 71266

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 71139

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 72330

Leadership Compass: Access Management and Federation - 71147

Leadership Compass: Access Governance & Intelligence - 71145

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings in a certain market segment. This Leadership compass focuses on the market segment of on-premises or cloud delivered Privileged Access Management. PAM has emerged as one of the most crucial IAM technologies that has a direct relevance and impact on an organization's cybersecurity program.

1.2 Market Segment

In the age of digital transformation, not only the requirements for IT, but also the way IT is done, are constantly evolving. To remain relevant, organizations must reinvent themselves by being agile and more innovative. Emerging technology initiatives such as digital workplace, DevOps, security automation and the Internet of Things continue to expand the attack surface of organizations as well as introduce new digital risks. To stay competitive and compliant, organizations must actively seek newer ways of assessing and managing the security risks without disrupting the business. Security leaders, therefore, have an urgent need to constantly improve upon the security posture of the organization by identifying and implementing appropriate controls to prevent such threats.

Privileged Access Management (PAM), over the past few years, has become one of the most relevant areas of Cyber Security associated with IAM (Identity and Access Management) that deals with identifying, securing and managing privileged credentials and the resulting access across an Organization's IT environment. Once considered a technology option for optimizing administrative efficiency by managing passwords and other secrets, PAM has evolved into a set of crucial technologies for preventing security breaches and credential thefts. PAM today concerns Security and Risk Management leaders as well as Infrastructure and Operation (I&O) leaders across the industries for several security and operational benefits.

Privileged Access Management represents the set of critical cybersecurity controls that address the security risks associated with privileged users and privileged access in an organization. There are primarily two types of privileged users:

1. Privileged Business Users - those who have access to sensitive data and information assets such as HR records, payroll details, financial information, company's intellectual property, etc. This type of access is typically assigned to the application users through business roles using the application accounts.
2. Privileged IT Users – those who have access to IT infrastructure supporting the business. Such access is generally granted to IT administrators through administrative roles using system accounts, software accounts or operational accounts.

The privileged nature of these accounts provides their users with an unrestricted and often unmonitored access across the organization's IT assets, which not only violates basic security principles such as least privilege but also severely limits the ability to establish individual accountability for privileged activities. Privileged accounts pose significant threat to the overall security posture of an organization because of their heightened level of access to sensitive data and critical operations. Security leaders therefore need stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Available Identity and Access Management (IAM) tools are purposely designed to deal with management of standard users' identity and access, and do not offer the capabilities to manage privileged access scenarios such as managing access to shared accounts, monitoring of privileged activities and controlled elevation of access privileges. Privileged Access Management tools are designed to address these scenarios by offering specialized techniques and process controls, thereby significantly enhancing the protection of an organization's digital assets by preventing misuse of privileged access.

While credential vaulting, password rotation, controlled elevation and delegation the focus of attention for PAM tools, more advanced capabilities such as privileged user analytics, risk-based session monitoring and advanced threat protection are becoming the new norm. With the attack surface expanding and the number and sophistication of attacks increasing every year, an integrated and more comprehensive PAM solution is required – one that can automatically detect unusual behavior and initiate automated mitigations. A successful attack can be conducted in minutes; therefore, a PAM solution must be capable of thwarting this attack without human intervention. And although we see more comprehensive PAM suites and solutions being offered, vendors are taking different approaches to solve the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts.

Among the key challenges that drive the need for managing privileged access are:

- Abuse of shared credentials
- Abuse of elevated privileges by authorized users
- Hijacking of privileged credentials by cyber-criminals
- Abuse of privileges on third-party systems, and
- Accidental misuse of elevated privileges by users

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software and service accounts across the IT infrastructure
- Identification and continuous tracking of ownership of privileged accounts throughout their life-cycle
- Establishing and managing privileged session to target systems for enhanced operational efficiency of administrators
- Auditing, recording and monitoring of privileged activities for regulatory compliance
- Managing and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems, and
- Managing and monitoring privileged access of business users and IT administrators to cloud infrastructure and applications

Consequently, multiple technologies and solutions have been developed to address these risks, as well as provide better activity monitoring and threat detection.

1.3 Required Capabilities

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

tools and technologies used for managing privileged access have been marketed under various terms used by vendors – Privileged Account Management, Privileged Identity Management, Privileged User Management and Least Privilege to name a few. While we referred to this market as PxM in the past, we decided to rename it as 'Privileged Access Management' or 'PAM' to reflect on the 'access management' aspect that primarily focuses on managing privileged access of users and IT administrators through individual or shared accounts and other privilege delegation and elevation mechanisms.

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

Shared Account Password Management (SAPM): Shared Account Password Management offers technology to securely manage privileged credentials including system accounts, service accounts or application accounts that are generally shared in nature. At the core of SAPM products is an encrypted and hardened password vault for storing passwords, keys and other privileged credentials for a controlled, audited and policy-driven release and update. These products support periodic, scheduled or event-driven randomization of passwords and other credentials as the fundamental requirement.

Privileged Session Management (PSM): Privileged Session Management offers the technology to establish a privileged session to target systems including basic auditing and monitoring of privileged activities. PSM tools also offer authentication, authorization and Single Sign-On (SSO) to the target systems.

Application-to-Application Password Management (AAPM): AAPM is an extension of SAPM tools to manage accounts used by an applications or systems to communicate with other applications or systems (such as databases etc.). This includes use of service accounts used to execute certain functions or trigger processes with necessary privileges for a successful execution. AAPM tools offer elimination of hardcoded credentials in application code, scripts and other configuration files by offering a mechanism (generally APIs) to make credentials securely available when requested.

Session Recording and Monitoring (SRM): SRM is an extension of PSM tools to offer advanced auditing, monitoring and review of privileged activities during a privileged session, including but not limited to key-stroke logging, video session recording, screen scraping, OCR translation and other session monitoring techniques.

Controlled Privilege Elevation and Delegation Management (CPEDM): Technology that deals with controlled elevation and policy-based delegation of a users' privileges to super-user privileges for administrative purposes.

Privileged User Behavior Analytics (PUBA): PUBA uses data analytic techniques to detect threats based on anomalous behavior against established behavioral profiles of administrative users as well as user groups and administrator roles.

Privilege Account Discovery and Lifecycle Management (PADLM): This deals with discovery mechanism to identify shared accounts, software accounts, service accounts and other unencrypted/ clear-text credentials across the IT infrastructure. PADLM tools offer workflow capabilities to identify and track the account's business and technical ownership throughout its lifecycle and can detect changes in its state to invoke notification and necessary remedial actions.

Endpoint Privilege Management (EPM): EPM offers capabilities to manage threats associated with local administrative rights on windows, mac or other endpoints. EPM tools essentially offer controlled and monitored escalation of user's privileges on endpoints and include capabilities such as application

whitelisting for endpoint protection. Categorically, we define EPM solutions to primarily offer three distinct technologies:

a. **Application Control**: This allows organizations to control what applications can be allowed to run on an endpoint. This is usually achieved through application whitelisting in which only known good applications are placed on a pre-approved list and are allowed to run. Application control provides effective protection against shadow IT challenges for organizations.
b. **Sandboxing**: This technology uses the approach to isolate the execution of unknown applications or programs by restricting the resources they can access (for eg., files, registries etc.). This technology, also known as application isolation, provides an effective protection against cyberattacks by confining the execution of malicious programs and limiting their means to cause the harm.
c. **Privilege Management:** This technology encompasses user and application privilege management. For user privileged management, it deals with controlled and monitored elevation to local admin privileges. Application privilege management deals with exception or policy-based elevation of administrative rights for known and approved applications to execute successfully.

Privileged Access Governance (PAG): PAG deals with offering valuable insights related to the state of privileged access necessary to support decision making process. PAG includes privileged access certifications and provisions for customizable reporting and dashboarding.

At KuppingerCole, we define PAM solutions to constitute of the tools and technologies demonstrated in the Figure 1.

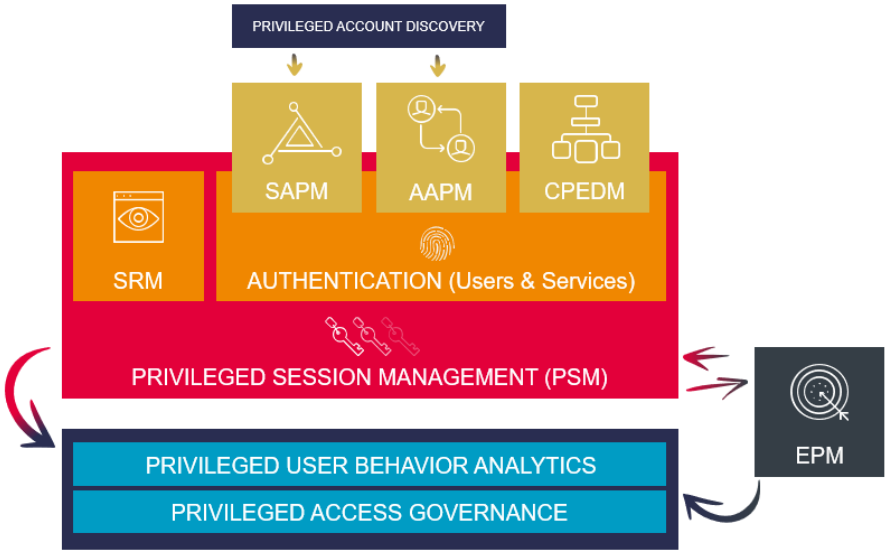


Figure 1: Architecture Blueprint of PAM tools and technologies

Privileged Account Discovery and Lifecycle Management (PADLM)
Shared Account Password Management (SAPM)
Privileged Session Management (PSM)
Session Recording and Monitoring (SRM)
Privileged User Behavior Analytics (PUBA)
Controlled Privilege Elevation and Delegation Management (CPEDM)
Application-to-Application Password Management (AAPM)
Endpoint Privilege Management (EPM)
Privileged Access Governance (PAG)

We look at all types of products that support customers in solving the Privileged Access Management challenges fully or partially. This includes, e.g., Session Monitoring and Recording as well as Password Vaults or Privileged User Behavior Analytics.

We do not look at general-purpose tools such as Identity Provisioning tools or Real Time Security Intelligence with very limited support for the specific requirements of the Privileged Access Management challenges. However, integration with such solutions is on the list of features we consider as being relevant in our analysis.

Particularly, we are looking for features and functionalities in the following areas corresponding to privileged access:

- Shared Account Password Management
- Privileged Single Sign-On (SSO access to multiple privileged sessions)
- Privileged Account Discovery and Lifecycle Management
- Session Monitoring, Analysis, and Recording
- Privileged User Behavior Analytics
- Privilege Elevation Management (Restriction)
- Application-to-Application Password Management
- Endpoint Privilege Management
- Reporting, Audit, and Compliance

We appreciate seeing integrated solutions with a tight integration of the various feature sets. Key features that we expect to see in the various PAM areas include:

- Shared Account Password Management
  - ✓ Password vaulting
  - ✓ Central management of shared account privileges
  - ✓ Automated credential rotation or OTPs
  - ✓ Secured Access to privileged credentials
- Privileged Single Sign-On (SSO access to multiple privileged sessions)
  - ✓ Simple management of session assignments to users

- ✓ Ad-hoc and upfront authorization of access with support of approval lifecycles
- ✓ Simple yet secure UIs

- Privileged Account Discovery and Lifecycle Management
  - ✓ Automated discovery of privileged accounts on servers, clients, and other systems in scope (e.g. network devices)
  - ✓ Integration into CMDBs
  - ✓ Simple (automated) grouping of accounts and systems
- Session Monitoring, Analysis, and Recording
  - ✓ Session Monitoring
  - ✓ Session Recording
  - ✓ Session Analysis
  - ✓ All for both CMD based and GUI based sessions
- Privileged User Behavior Analytics
  - ✓ Anomaly detection in privileged user behavior
  - ✓ Adaptation of analysis to custom requirements
  - ✓ Support for privacy and compliance, e.g. four-eye-principle for reviewing anomalies
- Privilege Elevation Management (Controlled Privilege Elevation)
  - ✓ Restricted (least privilege) access to managed systems
  - ✓ Command filtering
  - ✓ Command/ Shell substitution
- Application-to-Application Password Management
  - ✓ Identification of hard-coded credentials in scripts, configuration files, etc.
  - ✓ APIs for replacing hard-coded credentials
  - ✓ Application or service authentication calling password vault for credential checkout or injection
- Endpoint Privilege Management
  - ✓ Application Control (Whitelisting/ Blacklisting capabilities)
  - ✓ Application Sandboxing (Executing untrusted or less trusted applications in a controlled environment)
  - ✓ Privilege elevation of local users
- Reporting, Audit, and Compliance
  - ✓ Flexible reporting interfaces, customizable

Providing tightly integrated offerings that cover all major features is one of the criteria we have high on our list, given that customers prefer such integrated approaches over a variety of disparate, non-integrated or only loosely coupled offerings.

A strong focus will be put on integration into existing security infrastructures to provide consolidated monitoring, analytics, governance or compliance across multiple types of information stores and applications. Most importantly, this includes integrations with SIEM/SoC solutions, existing identity and access management systems and information security governance technologies.

Additional architectural and operational aspects that are considered in our vendor evaluation process are:

- Support for a broad range of target systems
- Support for cloud services and platforms
- Support for Multi-tenancy
- Support for High Availability (HA) and automated failover configurations
- Ease of integration with third-party security solutions including ITSM, SIEM etc.
- Delivery formats: Hardware or virtual appliances, PAM-as-a-Service or managed hosted service
- Deployment types: Agent or network proxy/ gateway based, remote passive monitoring Scalability and performance impact
- Easy of deployment and initial configuration, including involved friction to administrative behavior
- Flexibility and user-friendliness of the management console and overall user interfaces

2 Leadership

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

Based on our analysis of the vendor's products, we create several Leadership ratings for use by organizations during product evaluation. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Figure 2: The Overall Leadership rating for the Privileged Access Management market

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of evolving markets, where there are a fewer vendors in the leaders' segment than the challengers' segment. The market is getting crowded with about 3-4 new vendors entering the market last year. We chose to represent about 20 vendors in our Leadership Compass with a mention of 10 other notable vendors in the 'vendors to watch' section that either declined to participate or did not meet our basic evaluation criteria.

CyberArk retains its leadership position in the Overall Leadership evaluation of PAM market with BeyondTrust following it from a close distance. Centrify and Thycotic, having made some significant enhancements to their product strategy and partnerships, take a big leap forward with CA Technologies following them at a distance. One Identity, with the recent changes to its product architecture combined with marketing execution, has regained its leadership position to be in the long-established PAM players.

With a stronger focus on process innovation and privileged access governance, HitachiID gets placed in the Challengers' section, closely followed by WALLIX. Following them is ARCON, which has positioned itself considerably ahead of Micro Focus and EmpowerID in the challengers' section.

Other vendors in the challengers' segment include ManageEngine and SSH.COM – both of which find a considerable push into the challengers' segment with their improved ratings for market presence and partnership ecosystem.

MT4 Networks, Osirium and Fudo Security are positioned next in the Challengers' segment with fit-for-purpose PAM capabilities.

Krontech, iSprint and Sectona are featured in followers' segment as either they are very new to the market and trying to get a grip of it, or their approach to PAM market isn't very relevant according to customers' PAM requirements.

Overall Leaders are (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- One Identity
- Thycotic

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

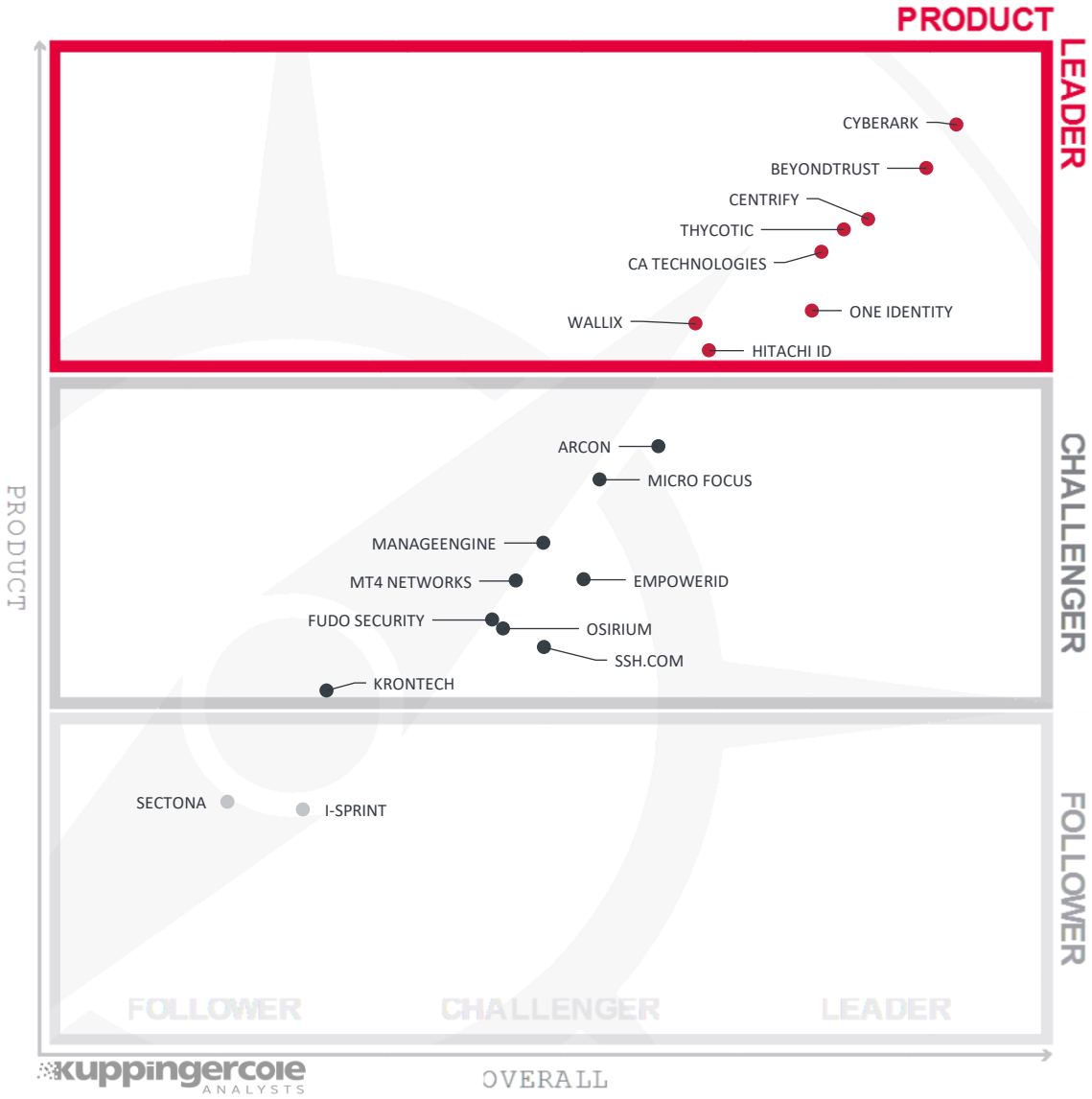


Figure 3: Product Leaders in the Privileged Access Management market segment

Product Leadership is the view where we look specifically at the functional strength and completeness of products. Here, we find some more vendors that have made it to the Leader's segment. Again, CyberArk is rated as the leading vendor, followed by BeyondTrust. Both have overall comprehensive feature sets which form a strong foundation for a Privilege Access Management implementation.

Following these two leaders, we find Centrify and Thycotic which also deliver strong and functionally comprehensive PAM products in the market. Next, we find CA Technologies that slipped its relative position in product leaders' segment due to the ambiguities associated with its Broadcom's acquisition. Next in the Leader's segment is WALLIX, that has evolved from a point vendor to a suite vendor and offers

a strong alternative to the leading vendors. Finally, we see Hitachi-ID in the leaders' segment, pushed further ahead for its PAM capabilities enhanced by closer integration with its Identity Manager.

ARCON and Micro Focus are positioned up in the challengers' segment with the group of ManageEngine, MT4 Networks and EmpowerID following them. All these vendors offer strong PAM features that might fit well for the specific PAM requirements of customers. Fudo Security, Osirium, SSH.COM and Krontech have specific strengths but still present certain gaps in the depth and breadth of supported functionalities, positioning them next in the challengers' section.

Lastly, we have Sectona and iSprint in the followers' segment – all these vendors have relatively newer PAM product and are still in the phase of executing on their PAM product roadmap.

Product Leaders (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Hitachi-ID
- One Identity
- Thycotic
- WALLIX

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging requirements they are facing. Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on delivering leading-edge new features which meet emerging customer requirements.

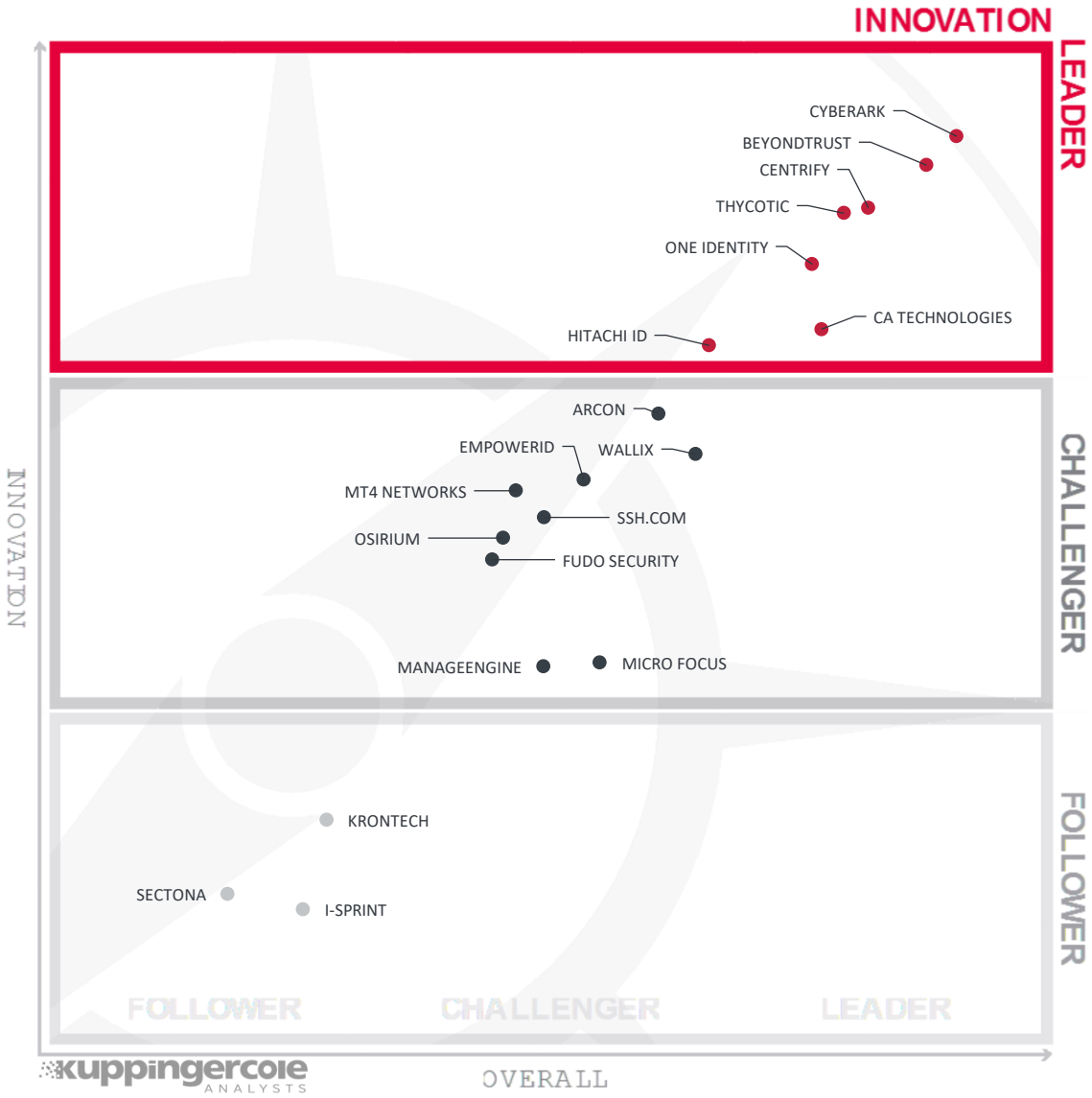


Figure 4: Innovation Leaders in the Privileged Access Management market segment

When looking at Innovation Leadership, we see a different picture. While most vendors still show gaps in functional completeness, affecting the Product Leadership rating, many vendors are putting a lot of work into innovative feature areas. Thus, we see many vendors in the Innovation Leader's segment.

Again, we see CyberArk in the lead, due to its focus on constant innovation amidst a challenging operating environment. Following CyberArk at a distance is BeyondTrust which also had a good culture for organic

innovation internally but takes a hit by the recent M&A activities. We find Centrify and Thycotic placed next, close to each other, depicting their increased focus on innovation compared to the competitors. Next in the league is One Identity that has taken on an impressive and innovative product roadmap and has been executing well to deliver value to its customers. CA Technologies and HitachiID are placed next with some good understanding of the market and continuing to innovate in relevant areas.

Placed in the upper part of the Challengers' segment for innovation leadership are ARCON and WALLIX. Positioned next are EmpowerID, MT4 Networks and SSH.COM, Osirium and Fudo Security - all that show a strong level of commitment to technology innovation that remained limited when it comes to expected value-add for the customers. Further below in the challengers' segment we find Micro Focus and ManageEngine, both having broader security portfolios, have made some progress but are still relatively less focused on PAM innovation as compared to their market size.

Further in the Followers' section are Krontech, Sectona and iSprint – all of which have been unable to depict sufficient understanding of market innovation thus far.

Finally, we see one vendor in the Follower's section, which is ManageEngine. They target the SMB market, not providing the same level of innovation in the feature set as some of the other vendors.

Innovation Leaders (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- Cyberark
- Hitachi ID Systems
- One Identity
- Thycotic

Finally, we looked at Market Leadership, i.e. the number of customers, the partner ecosystem, the global reach, and related factors affecting the leadership in a market. Market Leadership, from our point of view, requires global reach.

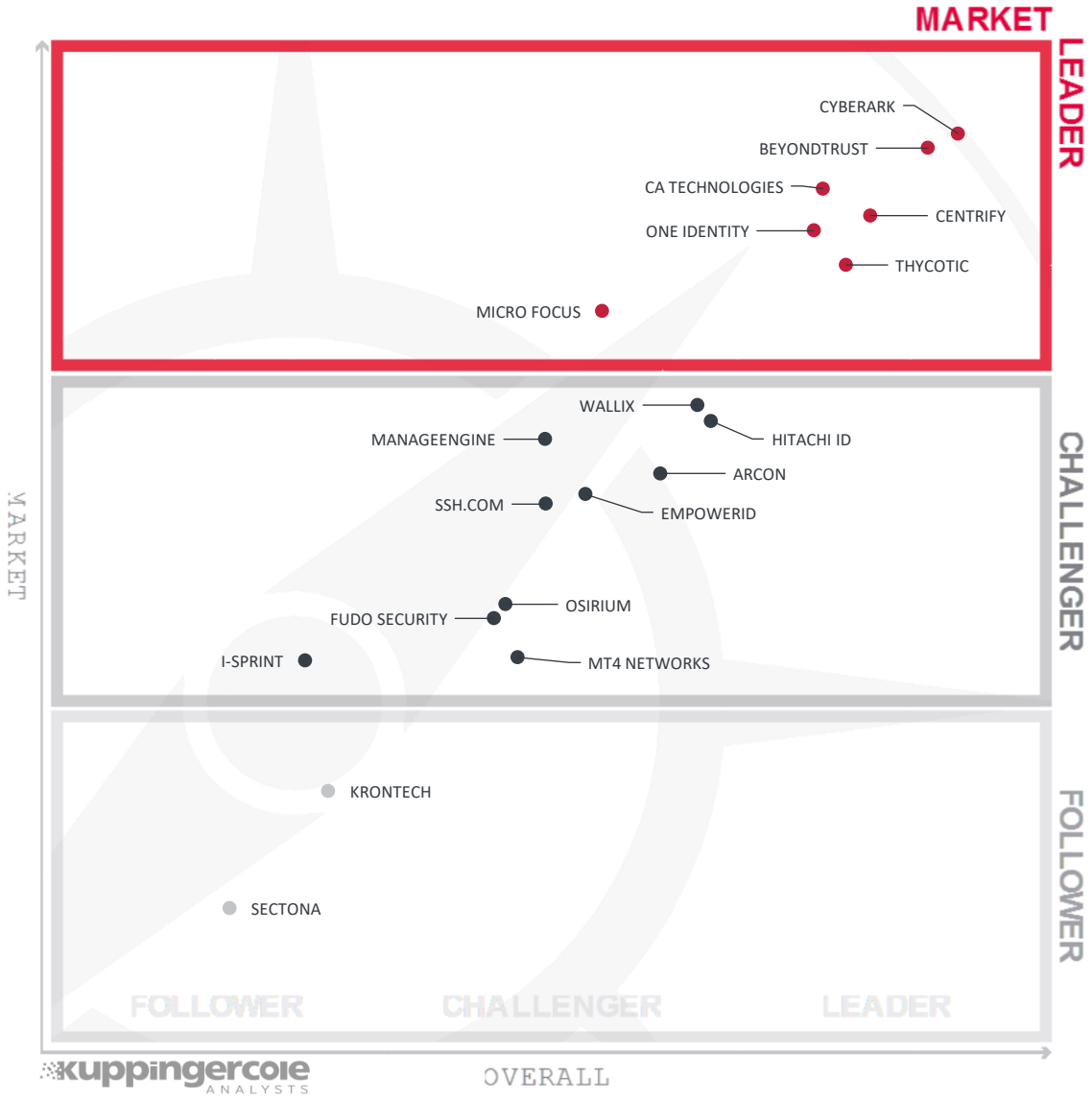


Figure 5: Market Leaders in the Privileged Access Management market segment

Here, we find CyberArk leading in the market leaders' segment. CyberArk over these years has established itself as the most prominent vendor in the Privileged Access Management market. Sharing the space with CyberArk is BeyondTrust which gets a good push in its overall market position from the recent acquisition by Bomgar. CA Technologies is another large software vendor that has a significant customer base for its PAM product, a considerably large and established partner ecosystem with global reach. Centrify and One Identity feature next with a selective but overall strong partner ecosystem and a growing customer base. Thycotic in partnership with IBM has gained a stronger market positioning while HPE helps Micro Focus expand and build stronger partner ecosystem.

WALLIX and HitachiID are positioned high up in the market challengers' segment with ManageEngine, ARCON, EmpowerID and SSH.COM following them at a close distance. Either lacking on a global partner ecosystem or having smaller than average deployment sizes, Osirium, Fudo Security, MT4 Networks and i-Sprint are next in the market challengers' section.

With a limited market reach and outlook, Krontech and Sectona are in the market followers' segment.

Market Leaders (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Micro Focus
- One Identity
- Thycotic

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, 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 deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views looks at Product Leadership and Market Leadership.

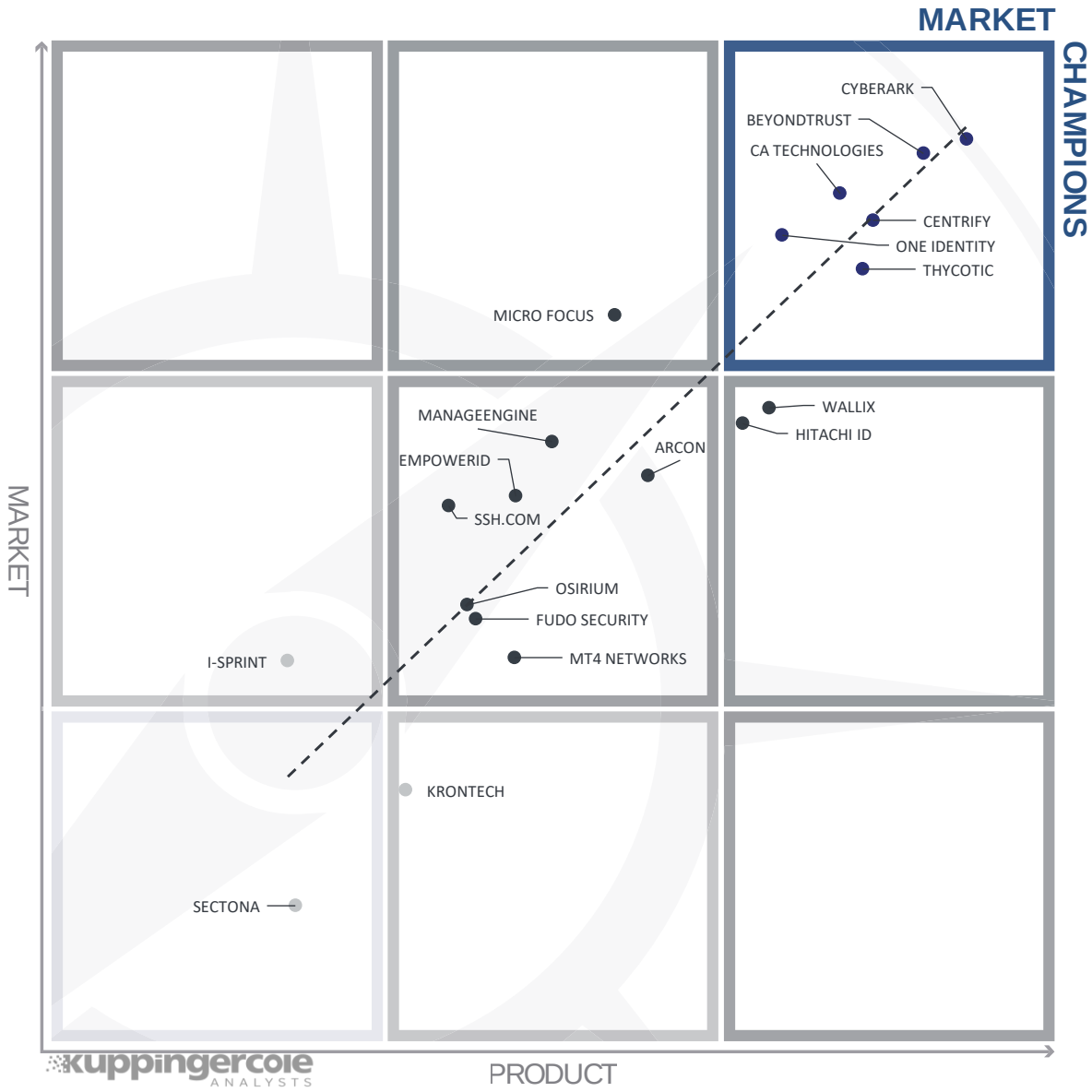


Figure 6: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. The more to the upper right edge, the better is the combined position. Vendors above the line are sort of “overperforming” in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line frequently are not as established in the market, but commonly show a comprehensive and innovative feature set.

The matrix shows a picture that is typical for evolving market segments, with a rather broad distribution of the various players across the quadrants and a weak correlation between Market Leadership and Product Leadership.

In the upper right box, we find CyberArk, BeyondTrust, CA Technologies, Centrify, One Identity and Thycotic. These vendors are leading in both the product and market ratings.

In the box to the left, we find Micro Focus depicting better market leadership in comparison to product leadership ratings.

In the box below, we find HitachiID and WALLIX, depicting their higher product leadership qualities as compared to market leadership ratings,

In the box at the center, we find (in alphabetical order) ARCON, EmpowerID, Fudo Security, ManageEngine, MT4 Networks, Osirium and SSH.COM – all that have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors

Finally, we see i-Sprint, Krontech and Sectona in the boxes towards the lower end of the graph showcasing limited market and product leadership ratings.

3.2 The Product/Innovation Matrix

The second 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 few exceptions. This distribution and correlation are typical for most markets with a significant number of established vendors plus some smaller players.

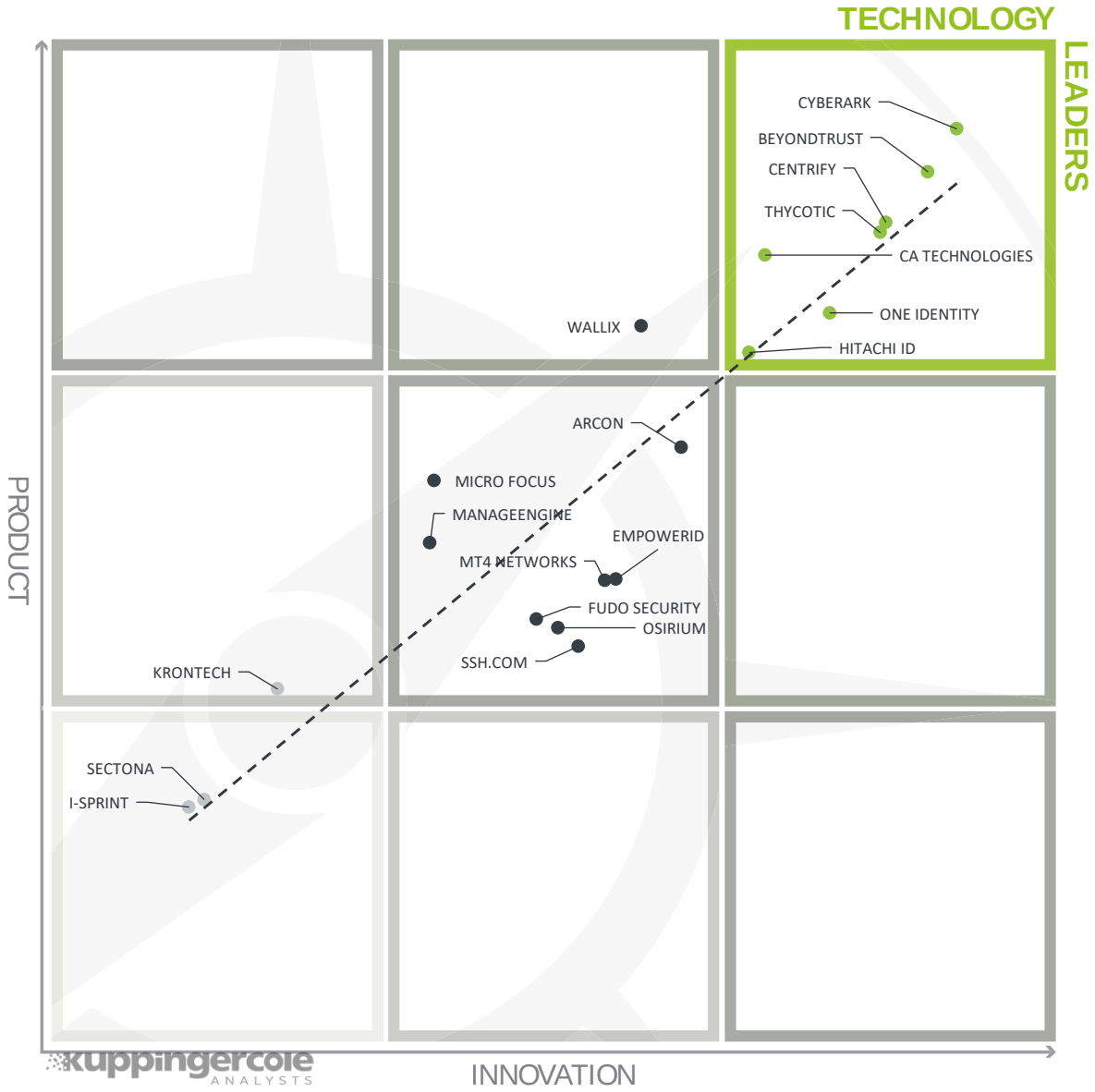


Figure 7: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most of the leading vendors in the upper right corner, scattered throughout the box. The top-notch vendors are CyberArk, BeyondTrust, CA Technologies, Centrify, HitachiID,

One Identity and Thycotic – all placed close to the axis depicting a good balance of product features and innovation. CA Technologies is positioned over the axis at a distance, showing a greater focus on product leadership as compared to innovation.

In the box to the left is WALLIX, indicating its greater focus on product leadership as compared to innovation in the PAM market.

Placed in a proximity to the axis in the same box are RSA Security and Beta Systems representing technology leaders with a good balance of product strength and innovation.

Down under the technology leaders' box are ARCON, EmpowerID, Fudo Security, ManageEngine, Micro Focus, MT4 Networks, Osirium and SSH.COM positioned in the middle of the chart, being the challengers for both product and innovation leadership.

Finally, we see i-Sprint, Krontech and Sectona in the boxes towards the lower end of the graph showcasing limited product and innovation leadership ratings.

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 to their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position but might also fail, especially in the case of smaller vendors.

Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relative weak position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

In the upper right-hand corner box, we see CyberArk, BeyondTrust, CA Technologies, Centrify, One Identity and Thycotic, all being successful in the market, but also showing strong innovation qualities.

To their left, at a distance over the axis, is Micro Focus with stronger market focus but limited innovation. In the box below the leaders, we find HitachiID with better innovation ratings compared to market leadership and showing stronger growth potential through their innovativeness.

In the box at the center, we find more challengers, ARCON, EmpowerID, Fudo Security, ManageEngine, MT4 Networks, Osirium, SSH.COM and WALLIX.

Finally, i-Sprint, Krontech and Sectona in the boxes towards the lower end of the graph for their limited market leadership and innovation ratings with i-Sprint having better market leadership ratings in comparison to its peers.

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 Privileged Access Management. 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.

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
ARCON	positive	positive	strong positive	positive	strong positive
BeyondTrust	strong positive	strong positive	positive	strong positive	strong positive
CA Technologies	strong positive	strong positive	positive	positive	strong positive
Centrify	strong positive	positive	strong positive	strong positive	strong positive
CyberArk	strong positive	strong positive	strong positive	strong positive	strong positive
EmpowerID	positive	neutral	strong positive	positive	positive
FUDO Security	positive	positive	neutral	neutral	positive
Hitachi ID	strong positive	strong positive	strong positive	strong positive	positive
I-Sprint	neutral	positive	neutral	weak	positive
Krontech	neutral	positive	neutral	neutral	neutral
ManageEngine	positive	positive	positive	positive	strong positive
Micro Focus	positive	positive	positive	positive	positive
MT4 Networks	positive	strong positive	positive	neutral	positive
One Identity	positive	strong positive	positive	positive	strong positive
Osirium	positive	neutral	positive	neutral	positive
Sectona	neutral	neutral	neutral	neutral	neutral
SSH.COM	positive	neutral	positive	positive	neutral
Thycotic	strong positive	strong positive	strong positive	positive	strong positive
WALLIX	strong positive	strong positive	positive	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	strong positive	positive	positive	positive
BeyondTrust	strong positive	strong positive	strong positive	strong positive
CA Technologies	positive	strong positive	strong positive	strong positive
Centrify	strong positive	strong positive	strong positive	strong positive
CyberArk	strong positive	strong positive	strong positive	strong positive
EmpowerID	positive	positive	positive	positive
FUDO Security	neutral	positive	positive	neutral
Hitachi ID	strong positive	positive	strong positive	positive
I-Sprint	neutral	neutral	positive	positive
Krontech	neutral	neutral	positive	weak
ManageEngine	neutral	strong positive	strong positive	positive
Micro Focus	neutral	strong positive	strong positive	strong positive
MT4 Networks	positive	neutral	positive	positive
One Identity	strong positive	strong positive	strong positive	positive
Osirium	positive	neutral	neutral	positive
Sectona	neutral	weak	neutral	neutral
SSH.COM	positive	positive	positive	strong positive
Thycotic	strong positive	strong positive	strong positive	strong positive
WALLIX	positive	positive	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

Table 2 requires some additional explanation regarding the “critical” rating.

In Innovativeness, this rating is applied if vendors provide none, or very few, of the more advanced features we have been looking for in that analysis, like support for DevOps, privileged user behavior analytics, built-in privileged access governance, multi-tenancy and built-in high availability.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn’t imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it’s also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no, or a very limited, ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/service evaluation

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

5.1 ARCON

Based in Mumbai (India), ARCON offers ARCON Privilege Account Management Suite to manage privileged access across a heterogenous mix of IT systems. ARCON's Privileged Account Management suite is delivered as a bundle of different modules that are licensed separately and offered in software, virtual and physical appliance and PAM as a service option. While most PAM functions are offered as part of the PAM suite, PUBA and CPEDM are available as separate modules from ARCON.

Primarily built on a ASP.NET framework, ARCON extends a set of APIs to integrate user configuration, vault and service access functions into web UIs. With built-in support available for most commercially available operating systems, servers, network devices and SaaS applications, ARCON offers password management, granular access and command control for databases – a capability missing from several leading PAM vendors in the market. ARCON's ability to develop customized connectors for password and account management for legacy applications and systems is viewed as a distinct advantage by several organizations that deem legacy infrastructure important to support critical business functions.

Strengths	Challenges
• Feature-rich comprehensive PAM solution • Large target connector base • Soft OTP and biometric authentication • Granular command control for databases • Readily integrable with SIEM and help-desk tools • Ease of deployment and administration • Available as a hosted and managed service, and PAM as a Service	• Client-based approach creates additional maintenance overheads • Increasing but limited penetration in North America and European markets • Pricing remains inconsistent across geographies and industry verticals • Growing but still weak brand awareness in some markets • Limited but sufficient EPM capabilities

Table 3: ARCON's major strengths and challenges

In addition to native software-based OTP authentication methods for session initiation, ARCON offers OOB integration with RSA and Entrust for hardware OTP tokens and with Gemalto for biometric authentication methods.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 4: ARCON's rating

With local presence in London, Dubai, Kenya, Toronto and Philippines and an operations and R&D centre in Mumbai, ARCON continues to observe some steady growth in Asia Pacific and Middle East & Africa markets.
Indian IT giants such as HCL, Wipro, Tech Mahindra and Tata Consultancy Services are among its key resellers, helping ARCON to position as a promising PAM vendor for large complex data center deployments. ARCON's product architecture combined with its in-built high availability, real-time password replication and automated recovery features makes it a preferable choice for large distributed data center deployments with requirements to support multi-tenancy and third-party remote access use-cases.

5.2 BeyondTrust

US based BeyondTrust, a long-established PAM vendor, now represents the combined entity resulting from the notable acquisitions of Lieberman Software, Avecto and BeyondTrust by Bomgar in 2018. The resultant entity that follows the aspiring M&As is labelled BeyondTrust and potentially represents one of the largest PAM vendors in combined revenue and customer size. BeyondTrust Privileged Access Management platform is now the combined product delivered across all major PAM streams. The privileged password and session management offers password vaulting and SAPM capabilities from formerly PowerBroker Password Safe and Lieberman RED products. A combination of Avecto Defendpoint and PowerBroker for Windows offers a strong EPM product with some considerable functionality overlaps. With Bomgar bringing in remote access management capabilities, BeyondTrust has one of the most complete PAM platforms in the market with some overarching product integration challenges in the short-term.

Strengths	Challenges
• Long-established market product, now with potentially largest market share • Host-based approach for CPEDM delivers strong and granular command control for privilege elevation • Integration with its popular vulnerability management platform offers unmatched asset discovery and threat detection capabilities • Integrated secure remote access capabilities with PAM allows for better visibility and control of third-party remote access • Expanded global presence and partnership consolidation strengthens its competitive position and creates additional opportunities in the market • Further simplified pricing model presents a strong alternative to market competition	• Considerable functionality overlaps resulting from multiple acquisitions by Bomgar over the last year • Difficulty rationalizing sales and partnership channels sends mixed signals in the market • Increased pipeline for engineering and development teams to integrate products under one umbrella and offer a consolidated platform • Difficulty positioning against Microsoft's own Device Guard and AppLocker components for Desktop EPM • Inconsistent scalability and availability across the products • While it supports most basic requirements, a focused approach for DevOps, PUBA and PAG is relatively absent

Table 5: BeyondTrust's major strengths and challenges

Integration with BeyondTrust vulnerability management platform brings advance threat analytics capabilities through asset discovery, vulnerability assessment, risk scoring and built-in reporting functions. BeyondTrust has a clear integration roadmap and promises a smooth transition for its customers into the integrated platform.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 6: BeyondTrust's rating

An expanded sales and partner ecosystem present enormous growth opportunities for BeyondTrust both in new regions and across new industry verticals. At the core, BeyondTrust remains a trusted solution for organizations looking to address PAM requirements of a complex hybrid IT environment.

5.3 CA Technologies

New York based CA Technologies has enjoyed a rich and long history of being a leader in the Identity and Access Management market, mostly through the several acquisitions made over a decade. The recent acquisition of CA Technologies by Broadcom brings about a major shift in the equation and raises some concerns on future of CA's security portfolio and the IAM product line. However, Broadcom has shown considerable interest and commitment towards CA's security portfolio in the early stages of integration.

CA Technologies offers CA Privileged Access Management Suite comprising of CA Privileged Access Manager, CA Privileged Access Manager Server Control and CA Threat Analytics – all integrated in one platform with flexible licensing options. Once a market leader in PAM, CA Technologies made significant investments in consolidating its legendry privileged access management product with capabilities added from the acquisition of Xceedium Xsuite under a common platform suite. Built upon one of the oldest and trustworthy Privileged Access Management products in the market (CA Access Control), CA PAM Suite leverages substantial install base, direct sales team and a strong channel partner network across geographies to cut across market competition and position itself as a leading PAM provider.

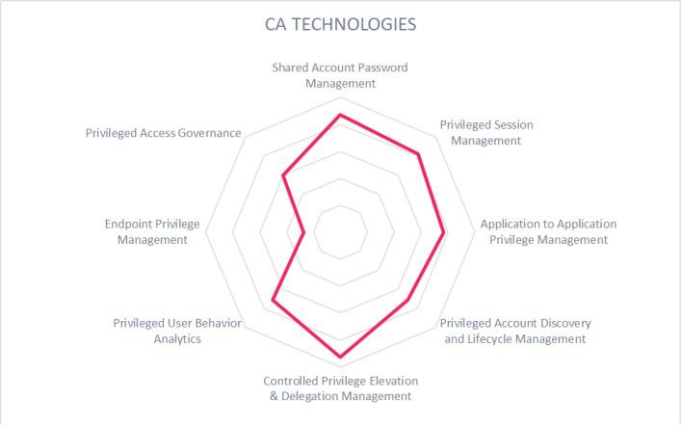
Strengths	Challenges
• Supports a broad range of target IT systems • Full support for AAPM • Support for virtualized and Cloud environments • Fine grained command control • Support for both host and proxy-based approaches to PAM • Unix AD authentication bridging for extending AD policies to Unix systems • Strong partner ecosystem	• Support for DevOps is present but is in early developmental stages • CPEDM is extensive but expensive • Threat Analytics lacks support for customization • Lack of targeted communication from Broadcom adds to uncertainty on Broadcom's continued investment in CA's security portfolio • Lack of focus on mid-market segments

Table 7: CA Technologies' major strengths and challenges

CA Privileged Access Manager provides a simple-to-deploy solution for privileged access management in physical, virtual and cloud environments that offers combined SAPM, AAPM and PSM capabilities in one solution. CA Threat Analytics delivers advanced threat analytics leveraging machine learning techniques for automated detection of risky privileged behavior. The CA PAM Server Control offers an agent-based architecture to intercept control and restrict commands at OS Kernel level enabling a fine-grained command control and privilege elevation while enabling authentication of UNIX and Linux users using AD and Kerberos credentials for Unix-AD bridging.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 8: CA Technologies' rating



As a natural fit for most medium to large-sized organizations with complex PAM requirements, CA PAM provides native integration with CA IAM suite to offer additional value. Existing CA customers should ask for more clarity in the product roadmap plans post CA's acquisition by Broadcom.

5.4 Centrify Corporation

Based in the US, Centrify offers Centrify Zero Trust Privilege Services (formerly Centrify Infrastructure Services) as its comprehensive privileged access management solution that offers the full suite of PAM capabilities as well as secure remote access capabilities. Privileged Access Service is Centrify's SAPM solution that leverages its access management capabilities. Centrify offers in-built adaptive MFA and brokered authentication for privileged access. Deployment options include as a SaaS model, from the AWS Marketplace, deployed in the cloud, and on-premises/customer managed. CPEDM is available with just in time privileged access via built-in workflows or available through integration with 3rd parties such as ServiceNow and SailPoint Technologies. Its PSM includes auditing and monitoring at both the host and gateway levels, adaptive MFA for privileged access and privileged analytics.

Strengths	Challenges
• Deep AD integration supporting complex multi-domain/ forest configurations • Strong MFA and identity federation support with risk adaptive capabilities • Mature PAM as a Service offering in addition to a managed, on-premises delivery • Strong privileged analytics with advanced machine learning techniques • Suitability for hybrid and containerized IT environments • A well-functioning marketing machinery with strong messaging for Zero Trust approach	• Lack of comprehensive Endpoint Privilege Management capabilities for desktops • Pricing is on the higher side of the spectrum • A growing but relatively limited partner ecosystem • Strong focus on US as primary market has constrained growth in EMEA and Asia markets

Table 9: Centrify's major strengths and challenges

Centrify Privileged Access Service provides password vaulting, offering SAPM, secure administrative access via a distributed local jump box and secure remote access for privileged users to target systems. Centrify Authentication Service offers adaptive MFA and identity consolidation in addition to Unix-AD bridging. Centrify Privilege Elevation Service delivers delegated privilege role and policy management, time-based role assignment and built-in MFA at privilege elevation. Centrify Privilege Threat Analytics Service leverages machine learning techniques to provide threat analytics and enforces access policies based on user behavior.

Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 10: Centrify's rating

Centrify Audit and Monitoring Service provides detailed monitoring and auditing capabilities at both shell and process levels and supports both host and proxy-based deployments. Centrify appeals to organizations looking for an integrated identity federation, deep AD integration, strong MFA support and mobile access management for privileged access.

5.5 CyberArk

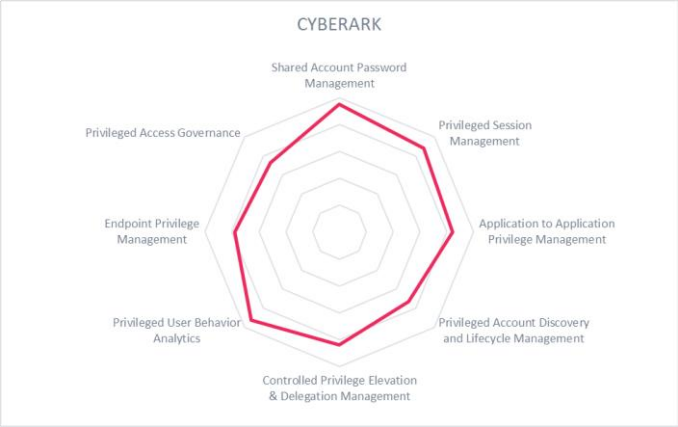
Headquartered in Israel and the US, CyberArk, has established itself as a leader in the Privileged Access Management market for a long time now. Originated in Israel in 1999, CyberArk has solely focused on securing privileged access across an organization's IT environment through continued growth and innovation. CyberArk offers its Core Privileged Access Security Solution as a fully integrated suite comprising of several modules, namely, Credential Management (formerly, Enterprise Password Vault), Session Management (formerly, Privileged Session Manager), Threat Analytics (formerly, Privileged Threat Analytics), and On-Demand Privileges Manager for privileged elevation. Its DevOps and Apps Secrets Management solution consists of Conjur and Application Identity Manager (AIM) as the AAPM component. CyberArk Endpoint Privilege Manager (EPM) is a separate but integrable product targeted at Endpoint Privilege Management capabilities.

Strengths	Challenges
• Broad target platform support • Easy integration of own and 3rd party components • 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 • Convenient and re-purposed pricing structure • A strong and functional partner ecosystem	• High modularity of solution could be unfavorable for certain deployments • Justifying solution complexity for simpler PAM deployments can be daunting • A lack of focus on small and mid-market segments • Market expectations to move fast and maximize shareholder value while operating within permissible risk margin creates additional pressure

Table 11: CyberArk's major strengths and challenges

Built to offer required flexibility, scalability and high availability, most CyberArk components can be installed on hardware, VMs, in AWS, Azure or Google Cloud.

CyberArk Conjur, available in both enterprise and open source versions, provides secrets management across native cloud, DevOps, containerized and other dynamic environments enabling developers to secure and manage secrets used by users, applications, microservices, containers, APIs etc. throughout the DevOps pipeline to expedite and streamline application deployments. Offered as a virtual appliance, CyberArk Privileged Threat Analytics is another matured offering aimed at detecting user anomalies and risky activities and integrates with its Privileged Session Management capabilities and Endpoint Privilege Manager for threat detection and alerting.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 12: CyberArk's rating

CyberArk remains the vendor of choice for global organizations seeking a comprehensive, market leading PAM solution for complex PAM requirements.

5.6 EmpowerID

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

Strengths	Challenges
• PAM, as a new addition, completes the IAM portfolio, integrating well into a broader IAM suite • Integrated support for workflow and policy management deliver strong PAG • Leading-edge adaptive authentication support	• Runs primarily on Windows platform, • Lack of advanced AAPM and privilege elevation capabilities • Endpoint Privilege Management (EPM) is absent • Limited search capabilities for graphical sessions • A small but selective partner ecosystem mostly concentrated across Europe

Table 13: EmpowerID's major strengths and challenges

Delivering baseline capabilities for shared account password management (SAPM) through a secured encrypted password vault and privileged session management (PSM) across SSH, RDP and web-based SSO sessions used for accessing privileged systems in organizations, EmpowerID's PAM product completes its IAM portfolio and benefits the customers of its existing IAM products that require basic PAM features to manage privileged access.

While EmpowerID PAM supports checkout of credentials from the password vault through APIs and a native PowerShell module, other advanced application to application password management (AAPM) capabilities aren't supported. EmpowerID offers a EmpowerID PAM also lacks privilege elevation and endpoint privilege management (EPM) capabilities. While session playback, search and common reporting capabilities are available, privileged user behavior analytics isn't yet supported.

Security	positive
Functionality	neutral
Integration	strong positive
Interoperability	positive
Usability	positive

Table 14: EmpowerID's rating

EmpowerID PAM is included at no additional cost for managing EmpowerID infrastructure but additional licenses are required to extend it to rest of the IT environment. Integration with its adaptive authentication and workflow management capabilities from its Identity Governance product offer stronger privileged user authentication and privileged access governance capabilities for its customers. With policy and workflow management for privileged access that is available as part of EmpowerID's integrated IAM solution makes EmpowerID a vendor of choice for Microsoft technology centric organizations looking for a good baseline support for SAPM and PSM capabilities with stronger privileged access governance (PAG).

5.7 FUDO Security

Based in California, FUDO Security, previously Wheel Systems, offers FUDO PAM as its primary PAM product in the market. FUDO also offers FUDO Session Recorder as a separate product targeted at remote session monitoring. FUDO Security has a substantial install base across Europe and Middle East with expansion plans in North America and Asia regions.

Strengths	Challenges
• Supports a broad range of target systems • Strong PSM & SRM capabilities • Support for multi tenancy and HA • Use of behavioral biometrics for enhanced privileged analytics • Appliance based delivery offers faster deployment and configuration	• Limited AAPM capabilities • CPEDM and EPM are absent • Weak marketing machinery • Lack of support for cloud platforms and DevOps • Limited partnerships and interoperability with 3rd party security tools • Limited partner ecosystem and presence outside of EMEA

Table 15: FUDO Security's major strengths and challenges

Offered in Virtual and hardware appliance formats, additional licenses are available for HA and VM options. Supporting a wide array of target systems for shared account password management (SAPM), FUDO PAM offers strong privileged session management (PSM) and session recording & monitoring (SRM) capabilities. With available provisions for dual control and session delegation, FUDO security offers own MFA solution and OAuth integration with 3rd party authentication providers, such as Yubikey. FUDO PAM's strength lies in its strong session recording features that include full bit-by-bit, protocol-level session recording including mouse movements, sub sessions, file transfers, USB access, sound, hidden windows content and full OCR translation of sessions.

Operating an agent-less approach, FUDO PAM offers fast deployment and initial configuration. FUDO's HA architecture supports multi-master, multi node HA configuration and is suitable for geographically distributed deployments. While FUDO offers great SRM capabilities, there's scope for better privileged analytics that can support business decisions. FUDO also lacks integration and interoperability with 3rd party security solutions such as IGA and UEBA tools for privileged access governance and behavioral analytics.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 16: FUDO Security's rating

With basic AAPM capabilities, FUDO doesn't offer CPEDM and desktop EPM capabilities. Organizations looking for a regional integration support and faster deployment with common password management and some strong Session Recording and Monitoring capabilities should consider FUDO PAM.

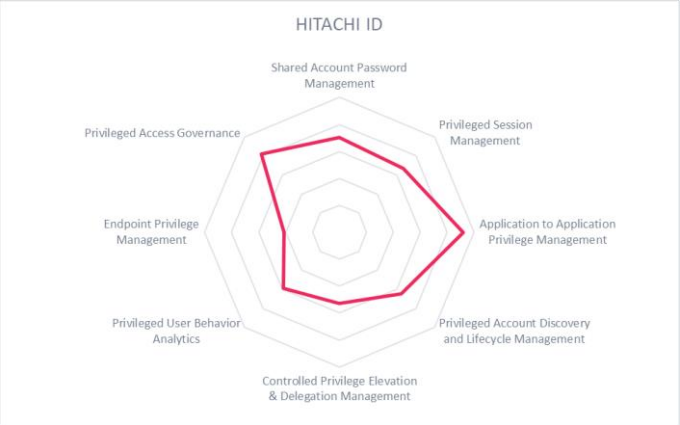
5.8 Hitachi ID

Hitachi ID, headquartered in Canada, is a global IAM software provider that originated as MTech Information Technology and was acquired by Hitachi in 2008. It offers Hitachi ID Privileged Access Manager as its primary offering aimed at the PAM market. With robust SAPM capabilities, Hitachi ID Privileged Access Manager is a broader PAM product featuring most enterprise-grade PAM functions. Its ease of deployment combined with suitability for lean privileged operations makes it a strong contender to several leading vendors in the market.

Strengths	Challenges
• Strong contextual support for API/ service authentication • An active-active architecture supporting High Availability • Built-in 2FA for authentication • Session recording is included at no additional cost • Detailed account discovery and provisioning support • Mobile support for access request management • Access certification capability of Hitachi ID Identity Manager is included at no additional cost	• Limited CPEDM capabilities • No EPM module • Lack of an effective sales and marketing machinery • OOB connectors for cloud applications are limited but growing • Limited partner ecosystem impacts market outreach and growth

Table 17: Hitachi ID's major strengths and challenges

The solution supports an exhaustive list of target systems covering both physical and virtual targets. Privilege elevation is based on temporary security group membership and SSH trust injection instead of command line or shell substitution approach. The Identity Express: Privileged Access edition incorporates business rules and policies built around Privileged Access Manager to simplify control over access to privileged accounts and security groups across a variety of systems, thereby standardizing PAM deployments across multiple customers. Most relevant IAM capabilities are included out of the box in Hitachi ID Privileged Access Manager, including discovery, access certification, SoD detection and policy enforcement along with request and approval of group membership in directory objects supporting real-time surveillance of AD groups to detect and reverse unauthorized out-of-band changes.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 18: Hitachi ID's rating

Overall Hitachi ID offers good support for hybrid IT environments and offers SaaS delivery for PAM including connectors for most commonplace cloud applications and platforms. With recent product enhancements, Hitachi ID has emerged as a promising PAM vendor and should be included in vendor evaluation processes by organizations with critical SAPM, PSM and PAG requirements.

5.9 I-Sprint

Singapore based I-Sprint is an access management vendor that offers AccessMatrix Universal Credential Manager as its PAM product. With substantial presence in Asia, particularly South East Asia (SEA) and China, I-Sprint caters mostly to Asian businesses and offers great understanding of regional business processes that deviate significantly from global standards.

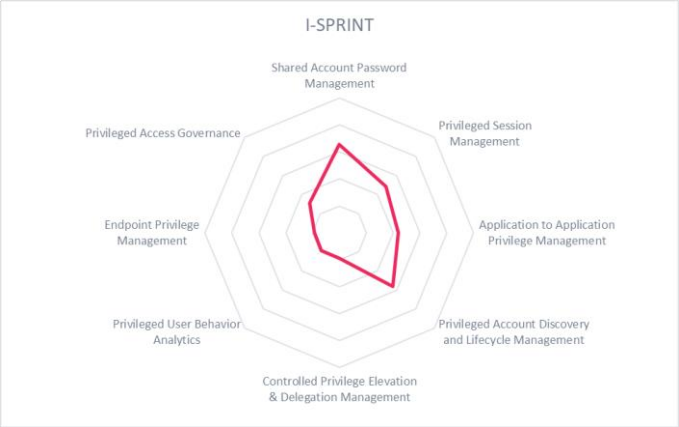
Strengths	Challenges
• Ease of deployment and initial configuration • Strong authentication support from UAS • HSM integration offers strong encryption and supports high assurance use-cases • Good understanding of regional PAM requirements • Supports PAM related regulations in the region	• Still maturing, lacks several PAM functions • Marketing is regionally aligned and ineffective • Regional focus limits international outreach and confines market growth • Though growing, partner ecosystem is small and regional

Table 19: I-Sprint's major strengths and challenges

Universal Credential Manager (UCM) provides a virtual password safe with strong encryption using HSM devices to store privileged accounts and credentials. I-Sprint Privileged Session Manager (PSM) provides add-on Windows RDP Gateway Recorder and a set of network protocol proxy modules to monitor and record privileged sessions that supports video recording and session playback for forensic analysis. It also supports command access control for selected protocols.

Security	neutral
Functionality	positive
Integration	neutral
Interoperability	weak
Usability	positive

Table 20: I-Sprint's rating



UCM allows for privileged account discovery based on system configuration and creates corresponding records in UCM to be managed. UCM also offers programmatic checkout of passwords by applications using PKI certificate authentication. UCM benefits considerably from I-Sprint's flagship authentication product, Access Matrix Universal Authentication Manager by offering multiple authentication form factors and session management capabilities for privileged users and leveraging on the upsell sales opportunities it generates for UCM.

I-Sprint UCM continues to be an evolving product in the PAM market with basic provisions for account management, session recording and auditing. With an increasing connecter base and integrations for target systems, including SaaS apps, I-Sprint currently lacks certain PAM functionalities to be a complete PAM solution as of today. However, this might change sooner than expected as I-Sprint continues to invest in developing its UCM product to match up to the global standards.

Small and mid-size organizations with basic SAPM and PSM requirements with a need for regional integration support and process understanding should bring I-Sprint on their evaluation list of PAM vendors.

5.10 Krontech

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

Single Connect Dynamic Password Controlled module provides a secure password vault offering in an agentless fashion for SAPM and AAPM functions. Session Manager provides PSM functions and supports most session types with session recording, playback and dual control. The MFA Manager offers Single Sign-on (SSO) and MFA for privileged users across target systems and supports SMS and Soft OTP methods in addition to OOB Mobile Push authentication.

Strengths	Challenges
• Separate modules for distinct PAM functions, integrated under a common PAM platform • Good market and technology understanding • Good UI design for enhanced UX • Strong support for database administrative privileges • Early and effective emphasis on privileged task automation • Support for limited but most commonplace IaaS platforms	• CPEDM, EPM, PUBA and PAG functions are absent • Marketing messaging is fragmented and tends to be overpromising • Limited sales channels and partner ecosystem • Brand awareness remains weak with limited customer references • Relatively new entrant in an established market

Table 21: Krontech's major strengths and challenges

Access Directory Manager provides in-built TACACS+ and RADIUS protocol support for controlling access to network devices via SSH and Telnet sessions. Single Connect Data Access Manager is the module targeted at privileged database access and enables activity monitoring for privileged database sessions. This allows for managing DB admins roles and assigned DB privileges with granular command control and dynamic data masking. Single Connect Privileged Task Automation (PTA) Manager is targeted primarily at Telecom service providers and allows for better operational efficiency by delegating tasks instead of privileges and automating routine privileged operations.

Security	neutral
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 22: Krontech's rating

While it doesn't offer PAM-as-a-Service, the Single Connect Cloud PAM module extends Single Connect PAM features to AWS, Azure and Google Cloud platforms. With basic SAPM and PSM capabilities, Krontech Single Connect appeals to small and mid-size businesses (SMBs) with a need for routine task elimination by privileged task automation, thereby accelerating leaner privileged operations. It should equally appeal to organizations with a need for heightened database activity monitoring and dynamic data masking based on database privileges.

5.11 ManageEngine

Headquartered in Pleasanton, US, ManageEngine is a part of India-based Zoho Corporation that was founded in 1996. ManageEngine's PAM product, Password Manager Pro was launched in 2007 and is one of the most popular PAM products in the SMB market segment for its value proposition. Operating mostly out of Chennai (India), ManageEngine has one of the largest customer bases in the PAM market by number. However, the corresponding deal sizes stand within the lower quartile.

Strengths	Challenges
• Supports wide range of target systems including hypervisors • Strong auto discovery capabilities • Bundled middleware and database components • Integrates seamlessly within broader security and IT infrastructure management software portfolio • Reasonable pricing and easy licensing arrangement • A large and functional partner ecosystem	• Lack of CPEDM, PUBA and PAG functions • Only available in an on-prem software delivery format • Lack of integration with IGA tools • Focused on SMB marketplace • Lack of connector support for cloud applications and cloud-based delivery

Table 23: ManageEngine's major strengths and challenges

Password Manager Pro offers support for a multitude of target platforms including hypervisors, legacy systems and infrastructure components. Available in software and virtual appliance formats, Password Manager Pro (PMP) comes bundled with Apache Tomcat and RDBMS, with the option to choose from MS SQL Server or MySQL as backend RDBMS. PMP is also listed in Amazon Web Services and Microsoft Azure marketplaces to enable deployment in Amazon EC2 and Azure virtual machines respectively.

Built-in high availability, database replication and disaster recovery features position PMP as an enterprise grade product. With a reasonable user-based pricing, all PAM features are available as part of the base product install and could be turned on or off depending on the license purchased. The product integrates with any LDAP compliant directory service (including AD) for user management and authentication and integrates OOB with most authentication providers.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 24: ManageEngine's rating

The remote login feature allows administrators to launch emulated RDP, SSH, VNC and SQL sessions from a user browser without the need of any installed plug-ins or endpoint agents. The sessions are tunneled through the PMP server and the recordings are kept for playback and forensic review purposes. PMP integrates OOB with ManageEngine's EventLog Analyzer (SIEM) and ServiceDesk Plus (ITSM) products, in addition to other third party SIEM and ITSM tools. A lack of integration with IGA tools, however, leads to a lack of PAG capabilities.

With a large customer base and strong partner ecosystem, ManageEngine PMP primarily appeals to organizations that have invested in ManageEngine security and IT management portfolio and seek better business value for a given price.

5.12 Micro Focus

UK based Micro Focus offers Micro Focus Privileged Account Manager as its primary PAM product that derives its origin from Novell and later NetIQ codebase. Micro Focus had been executing on a comprehensive product roadmap during the time of its merger with Hewlett Packard Enterprise (HPE). Effects of Micro Focus's acquisition by Hewlett Packard Enterprise (HPE), however, yet to be confirmed, are believed to preserve the ongoing efforts of a major product upheaving for its Identity and Access Management portfolio, backed by strong development and professional services experience from HPE.

Strengths	Challenges
• A comprehensive set of PAM features • Session management support for business applications and databases • Scalable and flexible solution architecture • Risk-based analytics support for PSM • A large customer base and strong partner ecosystem, further strengthened by HPE's acquisition	• A lack of advanced AAPM capabilities • Endpoint Privilege Management (EPM) capabilities are absent • Complexity of deployment and configuration • Recent acquisition by HPE creates uncertainties in its long-standing market position • Relatively weaker marketing messaging and execution

Table 25: Micro Focus' major strengths and challenges

Formerly, NetIQ Privileged User Manager (PUM), Micro Focus Privileged Account Manager offers a comprehensive PAM portfolio with some advanced PSM and risk analytics capabilities. Offering an enterprise password vault for shared account password management (SAPM), it offers a framework manager for controlled privilege elevation on Unix/ Linux systems. With a lack of support for advanced application to application password management (AAPM) capabilities, Micro Focus Privileged Account Manager offers detailed keystroke logging and video session recording for privileged user connections. Offering a gateway approach, it supports privileged session management across a variety of systems including enterprise business applications such as SAP, databases and popular SaaS applications. Recent product advances to support risk-based analytics of privileged activity is of interest to some customers.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 26: Micro Focus' rating

From an architectural perspective, Micro Focus is executing on a roadmap to move from a purely host-based approach towards a mix of proxy and host-based architecture, which allows for deeper integrations on certain target systems while other capabilities such as the password vaulting etc. are run and managed centrally. Overall, Micro Focus' Privileged Account Manager is a good PAM product with a good set of PAM features that you would expect from an established vendor in the market. Having made some significant investment and efforts in the recent past to revive its IAM product portfolio, Micro Focus had been slower in reposing to fast emerging IAM requirements of its prevailing customers and the market in general. Micro Focus PAM appeals to organizations that have an existing install base of popular NetIQ Identity and Access Managers to offer close integrations for better privileged access control and overall governance.

5.13 MT4 Networks

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

Strengths	Challenges
• A comprehensive PAM offering covering most PAM areas • Supports a wide range of target systems, especially network devices • An operationally efficient UI • Flexibility to develop connectors for legacy systems • Highly modular but well-integrated components	• Lack of international languages and processes support • Inconsistent and weak marketing messaging • Lack of risk-based analytics • Limited CPEDM capabilities • Lack of Privileged Access Governance features • Small vendor with limited global footprint and a small partner ecosystem

Table 27: MT4 Networks' major strengths and challenges

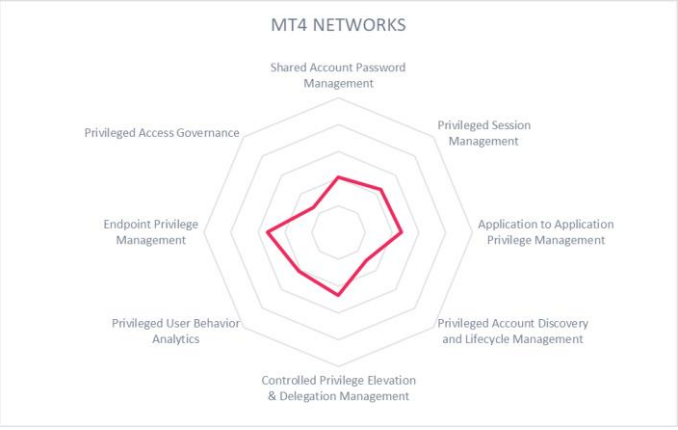
Offering a functional module for almost every PAM function in the market, Senhasegura has a broad feature-set but might lack the depth of capabilities in some areas including accounts on-boarding, risk-based analytics, endpoint privilege management and privileged access governance. However, in comparison to most new market entrants, Senhasegura offers a rather comprehensive PAM product.

Senhasegura has introduced several new modules, especially senhasegura Threat Analysis and Behavior Analysis modules since our last evaluation of the product but there's lack of sufficient customer references to attest to the technical and functional maturity of these modules. In addition to all basic PAM modules for account and password management, Senhasegura offers SSH Key Management, accounts discovery, AAPM and an endpoint MFA module.

An agentless architecture allows for easy installation and configuration while preserving administrator UX. A set of infrastructure modules offer high availability, load balancing and advanced monitoring capabilities.

Security	positive
Functionality	strong positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 28: MT4 Networks' rating



Offering an enterprise-level PAM product that is evolving and competitive, Senhasegura aims to expand beyond Brazil into Latin American, European and Middle Eastern markets. Senhasegura makes a logical choice of PAM vendor for organizations of all sizes in South America with requirements of regional integration and language support. Senhasegura should consider adding better support for other languages and building an effective partner ecosystem to enter global markets.

5.14 One Identity

California-based One Identity, a Quest Software Business, offers a good range of products aimed at managing and securing privileged access for organizations. Once a very popular PAM and IGA technology, Quest lost considerable market interest and share under Dell's ownership until its spin-off in 2016. Since then, Quest has made significant investment in product marketing, development as well as innovation to catch up with the market and in some cases clearly exceeded the market expectations.

Strengths	Challenges
• Strong feature set for both Unix/Linux and Windows environments • Based on established, industry popular technology • Unix-AD bridging and privilege account management across hybrid AD environments • Global presence and strong partner ecosystem • Integration with One Identity Manager and other One Identity products	• Limited customization possibilities particularly for Privileged Password Manager • Limited support for cloud applications and infrastructure • Increasing yet limited DevOps support

Table 29: One Identity's major strengths and challenges

Aimed at managing and securing most PAM use-cases in enterprises, One Identity's PAM portfolio includes One Identity Safeguard, Privileged Access Suite for Unix, Active Roles and Privilege Manager for Windows.

Delivered as hardware appliance, Safeguard for Privileged Passwords (SPP) is the vault component offering SAPM. Safeguard for Privileged Analytics (SPA) comes bundled with the PSM component, Safeguard for Privileged Sessions (SPS) in virtual or hardware appliance formats to analyze privileged activities and detect anomalies.

Available in installable client package, Privileged Access Suite (PAS) for Unix is a comprehensive suite delivering Unix-AD bridging, authentication, root delegation, sudo enhancement and a centralized management of policies across unix-based systems. Privilege Manager for Windows offers CPEDM capabilities for Windows-based platforms. Another key product, Active Roles, provides privileged account management in a hybrid AD environment.

While password vaulting and session management products are well integrated and available under one administrative console, integration with CPEDM products is on One Identity's future roadmap.

Security	positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 30: One Identity's rating

One Identity has delivered on the proposed product roadmap that included some major milestones targeted at product enhancement, and with a strong execution, we expect it to succeed in the longer term with a clearer progression path for existing and new customers.

5.15 Osirium

Based in UK, Osirium offers PxM platform that builds upon several products delivering privileged access management capabilities. This includes PAM (Privileged Account Management), PSM (Privileged Session Management), PTA (Privileged Task Automation) and PBM (Privileged Behavior Management) products in addition to a MAP server. Osirium takes a distinctive approach to PAM by alienating passwords from users and associating them with user roles instead. Besides the agentless approach, Osirium's strength lies in the task-based execution of privileges which is operationally more efficient, especially for routine administration tasks.

Strengths	Challenges
• Task-based approach allows for better security, operational efficiency and reduced error rates • Gateway approach provides the flexibility to extend PAM to a variety of target systems, particularly ICS environments • Good support for Privileged Behavior Analytics	• Lack of conventional AAPM and CPEDM capabilities • EPM is absent • Unsuitability of task-based approach for dynamic or fluid IT environments • Limited global footprint and lack of a global partner ecosystem

Table 31: Osirium's major strengths and challenges

Osirium's Privileged Access Management product delivers baseline support for managing passwords of shared accounts and enforcing least privilege access. The Privileged Session Management product provides necessary capabilities for monitoring and recording of privileged sessions across both command line and graphical sessions. Privileged Task Management is the component within Osirium PxM platform which differentiates Osirium from its competitors by delivering a task-based approach for privileged activities. While this approach could be operationally efficient in mature IT environments, it finds limited relevance in dynamic or fluid IT environments where pre-defining administrative activities can be difficult.

Osirium's task-based approach can eliminate the need for CPEDM through packaging of elevated privileges in a pre-defined task and allowing for task delegation. With a range of in-built templates for pre-configured tasks and a broad protocol support, tasks can be executed against variety of devices and management interfaces. Osirium's 'gateway' approach can be particularly suitable for supporting PAM requirements if legacy and ICS (Industrial Control System) environments.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 32: Osirium's rating

Osirium offers a promising alternative to the conventional vaulting technology in the PAM market and aims to provide value to organizations that find themselves ready for such an approach. With a small customer base that is concentrated primarily in the UK and a smaller partner ecosystem, Osirium presents a good fit for ICS/ IIoT focused organizations.

5.16 Sectona

Founded in 2017, Mumbai (India) based Sectona is the youngest of PAM market entrants and offers Spectra Privileged Access Management as its PAM product. Sectona is funded by its initial founders and has raised angel investments to support its ongoing operations. With an experienced management, Sectona brings a collaborative, cross-platform approach to PAM that is aimed at realizing business value through enterprise integrations.

Strengths	Challenges
• A relatively young start-up with experienced management • Smaller size allows to respond faster to customer demands and customizations • A collaborative, cross-platform approach allows for integrations offering desired flexibility • Good understanding of regional PAM requirements and customer sentiments • Few but good selection of partners	• Though offering a distinct approach, is late to enter an established market segment • A growing but limited PAM feature set • Functionally limited to PSM with lack of proven AAPM, CPEDM and privilege analytics capabilities • Presence is limited mostly to Asia with a handful of customers in Middle East and North America

Table 33: Sectona's major strengths and challenges

Spectra offers an in-built Plugin Designer Kit (PDK) that allows customers to develop own connectors to facilitate PSM and SAPM for non-standard applications and does not require extensive coding experience thereby avoiding development costs. Spectra's strength is the PSM technology that offers access to privileged sessions over any HTML5 supported browser from any platform without the need of agents or plugins to be installed. This includes SSH and RDP sessions, in addition to support for thick-client apps through virtualization using jump-hosts. Sectona Push for Desktop and Mobile provides notifications of high-risk activities in real-time and offers control of session over PCs and mobile devices.

Security	neutral
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 34: Sectona's rating

Spectra PAM also offers a discovery module across virtual and cloud infrastructure platforms including VMWare, AWS and Azure for accounts discovery. Spectra offers a collaboration module that helps reduce dependence on third party screen sharing utilities for purposes of sharing critical privileged sessions with internal or external users. Eliminating the need for a plugin, screen sharing and collaboration through Spectra works over a single secure port and records the entire session.

Spectra lacks detailed CPEDM, EPM or privilege analytics capabilities to be a complete PAM platform. However, with early support for privileged task automation and easy integrations with several ITSM and SIEM platforms, Sectona's Spectra makes a good choice of vendor for small to mid-size organizations seeking secure remote access and PSM capabilities with support for leaner privileged operations and regional integration. Sectona also offers an MSP edition of Spectra aimed at IT service providers to offer managed PAM services.

5.17 SSH.COM

Based in Helsinki, Finland, SSH.COM offers PrivX as its primary product in the PAM market. PrivX is a relatively new offering in the market by SSH.COM that attempts to offer an alternative to conventional shared account password management technology by providing a certificate authority for SSH and RDP access. PrivX acts as a certificate authority for SSH and RDP clients by issuing short-lived certificates for on-demand access. While the approach eliminates the need for password vaulting for specific SSH and RDP access, it doesn't address the basic shared account password management use-cases such as password vaulting or password rotation. PrivX also doesn't offer any session management capabilities such as session auditing, recording or monitoring of privileged user activities.

Strengths	Challenges
• A unique but limited-in-scope approach for managing SSH and RDP access with good session monitoring features • Global presence with a strong partner ecosystem	• Lacks basic PAM features such as shared account password management and privilege elevation • Though detailed, functionality remains limited to management of SSH keys and session monitoring • Lack of focus on innovation has limited its growth in recent years • Lacks support for advanced PAM capabilities such as Privileged Behavior Analytics Relatively • Limited support for windows systems including RDP sessions such as session indexing and activity search

Table 35: SSH.COM's major strengths and challenges

PrivX claims to offer on-demand role-based access provisioning through ephemeral certificates and can be designed to work with AD, LDAP and other third-party directories via OpenID Connect in addition to its own directory which is rarely used. Able to manage access to hosts in on-premises and cloud environments, PrivX offers a consolidated view of target resources across the hybrid environment to manage access and audit user activity. Its account management capabilities remain limited to SSH and RDP access and don't offer password vaulting for system or application accounts. Universal SSH Key Manager offers lifecycle management for SSH keys that include discovery, provisioning, rotation and decommission of keys across the IT endpoints. While CryptoAuditor offers detailed session monitoring and filtering at protocol level, several PSM capabilities such as dual control or session delegation aren't supported.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	neutral

Table 36: SSH.COM's rating

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

5.18 Thycotic

Based in Washington D.C. (US), Thycotic offers Secret Server platform as its primary PAM offering in the market. Secret Server is known for its comprehensiveness, ease of deployment and configuration that can reduce product deployment and upgrade cycles substantially. Thycotic's recent partnership with IBM has accelerated Thycotic's market expansion through IBM's large customer base, strong presence and regional ties alongside a strong global sales and marketing team. While this partnership can bring cross-sell opportunities for both Thycotic and IBM, a deeper technological integration of Secret Server with IBM cloud platform is yet to bring desired value for existing customers.

Strengths	Challenges
• Support for a wide range of target systems • Simple and efficient UI • Support for mobile access • Strong support for AAPM • Partnership with IBM expands sales and market outreach • Ease of deployment and configuration • Cloud-ready, a mature PAMaaS in operation • Easy customization and support for Microsoft platform	• Built on .NET framework, runs primarily on Microsoft stack

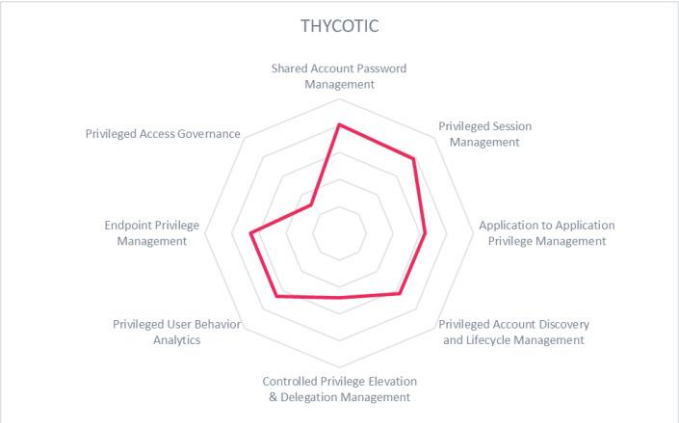
Table 37: Thycotic's major strengths and challenges

Thycotic with its early release of PAMaaS platform Secret Server Cloud and acquisition of Arellia to offer Windows EPM has recorded tremendous growth over the last several years. An aggressive and effective use of sales and marketing channels has contributed considerably to its impressive growth rate.

Besides support for most common PAM features, Thycotic Secret Server offers support for a wide range of target systems and an extensive set of APIs to Secret Server for customization. Privilege Manager is Thycotic's agent-based EPM solution for Windows and Mac endpoints that supports extensive EPM capabilities including application control and privilege elevation. Thycotic Privilege Behavious Analytics solution monitors user activities across Secret Server deployments and can alert upon detection of anomalies based on an alert threshold.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 38: Thycotic's rating



Thycotic with an impressive range of OOB integrations and support for cloud infrastructure and DevOps processes appeals to organizations of all sizes globally looking for a comprehensive and effective PAM solution with faster deployment cycles and easy configuration and are internally more aligned to Microsoft technology stack.

5.19 WALLIX

Based in France, WALLIX provides WALLIX Bastion as its primary PAM product in the market. At the core of Bastion is password management, session management and access management with built-in access request and approval capabilities. WALLIX has a large install base across Europe and Middle East with very limited presence in North America and Asia regions.

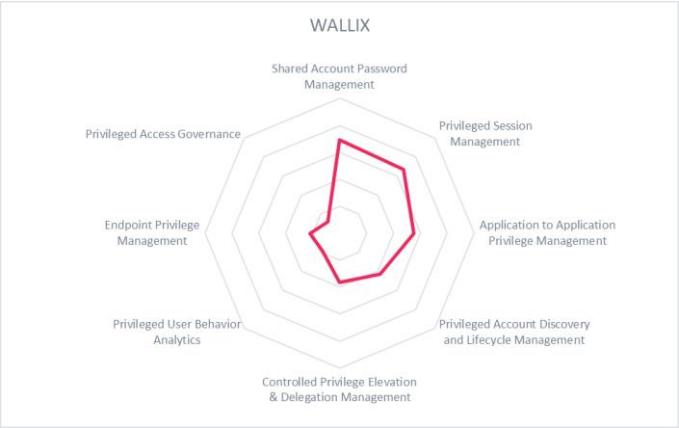
Strengths	Challenges
• Supports a broad range of target systems • Leading PSM capabilities • Web access gateway and a single administrative console for all Bastion instances • Support for multi tenancy and HA • Strong execution on a well-thought-out product roadmap	• No EPM module • Limited CPEDM and privileged analytics capabilities • Lack of support for cloud platforms and DevOps • Limited partnerships and interoperability with 3rd party security tools • Limited partner ecosystem and presence outside of EMEA

Table 39: WALLIX' major strengths and challenges

Operating a proxy-based approach, Bastion acts as a web access gateway providing protocol access and high-availability capabilities. Additional jump servers can be configured easily to scale Bastion up for new target systems. Supporting multi-tenancy, Bastion is available in most delivery formats with several MSSPs offering a managed hosted PAM service. WALLIX Bastion provides strong encryption and advanced session management features without interfering with administrative UX.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 40: WALLIX' rating



Bastion AAPM uses fingerprinting of the process calling the service or application to secure credential checkouts from the Bastion vault. Bastion offers limited CPEDM with superuser credential injection but no sudo or shell replacement.

WALLIX doesn't offer desktop EPM capabilities. Integration with other security tools including IGA for privileged access governance is limited and doesn't offer necessary interoperability. WALLIX currently lacks privileged analytics but has plans to introduce it later in 2019. WALLIX has made significant progress over the last few years by executing on a well-laid innovative product roadmap, positioning it in the product leader's section in this LC. WALLIX has clearly made its way from a remote session management technology provider to a full-fledged PAM solution provider in an already established market. Organizations with common SAPM and AAPM needs with strong encryption and PSM requirements should consider WALLIX Bastion on their shortlist.

6 Vendors to watch

Besides the vendors covered in detail in this Leadership Compass document, we observe some other vendors that offer notable Privileged Access Management capabilities in the market. A few of these vendors have decided not to participate in this KuppingerCole Leadership Compass for own reasons, but since we find them interesting and worth a mention, we decided to include them here. These vendors either do not fully fit into the market segment of PAM due to their differentiated approach to PAM or do not meet the required eligibility criteria at this point of time to be considered in our Leadership Compass evaluation. We provide short abstracts for these vendors below.

6.1 Deep Identity

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

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

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

6.2 Devolutions

Canada based Devolutions offers Devolutions Password Server as its primary PAM product that provides password vaulting and password management targeted at business users as well as IT administrators. Available in an on-premises deployment format, Devolutions Privileged Account Management platform offers role-based access for users to connect to target systems through the Password Server as the common entry point. Web-based credentials are synchronized, stored and traced using Devolutions Web Login browser extension that is available for most commonplace web browsers allowing users to launch targeted websites from the Devolutions web console without having to manage own credentials.

Devolutions Launcher provides credentials injection via the Password Server to launch remote sessions over a variety of connection protocols through the admin interface. An integration with Remote Desktop Manager offers privileged session management across remote RDP connections and integrates with a variety of VPN connection providers for seamless connection to remote target systems.

With its Password Safe, Devolutions offers a baseline shared account password management solution focused on ease-of-use and remote support management use-cases. Organizations looking for entry-level SAPM capabilities with requirements for secure remote access should consider Devolutions on their shortlist.

6.3 HashiCorp

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

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

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

6.4 HelpSystems

Based in Minnesota (US), HelpSystems is a provider of security solutions targeted at IBM i-Series infrastructure. Its PowerTech portfolio is aimed at access control and session monitoring of privileged users for IBM i series and Unix/ Linux systems. PowerTech offers a complete PAM solution with separately licensed modules for password management, MFA, session recording and monitoring and privilege elevation. PowerTech Authority Broker offers controlled privilege elevation for IBM i systems and provides detailed auditing and logging of administrative activities. HelpSystems acquired California based Fox Technologies that offered BoKS Server Control as its flagship Unix/ Linux access control product. Now PowerTech Identity and Access Manager, it brings shared account password management and privilege elevation capabilities for Unix and Linux systems to the PowerTech portfolio.

HelpSystems doesn't provide privilege elevation or endpoint management capabilities for Windows platform. With one of the very few products that offer support for IBM i series, HelpSystem's PowerTech portfolio appeals to organizations that have a need to manage mainframe privileges and demand centralized administration across IBM i series and Unix/ Linux systems in a hybrid IT environment.

6.5 IdentityAutomation

Houston (US) based IdentityAutomation 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. Acquisition of Healthcast, a provider of access management solution targeted at healthcare

industry brings IdentityAutomation the required connectors for specialized healthcare systems along with the domain expertise. RapidIdentity PAM appeals to organizations, particularly in healthcare industry, with a need for an integrated PAM solution that offers password management, MFA and basic auditing and reporting of privileged activities.

6.6 Iraje

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

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

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

6.7 MasterSAM

Singapore based MasterSAM, a part of Silverlake group, offers several separately licensed products aimed at managing privileged access. MasterSAM Star Gate offers a proxy-based approach to shared account password management (SAPM) and application to application password management (AAPM) with built-in SSO and 2FA capabilities. MasterSAM's Secure @Windows and Secure @ Unix/Linux products offer a host-based approach to controlled privilege elevation and delegation (CPEDM) for Windows and Unix/Linux platforms, whereas Frontline product delivers recording and monitoring for windows desktop environment. MasterSAM Analyst product provides centralized logging, auditing and review capabilities for privileged activities. Lacking advanced AAPM capabilities, MasterSAM with a completer and more mature PAM portfolio offers a competitive cost-to-value proposition against several established market leaders globally. Malaysia based Firmus Security is the largest integration partner offering integration and managed hosted services for MasterSAM PAM in the region.

Offering one of the most reasonable pricing options in the market, MasterSAM appeals to APAC based organizations looking for regional integration support and deployment flexibility offering proxy-based, host-based or a hybrid approach.

6.8 NRI Secure Technologies

Japan based NRI Secure Technologies offers SecureCube Access Check primarily providing Privileged Session Management (PSM) capabilities. Operating in a gateway-based approach, SecureCube Access Check extends BeyondTrust Powerbroker Password Safe for password management. NTT Software Corporation builds its iDoperation PAM solution based on Access Check to offer session recording, monitoring and review capabilities. Supporting approval request workflows with role-based access control policies, Access Check

offers a distinct approach aimed at access control of privileged users. Access Check lacks Application to Application Password Management (AAPM) capabilities but supports command filtering and detailed session monitoring and alerting capabilities. SecureCube Access Check also provides access control and monitoring of file transfers and database sessions to Oracle RDBMS.

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

6.9 ObserveIT

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

With visual endpoint recording, ObserveIT can capture sessions across a variety of systems, supporting all major protocols such as RDP (Remote Desktop Protocol) including the citrix variants, SSH, Telnet and direct logins to application consoles. An agent-based approach allows for detailed logging and therefore more meaningful and efficient activity search in contrast to other similar solutions that are primarily proxy or gateway-based. ObserveIT with a well-established global partner ecosystem is a vendor of choice for organizations that either have critical PSM requirements only or are looking to complement their existing PAM deployments with stronger PSM capabilities.

6.10 OnionID

US based OnionID takes a differentiated approach to privileged access management by offering multiple delivery options including PAM-as-a-Service, on-prem or cloud hosted service. Offering ready templates and access request workflows for password management across multiple web and SaaS applications through a common administrative console differentiates OnionID's approach to PAM. Operating in an agentless fashion, Onion ID provides a layering of basic PAM controls starting with brokering of native or 3rd party authentication over existing privileged access methods and delivering real-time command filtering and control over established privileged sessions.

In addition to providing support for DevOps initiatives by providing out-of-the-box integration with most DevOps tools, OnionID provides SSH key management and privileged behavior analytics based on both endpoint and user attributes. OnionID lacks application to application password management (AAPM) as well as controlled privilege elevation and delegation capabilities (CPEDM) but supports basic command filtering. With a range of native integrations for SaaS, IaaS and social media platforms, OnionID is an interesting PAM as a service alternative to few established vendors who are in the process of rolling out cloud delivered PAM services. With a small customer base limited to North America, OnionID appeals to organizations that require rapid deployment of a lightweight privileged session management solution that extends existing

authentication technology and offers ready authorization workflows for managing privileged access to popular cloud applications and platforms.

6.11 Oracle

Based in California, Oracle is a popular and well-established software giant that offers Oracle Privileged Account Manager (OPAM) as its PAM product in the market targeted primarily at Oracle middleware and technology stack. Offering advanced integrations for managing privileged accounts across the range of Oracle fusion middleware products and Oracle's PaaS infrastructure, OPAM is the preferred PAM option for organizations with considerable Oracle technology presence. OPAM provides integration with Oracle's IAM portfolio including Oracle Identity Governance (OIG) that extends account provisioning, role-based administrative access and access review workflows to privileged access management.

There has been a lack of attention to the OPAM's product development roadmap from Oracle for some time which needs to be addressed. OPAM's license is most often included as part of larger product deals at no additional cost by Oracle but remains frequently undeployed by customers due to the associated deployment complexity, a lack of certain essential PAM features including privilege elevation and integration with non-Oracle products. The significant presence of Oracle's technology infrastructure globally, combined with its industry-leading sales and a strong partner ecosystem makes OPAM more of a necessity than choice for many Oracle customers worldwide, which however, is changing as many PAM vendors offer easy integration with Oracle technology.

6.12 Remediant

Remediant is a new market entrant that takes an entirely distinctive zero-trust approach to PAM. Remediant offers SecureONE as its agentless and vaultless PAM product that aims to solve the privileged access challenges by granting privileged access on a just-in-time and just-enough (least privilege) basis thereby eliminating the need of sharing passwords. Aligning with a zero-trust security approach, SecureONE reduces the attack surface to a considerable extent by limiting the privileged access to approved systems only and incorporating 2FA in the process for establishing additional trust.

SecureONE offers integration with SIEM solutions to enable detection of privileged escalations and identification of potential risks. While Remediant takes a distinct approach to PAM, it's not entirely unique and resembles to what few vendors like Osirium have been exercising in the PAM market to create a niche.

While SecureONE offers a replacement for common shared account password management, it lacks controlled privilege elevation and endpoint privilege management capabilities.

Organizations looking for a rapid PAM deployment and find themselves ready for a vaultless PAM approach, should consider StepONE - Remediant's trial version of SecureONE for piloting purposes to help demonstrate product's capabilities during vendor PoC stages.

6.13 Saviynt

California (US) based Saviynt is one of the leading providers of cloud based IGA services and makes its entry in the PAM market with a unique vault less approach to PAM. Saviynt PAM uses Hashicorp vault as the password vault. Currently supporting SSH and RDP connections to most commonplace IaaS platforms, a new connection request spins up a transient docker container in the Saviynt cloud to render the target connection

with access authorizations derived from the defined user's role. The privileged activities in the container are key-stroke logged and available for search and analysis through AWS Elastic Search.

With its distinctive and industry-first approach to privileged session management (PSM) technology, Saviynt delivers just-in-time and just-for-use privileged access to target applications. While the solution is still in its early development phases, we expect it to leverage upon Saviynt's expertise in cloud delivery and therefore recommend cloud-ready organizations and existing Saviynt customers to evaluate this approach for future consideration.

6.14 SecureLink

Based in Austin, Texas (US), SecureLink is a provider of secure remote access solutions as a PSM product targeted at managing privileges for third party vendors' access. Offered primarily as a service, SecureLink's service comes in two independent variants - SecureLink for Enterprises and SecureLink for Vendors.

SecureLink for Enterprises aims at managing third-party remote access while offering controls for managing access privileges for external vendor technicians and system administrators with detailed logging and auditing of outsourced operations. The other service variant, SecureLink for Vendors, is aimed at providing efficient remote support for customers by automating routine administration tasks and offering task-based privileges. Both services require SecureLink's gateway as a lightweight software plugin to be installed for enabling technology vendor's remote access.

SecureLink makes a good choice of PSM technology for organizations seeking PSM as a service for controlling third-party remote access with high-definition auditing controls for required visibility into outsourced privileged operations.

6.15 Venafi

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

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

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

6.16 XTON Technologies

Based in US, XTON Technologies is another notable market entrant that offers Xton Access Manager targeted at the PAM requirements of mid-market segment. XTON offers Privileged Account Management and Server Access Control as productized solutions that require minimal resources to implement and maintain, thereby favoring leaner PAM operations. Its agentless account management product, XTAM, provides web-based password vault and offers accounts discovery, shared account password management and privileged session management capabilities including password rotation, access request workflows and session and keystroke recording with playback. While XTON doesn't provide controlled privilege elevation and delegation management (CPEDM) capabilities, it offers support for elevated script automation for routine privilege escalation tasks, enhancing administrator efficiency.

For a new market entrant, XTON offers a considerably wider PAM technology portfolio that aligns well with the market direction and supports emerging PAM requirements of organizations. XTAM offering integrations with ITSM, SIEM and MFA providers, 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.

7 Methodology

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.

7.2 Types of Leadership

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

- 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 category, we evaluate products across three segments:

- 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 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 inputs and experience in a given market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, technical

forums, product documentations and a detailed questionnaire response submitted by vendors before creating the KuppingerCole Leadership Compass are amongst the primary information sources.

7.3 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 evaluation 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 characteristics 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 IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). 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. Also, if products use different databases or different administration tools with inconsistent user and administrative experience, they are not well integrated. On the other hand, if a single name and password can allow the administrator to deal with all aspects of the product suite, then a better level of integration is considered to have been achieved.

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

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 insure 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. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability —usability 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 that the vendor represents is of great importance. This is because lack of excellence in some or all these areas will inevitably lead identity and security failures.

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

7.4 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 over all 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.

7.5 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.

7.6 Spider graphs

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

Shared Account Password Management (SAPM)	Capabilities for managing shared account passwords, password rotation, providing single sign-on access to privileged accounts, and related capabilities.
Privileged Session Management (PSM)	Capabilities for establishing a privileged session to target systems including basic auditing and monitoring of privileged activities, offering authentication, authorization and Single Sign-On (SSO) to the target systems.
Application to Application Privilege Management (AAPM)	Capabilities for managing accounts used by an applications or systems to communicate with other applications or systems (such as databases etc.), offering identification and elimination of hardcoded credentials in application code, scripts and other configuration files by offering a replacement mechanism (generally APIs) to make credentials securely available.
Session Recording and Monitoring (SRM)	Capabilities to offer advanced auditing, monitoring and review of privileged activities during a privileged session, including but not limited to key-stroke logging, video session recording, screen scraping, OCR translation and other session monitoring techniques.
Privileged User Behavior Analytics (PUBA)	Capabilities to offer data analytic techniques to detect threats based on anomalous behavior against established behavioral profiles of administrative users as well as user groups and administrator roles

Privilege Account Discovery and Lifecycle Management (PADLM)	Capabilities to discover shared accounts, software accounts, service accounts and other unencrypted/ clear-text credentials across the IT infrastructure, offering integration into ITAM or CMDB tools for tracking account ownerships etc.
Endpoint Privilege Management (EPM)	Capabilities to offer management of privileged accounts on endpoints, including identification of such accounts, application whitelisting, controlled execution environment and other capabilities targeted at managing local administrative rights on desktop and mobile endpoints
Privileged Access Governance (PAG)	Capabilities to offer privileged access certifications and provisions for customizable reporting and dashboarding

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

7.7 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 about vendors not covered and their Privileged Access Management offerings in chapter 6, “Vendors and Market Segments to watch”. In that chapter, we also look at some other interesting offerings around the Privileged Access Management market and in related market segments.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports 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 Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstrasse 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com