KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | June 2017

Privilege Management

Leaders in innovation, product features, and market reach for Privilege Management. How do you control access to your critical systems and business information while allowing secure and optimised day to day business operations? This report provides an overview of the market for Privilege Management and provides you with a compass to help you to find the Privilege Management product that best meets your needs.

by **Martin Kuppinger**
mk@kuppingercole.com
June 2017

Leadership Compass
Privilege Management
By KuppingerCole

KuppingerCole Leadership Compass
Privilege Management
Report No.: **72330**

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

Executive View: Cloud Standards Cross Reference - 71124

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

Executive View: Executive View Microsoft Azure RMS - 70976

Executive View: PingFederate 7 - 70801

Executive View: Salesforce Platform as a Service – Security and Assurance - 70751

Executive View: Exostar Services for Life Sciences - 70878

Executive View: PingOne®- 70870

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

Scenario: Understanding Cloud Security - 70321

Scenario: Understanding Cloud Computing - 70157

Scenario: Understanding Identity and Access Management - 70129

Vendor Report: SecureAuth Corporation - 70260

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 solutions for Privilege Management. Privilege Management is among the most relevant areas of IAM (Identity and Access Management), but also tightly connected to Cyber Security, given that Privileged Users are a primary target of attackers.

1.1 Market Segment

With organizations embracing the cloud in conjunction the mobile evolution, ensuring the rigorous management of privileged users has become a business imperative. Where the exploits of a nation-state attack may read like a suspense novel, what goes unreported is the fact that even some of the most advanced attacks require privileged credentials, for example the username and password of a SAP administrator, to succeed. The media, too, tends to focus on external threat actors like nation-states or organized criminal gangs while ignoring the threat from the insider or, more importantly, the privileged insider. Let's not forget that Edward Snowden, of the USA, used or abused his privileged credentials to cause untold damage to national security. Simply put, even the most sophisticated attacker would find it almost impossible to succeed without having access to privileged credentials.

Managing privileged users or, as KuppingerCole refers to it, Privilege Management, is a significant undertaking for an organization. An insider is often more knowledgeable and aware of the business' process and technical landscape. And if an insider account gets hijacked, the outsider has the same opportunities for attacking. The malicious insider (or the hijacked one) with privileged credentials can cause significant damage including, but not limited to:

- Delete, modify or read all email and other communication records;
- View or modify salary records of all employees;
- Leak of intellectual property;
- Share confidential data, including personal information, with shareholders or hacktivists.

Privilege management is a complex collection of activities and tools that not only requires a robust policy and process framework but also requires technology that can support these policy requirements. In approaching the selection of products for the deployment of Privilege Management, important consideration must be given to the vendor's overall lifecycle management approach and the understanding of an organisation's own policy and process concerning identity management. In addition, there must be a particular focus on the ability to provision dynamic and granular access control (who can access what, when, and for how long), threat analytics and governance, and reporting capabilities. Furthermore, strong emphasis must be placed on the ability to scale as well as to integrate with both existing solutions and the overall security architecture.

Mature Privilege Management solutions go much further than simple password generation and access control to individual systems, but also provide a unified, robust and – importantly - transparent Privilege Management platform which is integrated into an organisation's overall Identity and Access Management (IAM) strategy. The information gathered during the deployment of a Privilege Management system and its communication to connected systems should further be used in the formation of an organization's overall Governance, Risk and Compliance (GRC) output.

The market for Privileged User Management products and Privileged Access Management products (usually referred to as PxM due to the fact that the categorizations of the products vary between vendors) has developed later in comparison with other sectors of IT security products.

The Privilege Management market has evolved significantly over the past several years, with new functionality being added. While "password vaults" had been at the center of attention in earlier years, capabilities such as advanced analytics of privileged user behavior and advanced capabilities in session monitoring and analysis are becoming the new normal, all integrated into comprehensive suites. However, we also see a growing number of vendors taking different approaches to solve the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts.

Furthermore, some vendors have started extending their scope to endpoint systems, in particular through application whitelisting, and/or in support of cloud environments.

Among security risks associated with privileged users are the following:

- Leakage of credentials for shared accounts
- Abuse of elevated privileges by fraudulent users
- Hijacking of privileged accounts by cyber-criminals
- Risks through abuse of elevated privileges on client systems
- Risks through mistakes in using elevated privileges by users

Furthermore, there are several areas of security, but also user convenience, requirements which are associated with privileged accounts:

- Managing the ownership and knowing all privileged accounts, both individual and shared accounts
- Single Sign-On to shared accounts for administrators and operators
- Reducing elevated privileges of administrators and, in particular, operators to mitigate associated risks
- Controls for managing, restricting, and monitoring access of MSPs when accessing internal systems
- Controls for managing, restricting, and monitoring access of internal users to cloud services

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

1.2 Required Capabilities

In this Leadership Compass, we are focusing on solutions that help organizations reduce the risks associated with privileged accounts, both individual and shared accounts. We refer to this market segment as Privilege Management. Products are variously titled as Privileged Account Management, Privileged Access Management, Privileged User Management, Privileged Identity Management, or in other forms. For brevity, we refer to the market as "PxM", with the x standing for the various terms used in vendor's marketing.

We look at all types of products that support customers in solving the Privilege 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 Privilege Management challenges. However, integration with such solutions is on the list of features we consider as being relevant in our analysis.

We are looking for features and functionalities in particular in the following areas:

- 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 Privilege Management
- Application Whitelisting on endpoints
- Reporting, Audit, and Compliance

We appreciate seeing integrated solutions with a tight integration of the various feature sets. Key features we expect to see in the various areas include, but are not limited to:

- Shared Account Password Management
  - Central management of shared account privileges
  - Automated credential rotation or OTPs
  - Secure 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 (Restriction)
  - Restricted access to managed systems
- Application-to-Application Privilege Management
  - Identification of hard-coded credentials in scripts, code, etc.
  - APIs for replacing such credentials
- Application Whitelisting on endpoints
  - Application whitelisting capabilities
- 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 aspects we expect to see in these products include

- Support for a broad range of target systems
- Support for cloud services and MSP access
- Support for various deployment scenarios
  - hardware appliances, SaaS, cloud deployments, …
  - local agents, network proxy, remote passive monitoring, …
- Scalability and performance impact
- 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, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

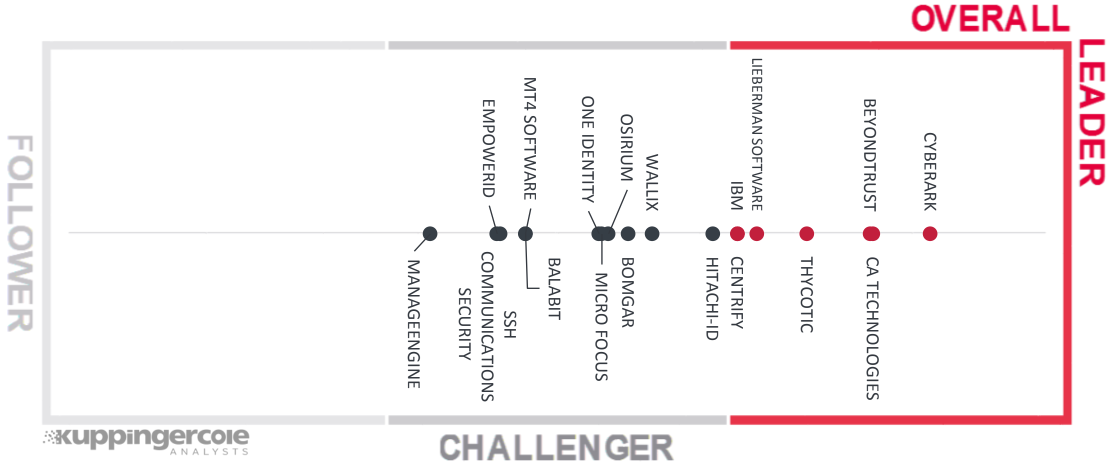


Figure 1: The Overall Leadership rating for the Privilege Management market segment

When looking at the Overall Leader segment in the Overall Leadership rating, we see a number of vendors, with the Challenger segment being very crowded. This is due to the fact that we took a broader view of Privilege Management capabilities than in earlier versions of the Leadership Compass for this market segment. We still see several vendors in the Leader's section, with CyberArk being in front, followed by CA Technologies and BeyondTrust. CA Technologies benefits from the integrated offering they now have, after the acquisition of Xceedium, while BeyondTrust is one of the established players in the market. Thycotic and Lieberman Software also made it into the Leader's segment, both being strong in Innovation Leadership and Product Leadership but less advanced in Market Leadership than the other players in this segment. Furthermore, IBM and Centrify just made it into the Overall Leader segment, with IBM benefiting from its market strength and Centrify from its innovativeness.

In the Challenger's section, we see Hitchi-ID being very close to entering the Leader's segment following themwe find Wallix and Bomgar, where Wallix is lacking global reach, while Bomgar takes a somewhat different approach to the Privilege Management market, based on their roots in the Remote Control market. Osirium is also close to that group, being a relatively young player that also differs slightly in the approach taken on Privilege Management, focusing on a task-oriented access control to privileged systems. Head-to-head to them, we see One Identity, which currently are in a phase of restructuring their Privilege Management product portfolio, and Micro Focus.

Other players in the segment include MT4 Software Studio as a Brazilian vendor, and, finally (in alphabetical order) Balabit, EmpowerID, ManageEngine, and SSH Communications Security. All three are specialized vendors, with Balabit being very strong in Session Management and Privileged Behaviour Analytics, but lacking Shared Account Password Management. EmpowerID does not provide the full breadth and depth other vendors provide, but the best integration into an overall IAM suite. ManageEngine, on the other hand, focuses more on entry-level use cases but can be a strong solution in that area. SSH Communications Security also is focused on specific aspects, as the name implies. While they offer far more than SSH security, this is still where they show their biggest strength.

There are no vendors in the Follower’s segment, since some of the point vendors in that market declined participation in this Leadership Compass.

Overall Leaders are (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- IBM
- Lieberman Software
- 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.

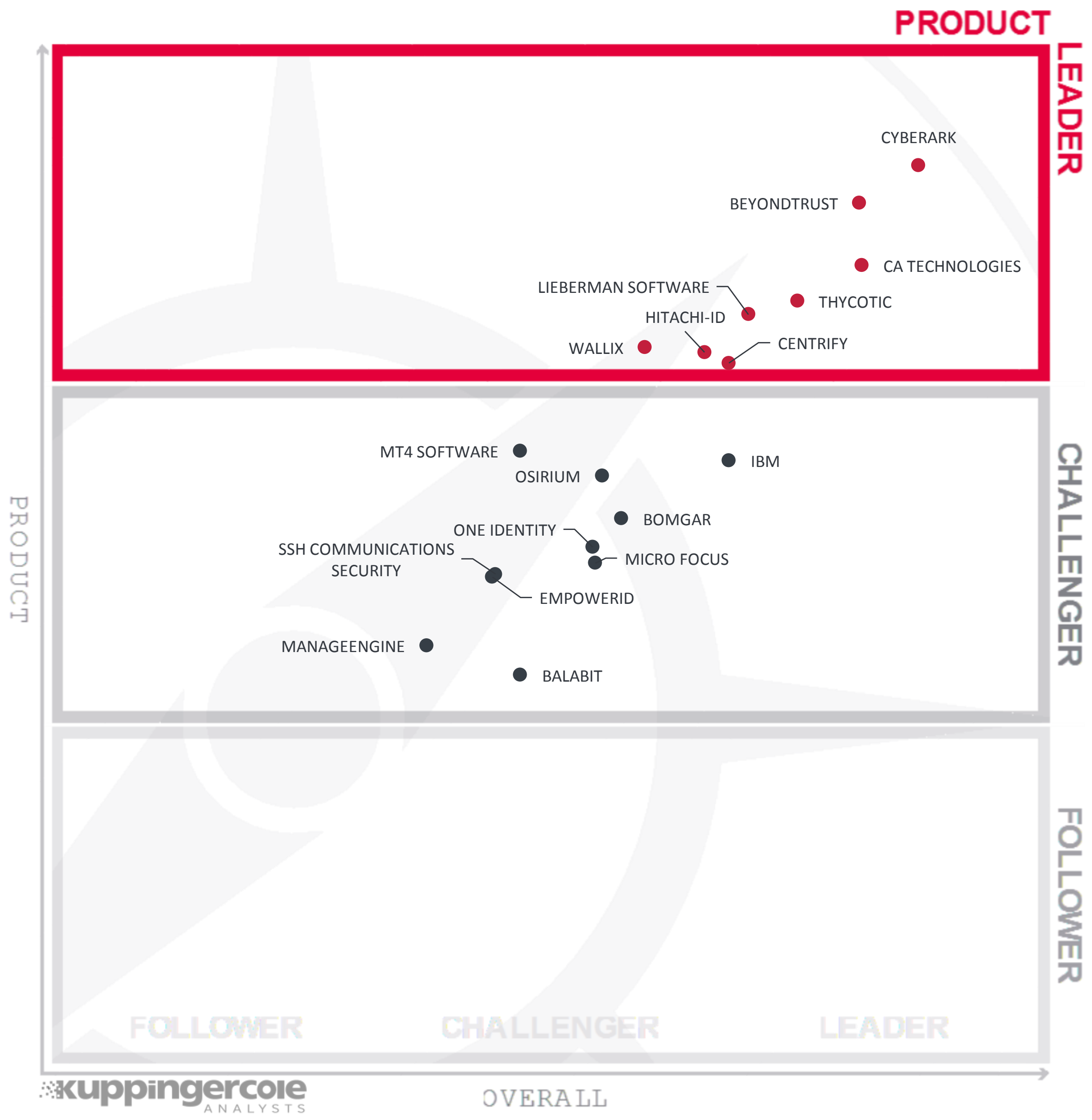


Figure 2: Product leaders in the Privilege Management market segment

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

Following these two leaders, we find CA Technologies, Thycotic, and Lieberman Software, which also deliver strong and functional comprehensive offerings to the market. Another vendor that made it into the Leader's segment is Wallix, a French company that evolved from a point vendor to a suite vendor and has become an interesting option to the leading vendors. Furthermore, we see Hitachi-ID and Centrify, which also made it into the Leader's segment.

IBM, MT4 Software Studio, and Osirium form the next group of vendors, all with strong offerings that might fit well the specific requirements of customers, followed by Bomgar. Bomgar has specific strengths, but also still shows some gaps in depth and breadth of supported functionality.

Further vendors in this segment include (in alphabetical order) Balabit EmpowerID, ManageEngine, Micro Focus, One Identity, and SSH Communications Security. Balabit and SSH Communications Security are rather specialized vendors that can be complementary to other vendor's offerings. Balabit, in particular, is among the leading vendors when it comes to Session Monitoring and Session Management capabilities, with their products frequently being deployed in conjunction with other vendor's offerings. Balabit even has partnerships with some of the other vendors in this Leadership Compass.

Product Leaders (in alphabetical order):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Hitachi-ID
- Lieberman Software
- 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.

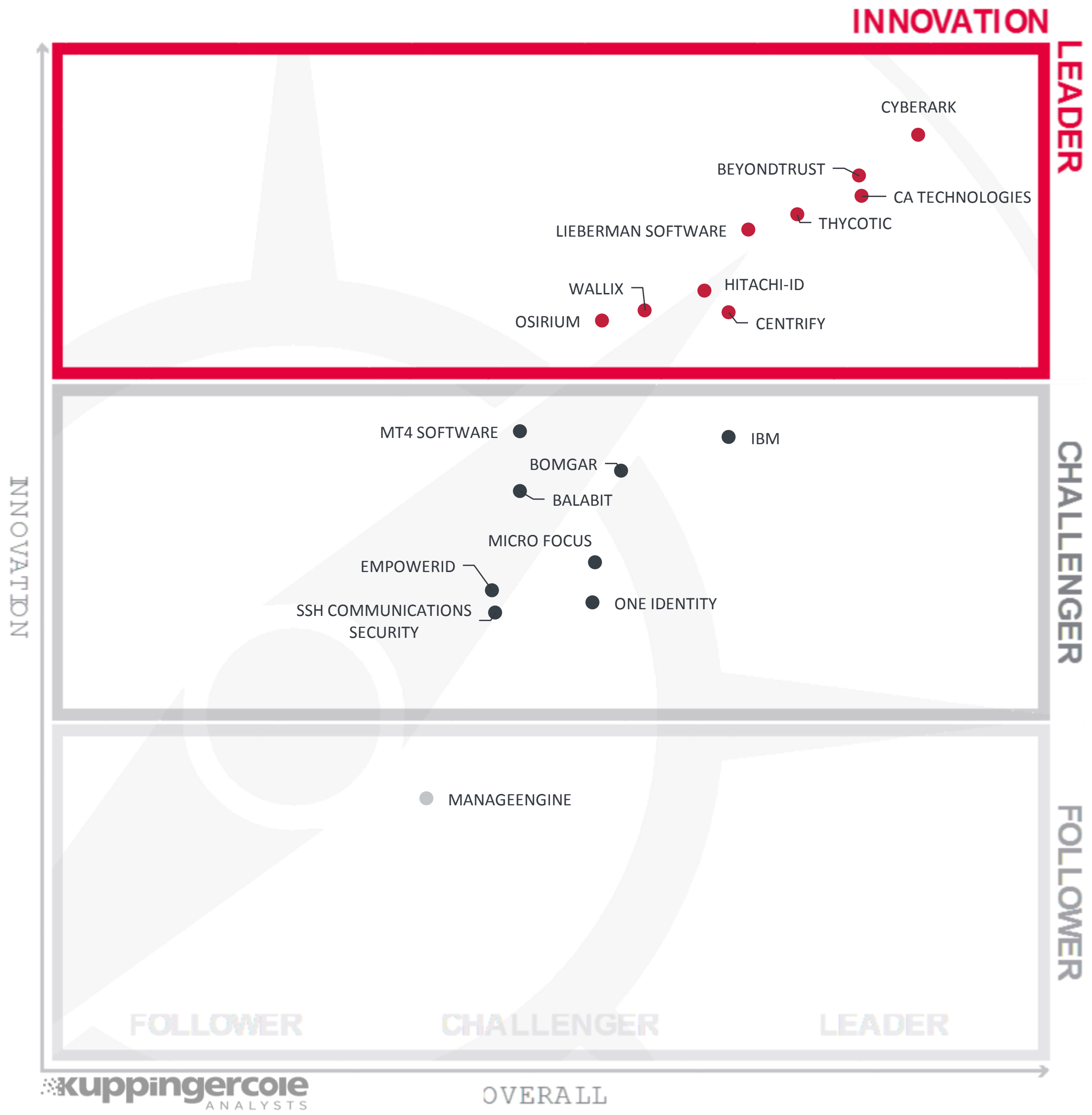


Figure 3: Innovation leaders in the Privilege Management market segment

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 front, due to the breadth of capabilities they are offering. Following them, we see (in alphabetical order) a group of vendors that are positioned well in the Innovation Leader's segment, including BeyondTrust, CA Technologies, Lieberman Software, and Thycotic.

Four other vendors made it into the Innovation Leader's segment. Here we find (again in alphabetical order) Centrify, Hitachi ID, Osirium, and Wallix. All are vendors that show a strong level of innovation, thus being definitely worth a deeper look when analyzing potential suppliers in the field of Privilege Management.

In the Challenger's section, we find (in alphabetical order) Balabit, Bomgar, IBM, and MT4 Software Studio being placed more towards the top. Micro Focus is following at some distance. One Identity is another vendor in this segment, and we again find Balabit and EmpowerID here. Balabit is, as mentioned beforehand, offering very strong capabilities in certain areas, but not covering the full breadth of Privilege Management capabilities. EmpowerID provides good baseline capabilities, but has its clear strength in providing Privilege Management in a unique integration with other IAM capabilities. SSH Communications Security also is a Challenger.

Finally, we see one vendors 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
- Lieberman Software
- Thycotic
- Osirium
- Wallix

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.

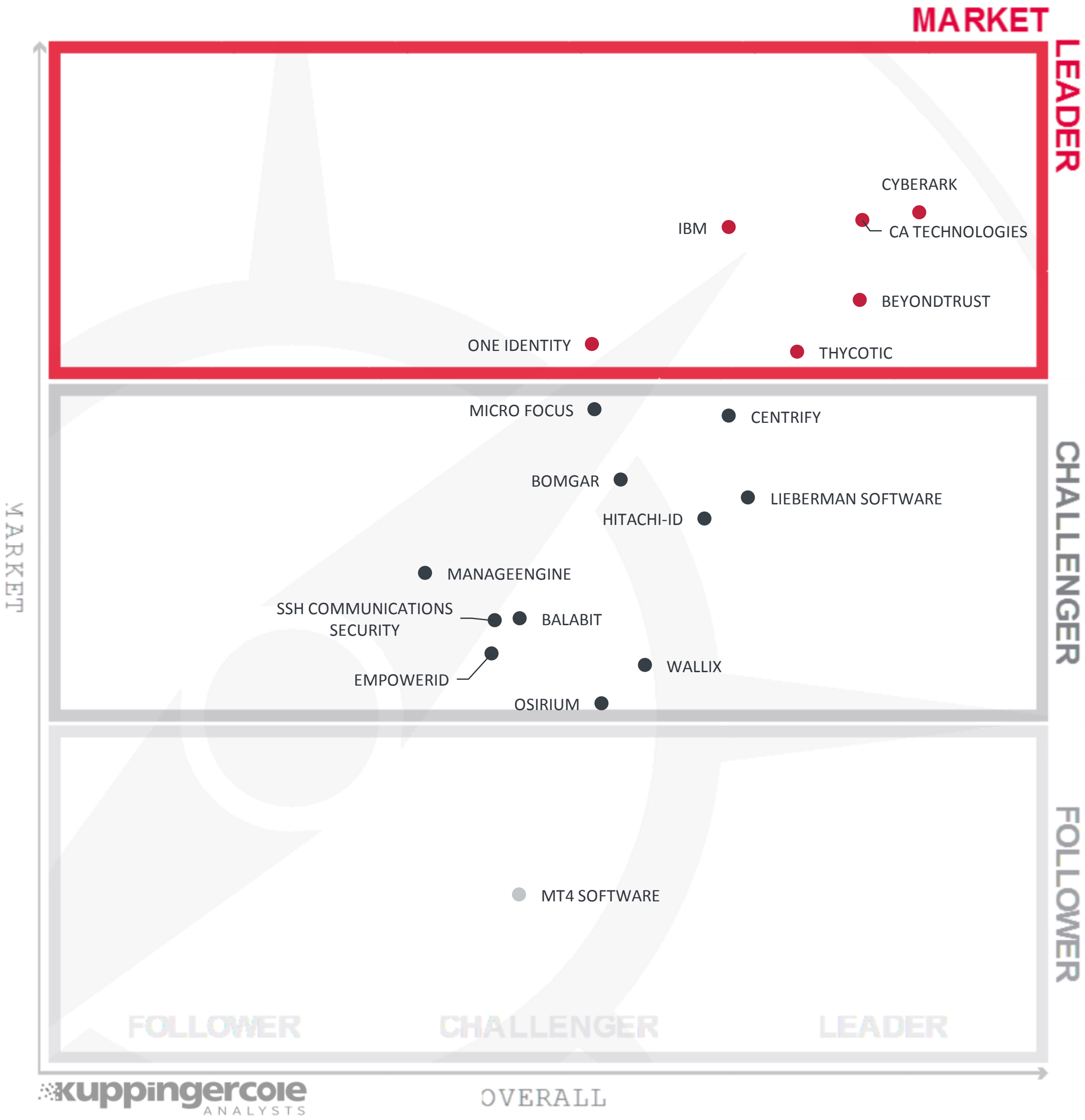


Figure 4: Market leaders in the Privilege Management market segment

Here, we find a group of three vendors leading the market. These include CyberArk as probably the most prominent vendor in the Privilege Management market segment, and CA Technologies plus IBM as two of the very large software companies that both have a very significant number of customers, a large partner ecosystem, and global reach. BeyondTrust also made it into the Leader's section. While having a very significant number of customers, their biggest strength is in the North American market, with relatively small partner ecosystems in other regions, compared to the other three vendors in this market segment. Thycotic and One Identity are two other vendors that just made it into this segment.

Micro Focus is close to entering the Leader's section, based on their global scale, particularly after the merger with HPE. Also, Centrify is close to entering the Leader's segment. Following them, we see a number of vendors at rather the same level, including (in alphabetical order) Bomgar, Hitachi ID, and Lieberman Software. Some of them, in particular Lieberman Software, suffer from the lack of a global partner ecosystem, while others are still not that large in the numbers of customers or the average size of deployments.

ManageEngine is following closely, with a very large number of customers, but a focus on smaller deployments. Balabit, EmpowerID, Osirium, SSH Communications Security, and Wallix (in alphabetical order) just made it into the Challenger's section. Balabit has a large number of customers and partners, but again is a very focused vendor. Wallix has its main market still in the French-speaking countries, while SSH Communications Security is still more of a a point vendor targeted at a certain set of capabilities. EmpowerID is a IAM suite vendor with good Privilege Management capabilities, while Osirium is still rather new in that market segment.

Finally, we see one vendor in the Follower's section, MT4 Software Studio from Brazil, which are currently mainly accessing the local market.

Market Leaders (in alphabetical order):

- BeyondTrust
- CA Technologies
- CyberArk
- IBM
- 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.

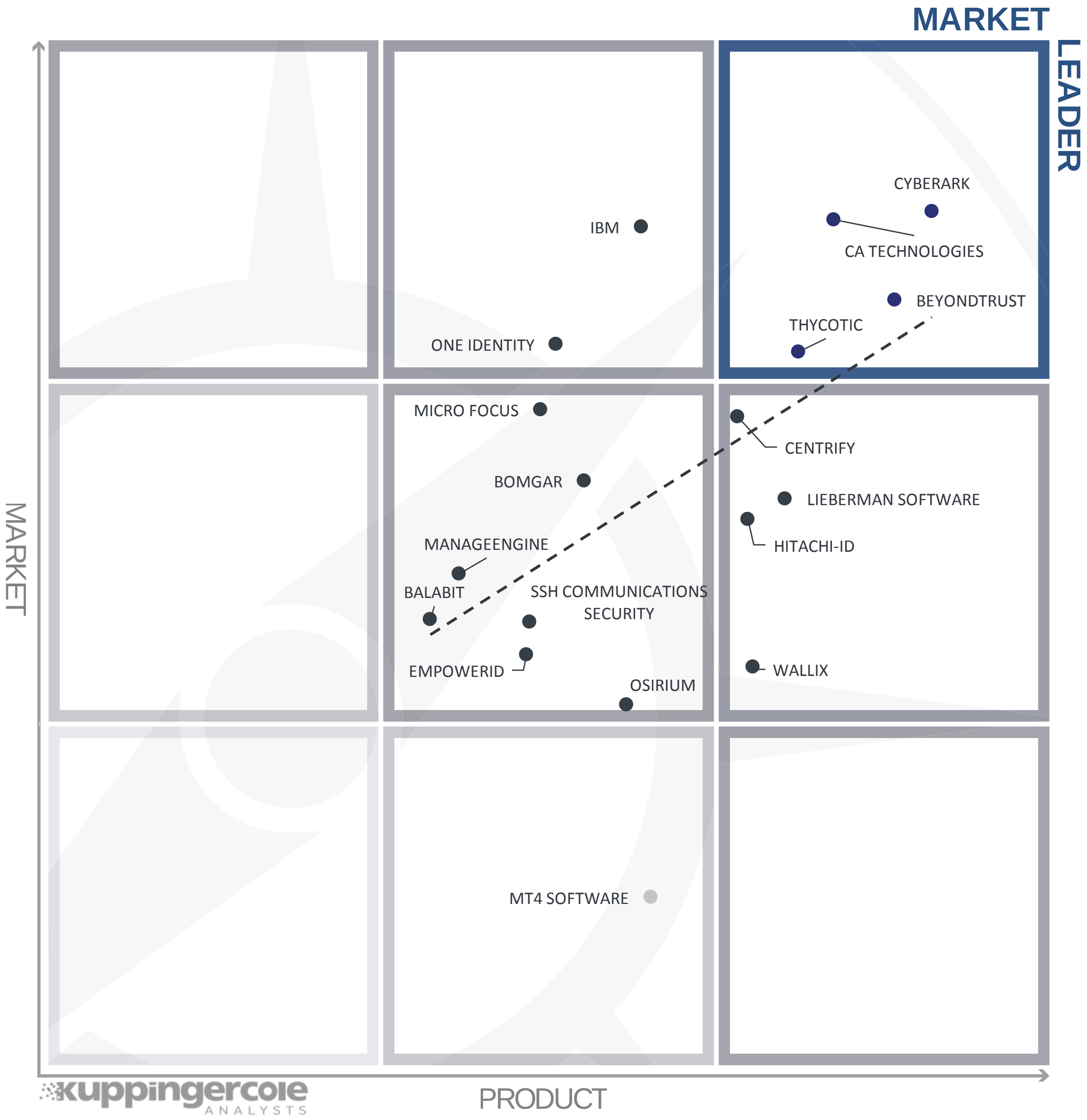


Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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, and Thycotic. These vendors are leading in both the product and market ratings.

Below these, we find (in alphabetical order) Centrify, Hitachi-ID, Lieberman Software, and Wallix, which all are product leaders but not (yet) in the Market Leader’s segment.

On the other hand, right to the Market Leader’s box, we see IBM and One Identity, both having a significant market share while not being counted amongst the Product Leaders.

In the center of the graphic, we find the biggest number of vendors, including (in alphabetical order) Balabit, Bomgar, EmpowerID, ManageEngine, Micro Focus, Osirium, and SSH Communications Security. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors.

Finally, we see MT4 Software towards the bottom, with their technically and feature-rich solution, but their limited market presence beyond their home market in Brazil.

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 is typical for most markets with a significant number of established vendors plus some smaller players.

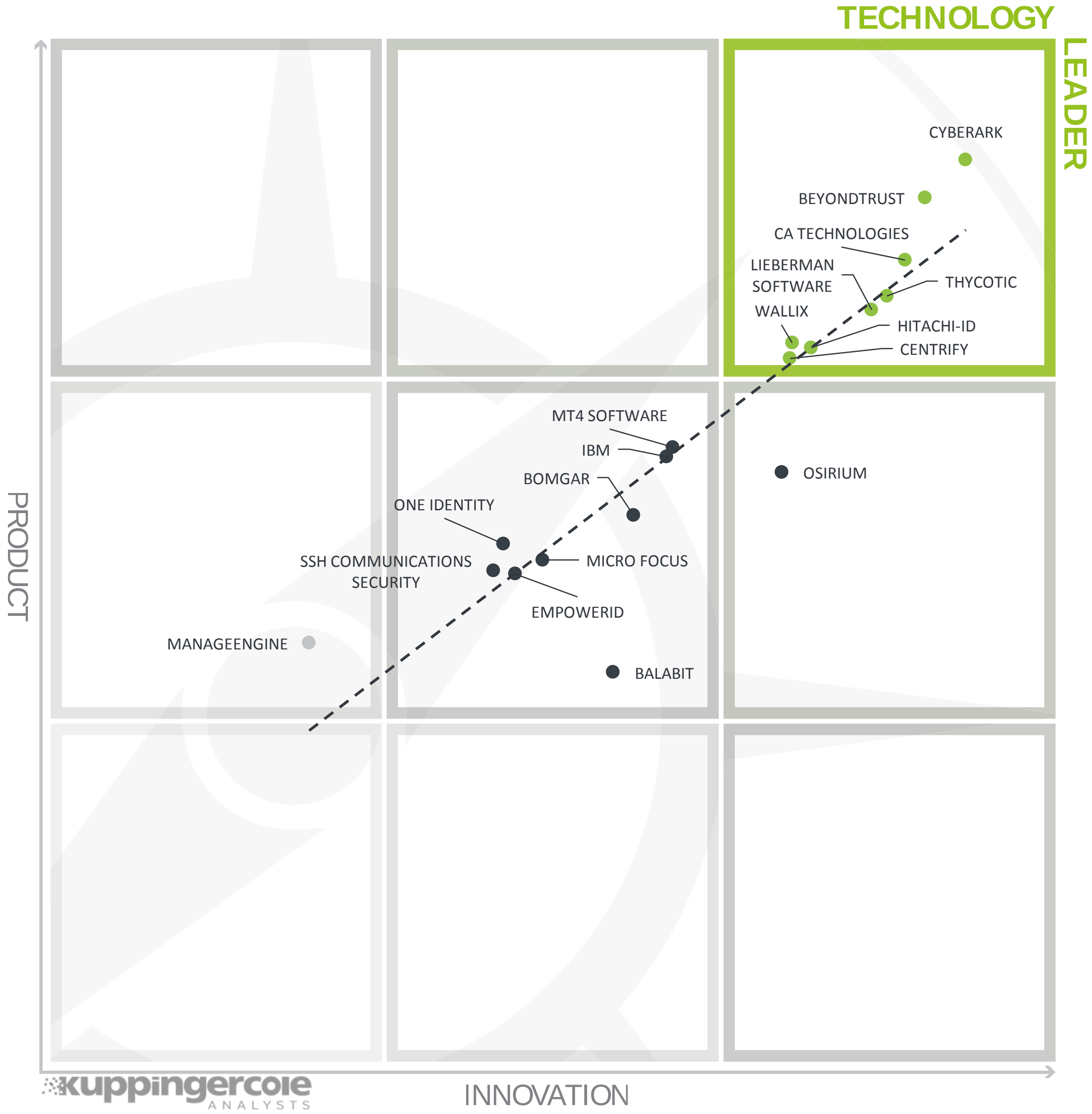


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

This chart shows a quite interesting picture. Most vendors are close to the standard curve showing a balanced ratio of product capabilities and innovation. Close to half of the vendors are placed in the Technology Leaders quadrant, with the overall leaders being more at the top and the others following.

In the upper right sector, we see CyberArk, BeyondTrust, CA Technologies, Thycotic, Lieberman Software, Hitachi-ID, Wallix, and Centrify, all providing offerings that deliver both a good number of innovative features and an overall comprehensive feature set.

Osirium is the only vendor below these, being innovative and taking a somewhat different path in solving some of the common Privilege Management challenges, but not yet supporting all feature areas we expect in Privilege Management.

In the middle segment, we find the Challengers, from both an innovation and product feature perspective. Here we find (in alphabetical order) Balabit, Bomgar, EmpowerID, IBM, Micro Focus, MT4 Software, One Identity, and SSH Communications Security.

Finally, there is ManageEngine, which provide a solution more targeted at SMEs, with a baseline feature set focused on Shared Account Password Management.

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.

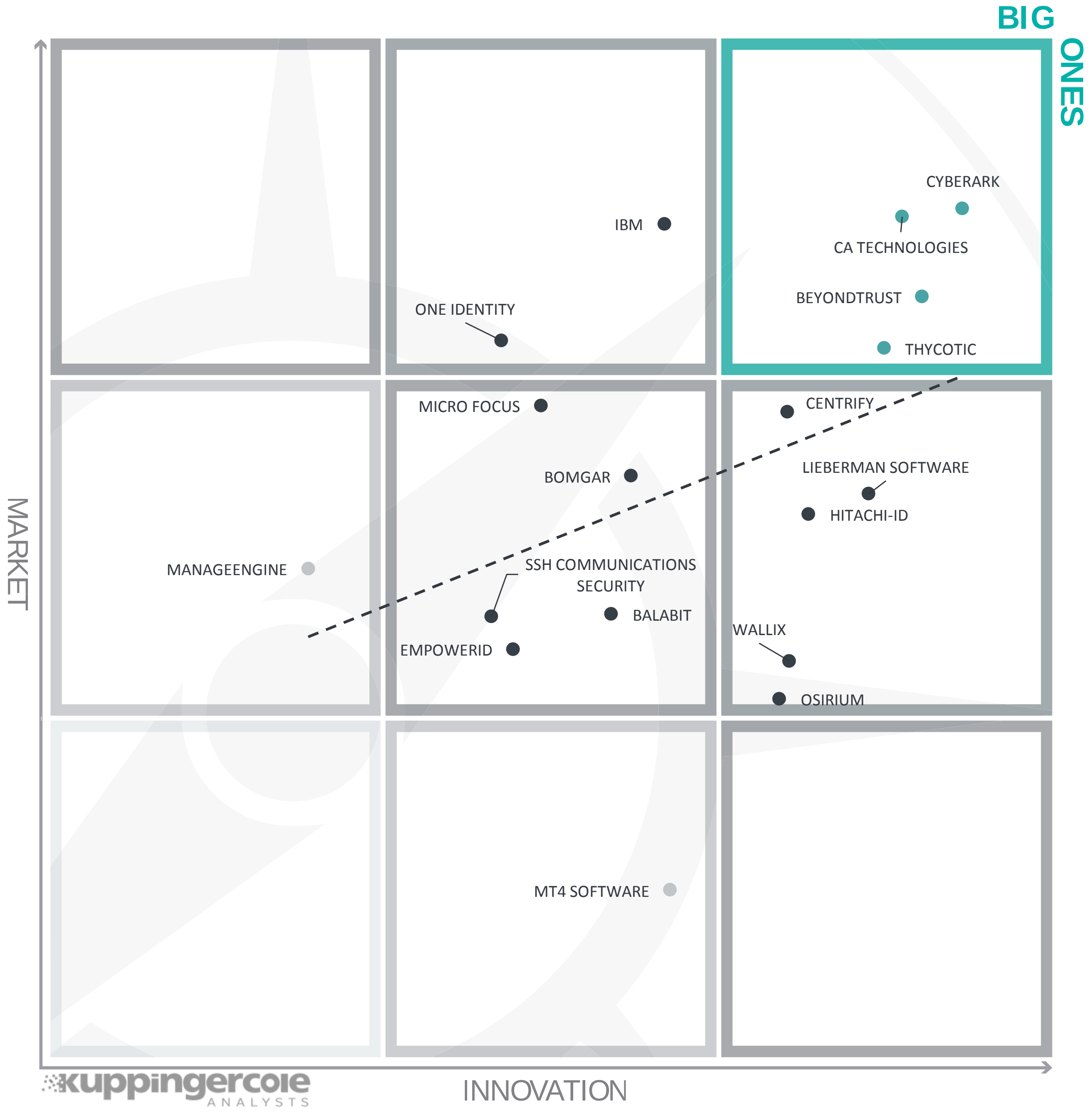


Figure 7: The Innovation/Market Matrix

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.

Again, as in the Product/Market Matrix, the vendors are widely distributed, showing only weak correlation between the market presence and the level of innovation they provide.

In the upper right corner, we see CyberArk, CA Technologies, BeyondTrust, and Thycotic, all being successful in the market, but also showing a strong number of innovative features.

To their right IBM and One Identity are stronger in the market, with One Identity being in the process of rearchitecting their solution.

In the box to the right at the middle, we find primarily younger, very innovative vendors such as Centrify, Lieberman Software, Hitachi-ID, Wallix, and Osirium. All are showing a strong growth potential through their innovativeness.

In the central box, we find more challengers, including (in alphabetical order) Balabit, Bomgar, EmpowerID, Micro Focus, and SSH Communications Security.

Finally, MT4 Software (due to their limited market presence on global scale) and ManageEngine (with their focus on a baseline offering in some part of the Privilege Management market) are placed more towards the bottom respectively to the left.

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 Privilege 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
Balabit	positive	neutral	positive	neutral	positive
BeyondTrust, Inc.	strong positive	strong positive	strong positive	strong positive	strong positive
Bomgar	positive	positive	neutral	positive	positive
CA Technologies	strong positive	strong positive	strong positive	strong positive	strong positive
Centrify Corporation	strong positive	positive	strong positive	positive	strong positive
CyberArk	strong positive	strong positive	strong positive	strong positive	strong positive
EmpowerID	positive	neutral	positive	neutral	strong positive
Hitachi ID Systems, Inc.	strong positive	strong positive	positive	strong positive	strong positive
IBM	strong positive	positive	positive	positive	strong positive
Lieberman Software Corporation	strong positive	strong positive	positive	strong positive	strong positive
MT4 Software Studio	strong positive	positive	positive	positive	positive
ManageEngine	positive	positive	neutral	positive	positive
Micro Focus International plc	strong positive	positive	neutral	positive	positive
One Identity	strong positive	positive	positive	positive	positive
Osirium Technologies PLC	strong positive	positive	positive	positive	positive
SSH Communications Security	strong positive	neutral	positive	neutral	positive
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
Balabit	positive	positive	neutral	neutral
BeyondTrust, Inc.	strong positive	strong positive	strong positive	positive
Bomgar	strong positive	positive	positive	strong positive
CA Technologies	strong positive	strong positive	strong positive	strong positive
Centrify Corporation	positive	strong positive	positive	Positive
CyberArk	strong positive	strong positive	strong positive	strong positive
EmpowerID	neutral	neutral	positive	neutral
Hitachi ID Systems, Inc.	positive	neutral	strong positive	positive
IBM	positive	strong positive	strong positive	strong positive
Lieberman Software Corporation	strong positive	positive	positive	positive
MT4 Software Studio	positive	weak	weak	weak
ManageEngine	weak	positive	positive	positive
Micro Focus International plc	neutral	positive	strong positive	strong positive
One Identity	neutral	positive	positive	positive
Osirium Technologies PLC	positive	neutral	neutral	neutral
SSH Communications Security	neutral	neutral	neutral	positive
Thycotic	strong positive	strong positive	positive	positive
WALLIX	positive	weak	neutral	neutral

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 multi-tenancy, shopping cart approaches for requesting access, and others.

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 Balabit Privileged Access Management

Balabit was founded in 2000 in Hungary and has grown into an international company with sales offices in several European countries, the United States, and Russia, with a large partner network. The company have won widespread recognition in the Open Source community by making their core products available as free editions under the GPL license. Balabit's flagship product is syslog-ng, a de-facto standard syslog server for various Unix-like platforms, which is used in over a million installations around the world.

Strengths	Challenges
● Among the most feature-rich Session Management products on the market ● Support for decrypting encrypted traffic ● Integration with third party PxM, ITSM, and SIEM products ● Fully searchable session replays, even for graphical protocols (based on OCR technology) ● Support for anomaly detection in privileged sessions through the Blindspotter product	● Not a complete Privilege Management solution yet, but leading-edge point solutions that frequently are used as a complement to other PxM products ● Does not protect servers from local privileged access

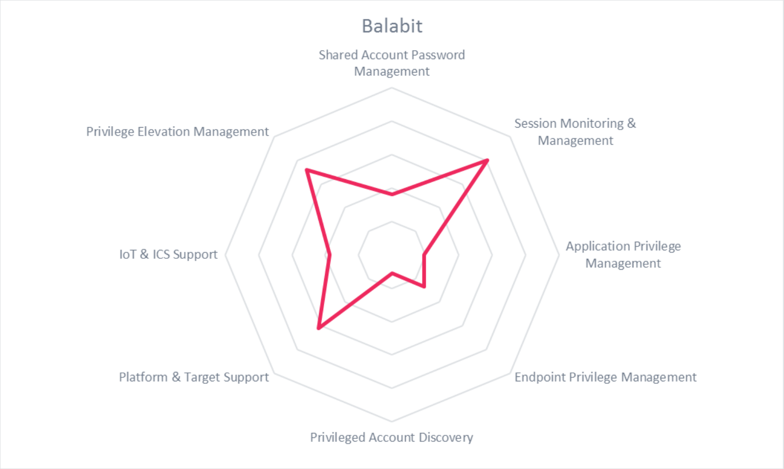
Table 3: Balabit's major strengths and challenges

In its commercial editions, the product delivers enterprise-class log management functionality beyond core syslog features.

Its other core product, Shell Control Box, offers industrial strength session monitoring and recording of privileged user activities in the form of audit trails, while preventing malicious actions by selectively granting or denying access. Shell Control Box is among the most mature and function-rich products in the session management market. This portfolio has been expanded with Blindspotter, a product supporting anomaly detection within privileged sessions, thus adding another core capability. Balabit focuses on privileged activity monitoring & analysis and is leading-edge in this area.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 4: Balabit rating



Balabit's appliance based product offers extensive support for network protocols such as SSH and RDP, but also for legacy protocol types like VNC, X11 and even Citrix ICA and Http. A key innovator in the recording field, Balabit offers OCR (Optical Character Recognition) on Windows for graphical administrative sessions, with effective alerting and detailed search capabilities.

Although Shell Control Box's and Blindspotter's scope of features, also in combination with the other Balabit products, doesn't cover the complete functionality of a traditional Privilege Management suite, concentrating specifically on privileged access management, several unique features of the products as well as integration with PxM, ITSM and SIEM solutions from other vendors make these valuable additions to the multi-layered security infrastructure of any organization.

5.2 BeyondTrust PowerBroker Privileged Access Management Platform

BeyondTrust is an US based vendor of Privilege Management and Vulnerability Management solutions. BeyondTrust's approach to Privilege Management is through a series of products forming the PowerBroker product line. BeyondTrust is privately held and the US remains still its primary customer base, while they are successfully expanding into other geographies and are growing their global partner ecosystem.

Strengths	Challenges
● Long-standing and stable company ● Support for both proxy- and host-based Privilege Management ● Significantly improved integration across product portfolio ● Supports adaptive dynamic authentication based on risks ● Deep integration into target platforms due to their host-centric approach	● Host-based approach for least privilege requires deploying and managing separate components for Unix, Windows, and Mac platforms ● Still relatively small, but steadily growing, partner ecosystem on global scale

Table 5: BeyondTrust's major strengths and challenges

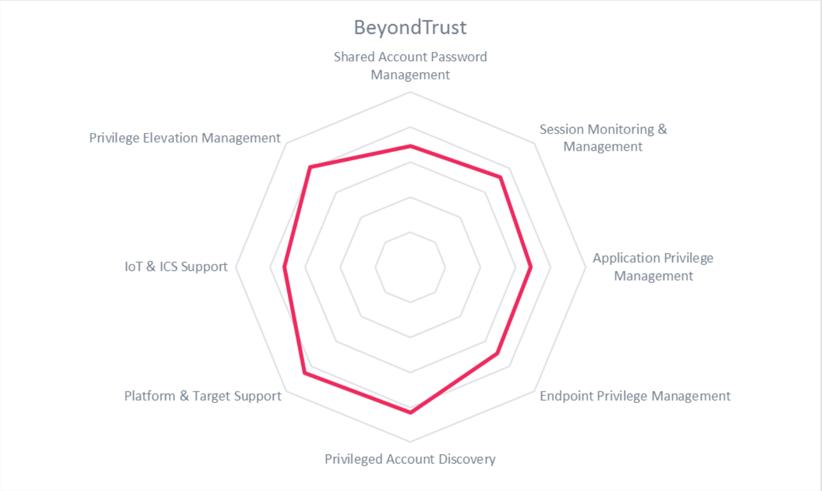
PowerBroker PAM consists of several components, with Password Safe being the central one. This is a password and privileged session management solution offering secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, operating system, network device, database and application accounts – even to SSH keys. A key strength appears to be its ability to dynamically discover and profile accounts.

Password Safe is complemented by other products. We find PowerBroker for Windows, Unix & Linux, and Sudo as host-based components enforcing least privilege access for administrators and delivering extended monitoring and logging capabilities.

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

Table 6: BeyondTrust rating

The PowerBroker product family offers a simple and straightforward deployment for the central components, making it easier for customers who include deployment timelines in their requirements. This integrates main components of the product, including the safe or vault, the policy manager, web access technology, and password synchronization manager on a software, a single, hardened appliance (physical or virtual), and cloud based marketplaces (Amazon AWS and Azure) with centralized configuration and management through their central console, the latter also being fully integrated with the host-based components.



5.3 Bomgar Privileged Access Management solution

While originally regarded as an add-on product for existing identity and access management systems, solutions for managing access for privileged and administrative accounts to critical IT systems have become an essential part of security infrastructures for almost every organization.

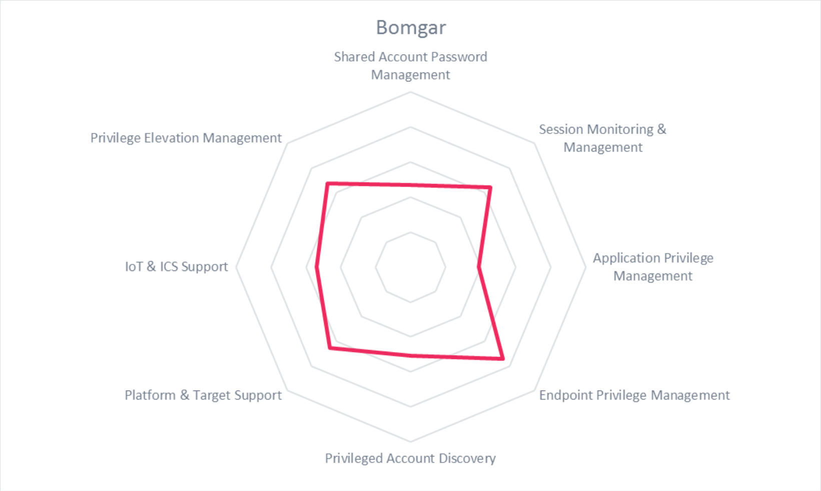
Strengths	Challenges
• "Session-management-first" approach allows fast initial deployments with immediate risk mitigation • Administration of both on-premises and cloud-based target systems • Integration with Bomgar Vault stores, rotates, and protects administrative credentials and includes seamless credential injection • Well-developed partner ecosystem already available	• Focused functionality compared to competitors, but aggressively pursuing a strategic roadmap approach with Privilege Elevation Management in focus • No real-time, behavioural administrative access analytics • Rather new product offering, but already deployed at an increasing number of customer organizations.

Table 7: Bomgar's major strengths and challenges

Bomgar's Privileged Access Management solution provides functionality for enabling secure privileged access to enterprise resources by deploying either a proprietary secure protocol (implemented with active agent components within corporate IT entitled Bomgar Jump) or by extending the reach of existing access methods like Microsoft's Remote Desktop Protocol (RDP), the windows command shell, secure shell (SSH), and Telnet, while securing all these connections leveraging additional cryptographic mechanisms using Bomgar Jumpoint components. Target systems include traditional on-premises platforms like windows or UNIX servers and many others. Additionally, the solution is also capable of managing access to a variety of cloud platforms providing Infrastructure as a Service (IaaS) like Amazon AWS, Microsoft Azure or VMware-based solutions. The Bomgar Vault launched last year, and directly integrates with Bomgar Privileged Access. It offers credential storage and management and includes functions such as password rotation, privileged account discovery, and app to app password management.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 8: Bomgar rating



The overall solution is designed as a lean and efficient platform providing core functionalities fulfilling the requirements of many organizations in the areas of privileged account and session management by focusing on a strict approach to deploying a gateway appliance for network separation plus agent components, with no VPN requirements. Nevertheless, the product as of now does not cover the full set of capabilities provided by other solutions competing in this market segment, however with various features being on the roadmap.

However, the availability of powerful mobile companion apps is a clear competitive advantage allowing for agile and effective implementation concepts with little administrative overhead while maintaining adequate levels of security and compliance.

5.4 CA Privileged Access Management

CA Technologies is a US based, multinational and publicly held company founded in 1976 and is a Market Leader in Identity and Access Management, with a strong footprint in Privilege Management. CA Privileged Access Management is the product that was submitted by CA Technologies. With the acquisition of Xceedium, CA Technologies has significantly broadened its approach to Privilege Management. CA has added several capabilities and also improved the UI significantly.

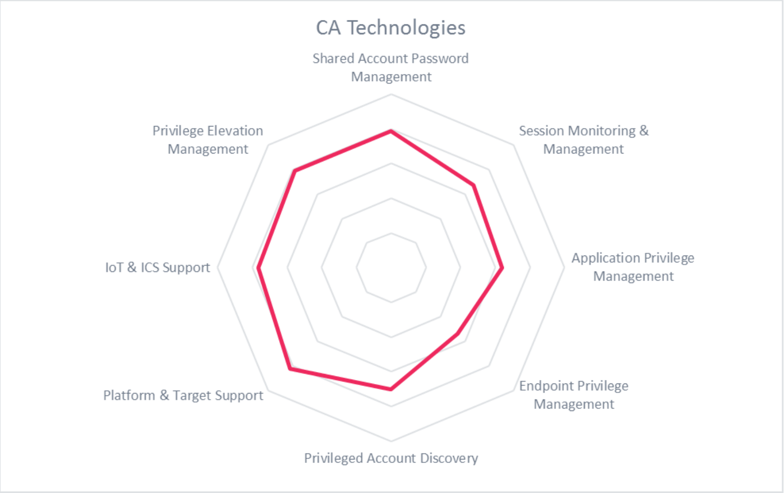
Strengths	Challenges
● Supports a broad number of systems and SIEM products ● Full support for Application Identity Management ● Support for virtualized and Cloud environments ● Modern, strongly improved UI ● Fine grained access control ● Support for both host-based and proxy-based approaches to Privilege Management	● Global but relatively small partner ecosystem ● Threat Analytics offering still lacks support for customization by customers

Table 9: CA's major strengths and challenges

The solution is a scalable one that supports both physical and virtual environments delivering privileged credential management, fine-grained access controls and user activity reporting with a strong focus on security integration and usability. CA technologies also support virtual environments as part of the integrated offering, including fine grained access control for hypervisors and support for container technology such as Docker.

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

Table 10: CA rating



The solution also supports managing shared accounts credential management for privileged user account identities and a session recording component that allows for DVR-like recording of administrative sessions. CA has recently added a Threat Analytics offering, which complements CA Privileged Access Management and adds further analytical capabilities.

CA Privileged Access Management is a comprehensive, mature and overall complete solution that would function well on its own but also integrates fully with other products in the CA Technologies.

5.5 Centrify Server Suite

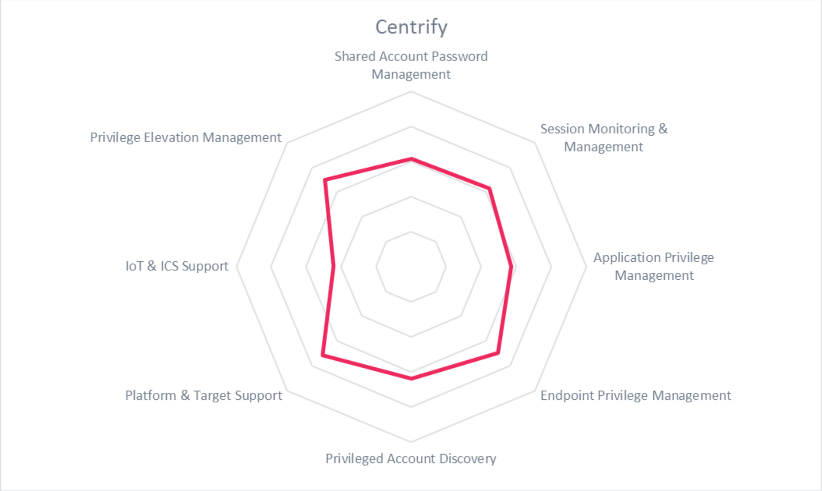
Centrify is a US based Identity Management software vendor that was founded in 2004. Centrify has achieved recognition for its identity management and auditing solutions including single sign-on service for multiple devices and for cloud-based applications.

Centrify is best known for their capability of integrating UNIX and Linux account management into Microsoft Active Directory, but also supports integration of Mac OS X. Centrify also provides identity services that include password vaulting and management, built-in multi-factor authentication (MFA), access request for privileged accounts and privileged roles, secure 3rd party access through federation, brokering of identities for authentication against your choice of directory services, and built-in mobility management. Centrify has traditionally focused on consolidating identities, privilege elevation and host-based privileged session auditing, but has within the last several years improved their position in the market with a unique approach to password vaulting by offering the service as either a SaaS or customer managed solution.

Strengths	Challenges
● Sophisticated integration of UNIX and Linux account management into Microsoft Active Directory ● Role-based control of entitlements for Windows, Linux, and UNIX environments ● Management and restriction of elevated privilege use ● Support for session monitoring and auditing, including capturing of meta-data ● Support for isolation of network zones ● Tight integration with application environments, support Single Sign-On	● Started with Privilege Elevation Management but rather newly added support for a vault as well ● Still relatively new on premises approach, having started in the cloud first ● No advanced behavioral analytics capabilities yet

Table 11: Centrify's major strengths and challenges

It allows for fine-grained, role-based authorization and monitoring of the use of Windows, Linux, UNIX accounts, and network devices. Its password vault was the first privilege management as a service offering to support hybrid cloud environments and 3rd party access, and also supports on-premises deployment options.



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

Table 12: Centrify rating

Looking at the Centrify privileged access security from the perspective of an activity auditing and monitoring solution, it combines shell-level with process-level monitoring and provides support for host and proxy based deployments. Overall, it is well worth evaluating Centrify's privileged access security solution for both securing privileged access in modern heterogeneous environments and as a way to minimize the number of privileged accounts in those environments.

5.6 CyberArk Privileged Account Security Solution

CyberArk takes the overall lead again this year and is the one to beat in Privilege Management. They are headquartered in Israel and since its foundation in 1999 have always been focused on managing privileged access, developing and marketing solutions for securing and managing privileged passwords and identities for users and applications. CyberArk's products are deployed worldwide in most verticals.

Strengths	Challenges
● Products provide both breadth and depth of functionality, particularly regarding support of managed targets ● Threat Analytics and Alerts ● Support AWS and Microsoft Azure management consoles ● Large and solid partner ecosystem	● Modular products; to achieve full functionality may not be cost effective

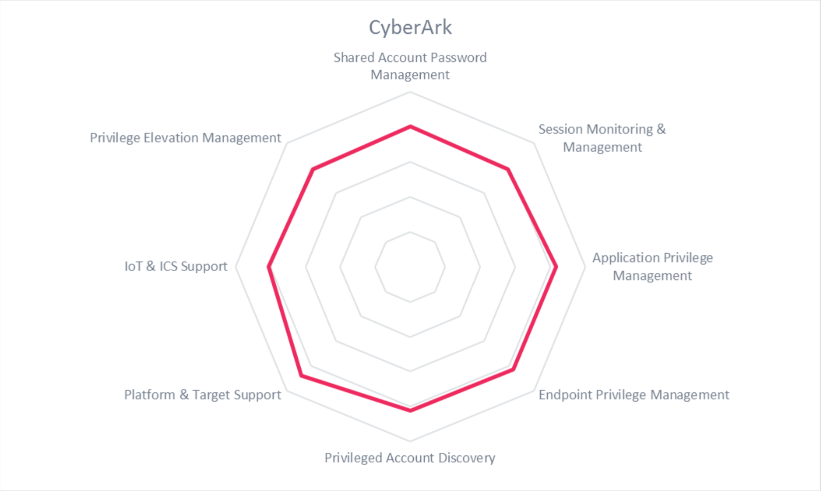
Table 13: CyberArk's major strengths and challenges

The CyberArk Privileged Account Security Solution has, for more than a decade, set the gold standard for Privilege Management and continues to be among the Leaders in this field. The solution consists of several components, four of which are:

CyberArk Enterprise Password Vault, which is the core component of the portfolio and protects privileged credentials based on privileged account security policy, controls who (and what) can access which passwords, and when. Key features include auto discovery and transparent connections that allow for access to systems or devices without exposing the password.

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

Table 14: CyberArk rating



CyberArk Application Identity Manager, which allows for elimination of clear text passwords in configuration files. By replacing credentials based on a signature of the application, it is now possible for any application to automatically retrieve credentials for the target required. In November 2016, the company added credential theft blocking and enhanced threat protection features to CyberArk Viewfinity, which is now available as CyberArk Endpoint Privilege Manager.

CyberArk Privileged Threat Analytics, which detects and alerts anomalous privileged user and system behaviour that could indicate an in-progress attack. The product takes feeds from SIEM and other sources and employs its own behaviour-based analytics to provide alerting on privileged accounts and activities. Other components include CyberArk Privileged Session Manager, CyberArk On-Demand Privileges Manager and CyberArk SSH Key Manager, which are available at an additional charge. Needless to say, CyberArk should be included in every vendor evaluation and product selection process for Privilege Management.

5.7 EmpowerID

EmpowerID is a US-based vendor that offers an integrated, Windows-based IAM suite with strong workflow and policy management capabilities, covering all major areas of IAM including Privilege Management. In the latter area, EmpowerID has enhanced their product significantly over the past years, now delivering good baseline capabilities in the main areas of Shared Account Password Management and Session Management.

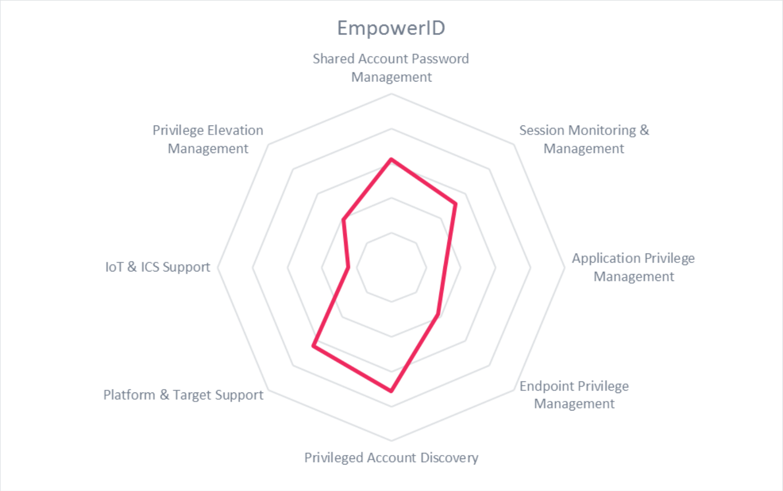
Strengths	Challenges
● Privilege Management fully integrated into a comprehensive IAM suite ● Strong support for workflows and central policy management ● Easy customization ● Leading-edge Adaptive Authentication support	● Runs only on Windows platform ● Good baseline features, but overall gaps in breadth and depth of capabilities ● Limited search capabilities for graphical session recordings

Table 15: EmpowerID's major strengths and challenges

While EmpowerID benefits from its integrated approach in many areas, e.g. by providing, compared with other Privilege Management tools, leading-edge Adaptive Authentication capabilities and workflow support, they provide less breadth and depth in features than most of the Privilege Management point vendors. Some of the major capabilities such as Privileged Threat Analytics or full support for advanced Application Identity Management are not supported, even while the exposed REST APIs allow creating good baseline solutions in the latter area. Also, some more specific feature sets such as the ability for unlocking firewalls, the support for jump hosts, or advanced search capabilities for graphical session recordings are lacking.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	strong positive

Table 16: EmpowerID rating



On the other hand, the workflow and policy management capabilities e.g. allow for a simple and rapid implementation of a four-eye-principle in accessing recorded sessions and for flexible control about which users can access which privileged sessions. Also, Access Governance capabilities are available as part of the integrated solution approach.

The obvious strength of EmpowerID is providing a comprehensive suite for IAM, where Privilege Management is fully integrated into the UI, the shopping cart, the workflow system, and the policy management. This makes EmpowerID an interesting choice for customers who are looking for a full IAM suite with a good baseline support for Privilege Management.

5.8 Hitachi ID Privileged Access Manager

Hitachi ID is headquartered in Calgary, Canada with offices globally. The company had its origins in M-Tech Information Technology, which was founded in 1992 and acquired by Hitachi in 2008. Today Hitachi ID is a provider of Identity Management and Access Governance Solutions.

Strengths	Challenges
● Strong and detailed approach to access control ● Supports advanced Application Identity Management ● Session recording available at no extra cost ● Detailed and advanced approach to discovery and registration of new target systems ● Full support for active/active replication	● No Unix/Linux Privilege Elevation Management yet ● No full Privileged Behavior Analytics capabilities included, but risk-based access control for privileged accounts

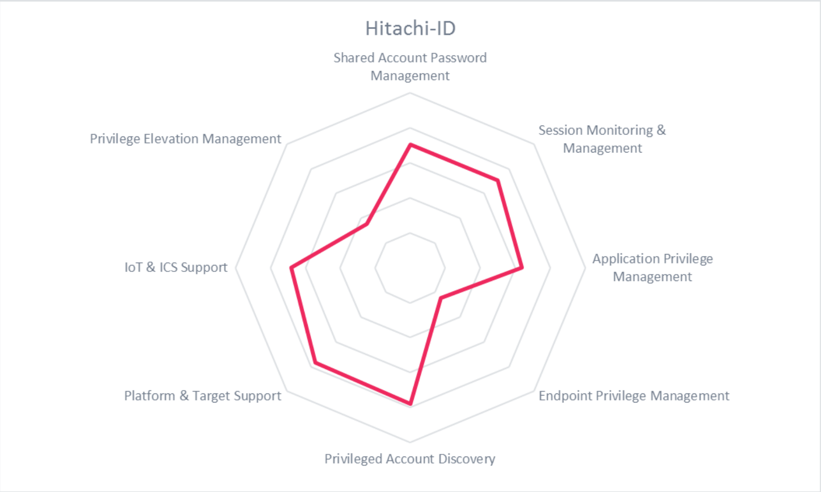
Table 17: Hitachi ID's major strengths and challenges

Hitachi ID Privileged Access Manager is a solution that is very well thought through and full-featured. It is well-positioned in our ratings and an interesting contender to the more well-known players in the market.

The solution supports an exhaustive list of platforms covering both physical and virtual targets. With the access control policy engine, the product also offers very fine-grained control in both Windows and UNIX environments while always keeping track of the original user account, which helps in audit reports.

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

Table 18: Hitachi ID rating



A unique feature of Hitachi ID Privileged Access Manager is that it can also be installed on a laptop running either Windows or Linux. This then allows it to secure access to systems that are sometimes turned off, or that for some reason have limited or no connectivity to the network e.g. windmills, that are often placed over a large geographical area, with limited connectivity but with critical systems. This feature benefits from the active-active, multi-master architecture for password repositories that is unique to Hitachi-ID.

Overall good support for most cloud platforms and for virtualized environments. Hitachi ID should be included in vendor evaluation and product selection processes for Privilege Management.

5.9 IBM Security Privileged Identity Manager (ISPIM)

IBM is one of the leading companies in IT. Founded in 1911, it currently employs approximately 435,000 people and with reported revenues in excess of USD 100 Billion it is the second largest US based firm in terms of employees according to Fortune Magazine (2012). They are very active in the broader IT Security and IAM market, showing noticeable innovation in most areas.

Strengths	Challenges
● Holistic approach across various IBM Security solutions with improved integration ● Strong feature set for anomaly detection through integration with IBM QRadar ● Deployed in virtual appliance form factor ● Massive partner ecosystem	● No support for hyper visor credential management ● Certain IBM technologies beyond virtual appliance need to be deployed

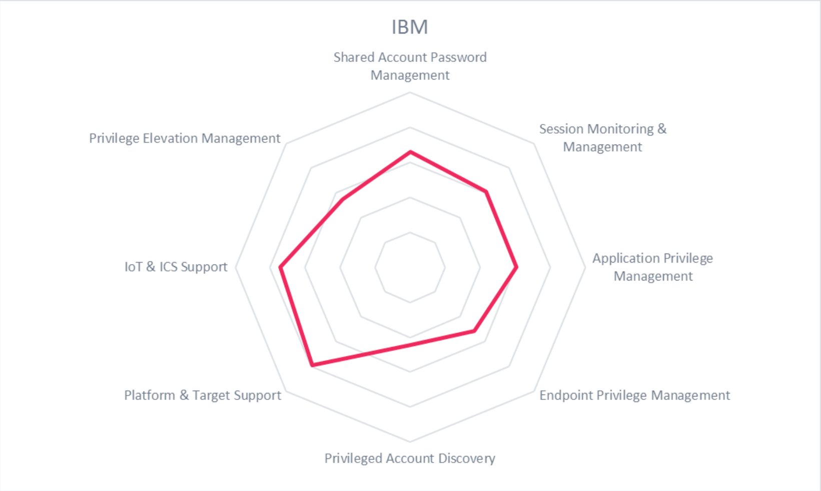
Table 19: IBM's major strengths and challenges

ISPIM has been created based on a number of other IBM technologies, but also extended with specific capabilities for the field of Privilege Management. The appliance form factor eases deployment, even while some other IBM Security components must be installed separately. Furthermore, ongoing integration with IBM Security's threat intelligence and discovery capabilities and IBM Guardium for extended database security capabilities is becoming a strength.

While the product is not leading-edge, it provides good baseline capabilities and benefits from its integration into other IBM Security technologies, if those are already in place. IBM has one of the largest installed bases for their privileged management solutions. Again, as you would expect IBM has one of the largest number of system integrators and partners.

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

Table 20: IBM rating



It is hard to see IBM as a Product Leader in the Privilege Management market; however, IBM provides a good set of baseline features with strong integration into the IBM Security portfolio. For existing IBM customers, that already are using one or more IBM products for IAM, this solution is an obvious choice to enhance their IAM service. It allows creating a holistic security solution well beyond Privilege Management with tight integration across functional areas and products, which can be beneficial from an enterprise architecture perspective compared to stand-alone Privilege Management solutions. However, the entry barrier for non-IBM customers is higher than with other solutions.

5.10 Lieberman Enterprise Random Password Manager

Lieberman Software is a US based software vendor. It saw its inception in 1978 as a software consultancy and released its first commercial product in 1994. The company is privately held and employs more than 60 people. Lieberman Software is a major player in the Privilege Management market with a global client list including more than 20 of the US Fortune 50 companies.

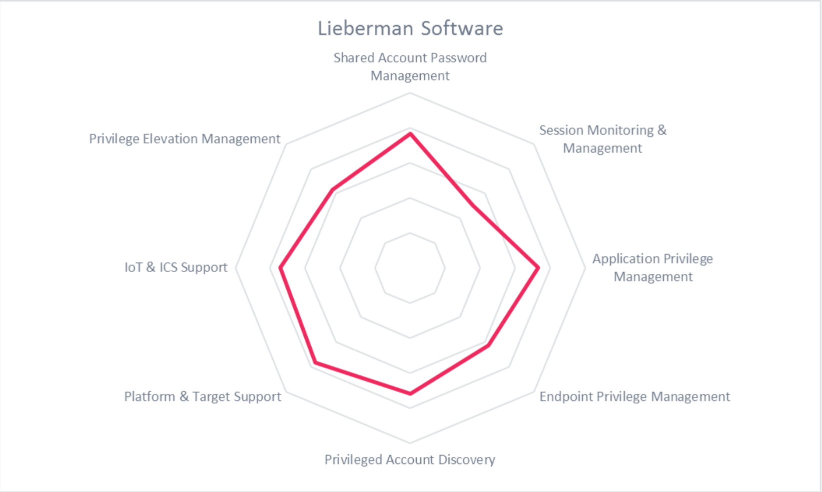
Strengths	Challenges
● Comprehensive system discovery, account discovery, account usage discovery ● Strong feature set particularly for Windows environments ● Proven capability for scaling in large environments ● Support for large variety of cloud and virtual environments	● Limited partner ecosystem and global scale ● Reliance on third party integration in various areas such as session monitoring ● Improved support for Unix and Linux environments with strong SSH key management capabilities, but overall not yet leading-edge in that area

Table 21: Lieberman's major strengths and challenges

Lieberman carries on from previous editions as one of the Leaders in this Leadership Compass in most categories. However, it clearly depends on the use cases whether or not the product is the best fit. While it offers a breadth of functionality, depth of capabilities differs.

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

Table 22: Lieberman rating



Lieberman continues to innovate in Privilege Management and offers comprehensive support for Cloud Computing by adding support for the majority of hypervisors as well as most cloud infrastructure providers. Lieberman also has a clear strategy to fully support the Internet of Things (IoT).

Lieberman's is one of the few products that can be deployed to a large number of systems within a very short period of time, claiming a deployment time of one week for an installation of 100 thousand systems. Again, this depends on the target systems and functionality being deployed, but is a strength particularly for managing large Windows environments.

Lieberman features all the functions you would expect, such as application-to-application password management, password vaulting, management of service accounts etc. A really interesting feature to note is the Known Password Discovery. This feature replaces the default password of devices when deployed, instantly securing your infrastructure. Another interesting feature is the so-called "Security Double-Tap" preventing attacks during automated password reset by resetting passwords twice.

With a robust, enterprise-class and easy and quick to deploy product Lieberman's Enterprise Random Password Manager (ERPM) is a clear choice for being included in vendor evaluations and product selection exercises. However, we would like to see Lieberman increase its presence in Europe and APAC.

5.11 ManageEngine Password Manager Pro

The ManageEngine brand is part of India-based Zoho Corporation that was founded in 1996. They are currently headquartered in Pleasanton, US. However, 90% of their employees are based out of Chennai, India. The company is privately held and has not taken any VC funding or loans. ManageEngine has an impressive number of customers, global reach and a significant partner eco-system.

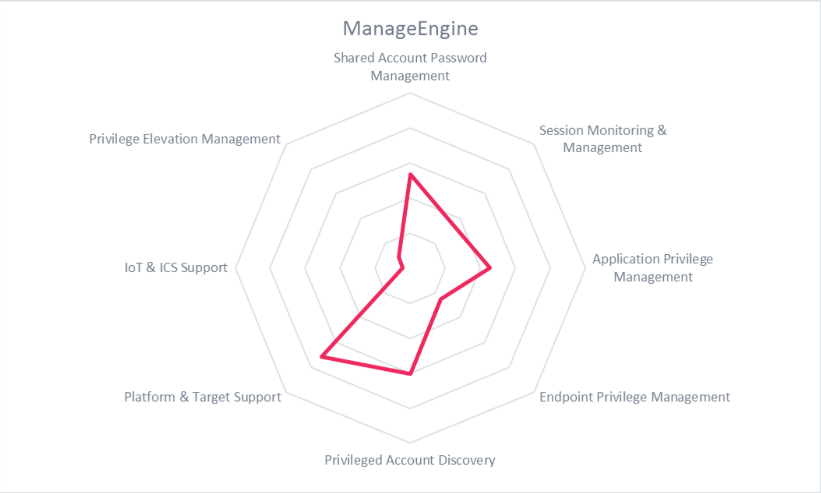
Strengths	Challenges
● Supports advanced Application Identity Management ● Auto discovery of new platforms ● Support for Privilege Management of Hypervisors ● Part of a suite for more than 90 offerings supporting administrators and operators	● Only baseline for SSH key management ● No Integration with Provisioning systems ● Targeted at SMB customers, no full coverage of feature sets

Table 23: ManageEngine's major strengths and challenges

Password Manager Pro offers support for a multitude of target platforms including traditional ones as well as infrastructure components and Hypervisors. The list of features is large which puts ManageEngine Password Manager Pro into the enterprise level class. One feature worth highlighting is the Remote Login Feature. Using this feature, it is possible to launch secure, reliable and completely emulated Windows RDP, SSH and telnet sessions from a browser without any need for plug-ins or agent software.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 24: ManageEngine rating



Another interesting feature, although not unique to ManageEngine Password Manager Pro, is Mobile Access, by which you can retrieve passwords and approve requests on the go. Support for several different cloud-based infrastructures, previously non-existent, has been added. We do however feel that the solution lacks some key features in terms of interoperability and integration, one of the more noteworthy missing feature being the lack of support for integration with provisioning solutions.

ManageEngine is an overall good offering, with most features that you would expect from a vendor in the Privilege Management space. They have a fairly large customer base with a good partner ecosystem. Finally, those with specific PCI-DSS requirements will find ManageEngine’s out of the box reporting capability for PCI-DSS useful. When looking at ManageEngine, it is worthwhile understanding that they provide a large set of tools to administrators and operators, well beyond Privilege Management.

5.12 Micro Focus Privilege Account Management

Micro Focus is among the companies with the most complex history. The product portfolio in Privilege Management is rooted in the Novell days, became NetIQ and then Micro Focus, with Micro Focus and HPE now merging. Micro Focus' product is Micro Focus Privileged Account Manager.

Micro Focus has an interesting grouping of customers spread across Europe, APAC, and the US.

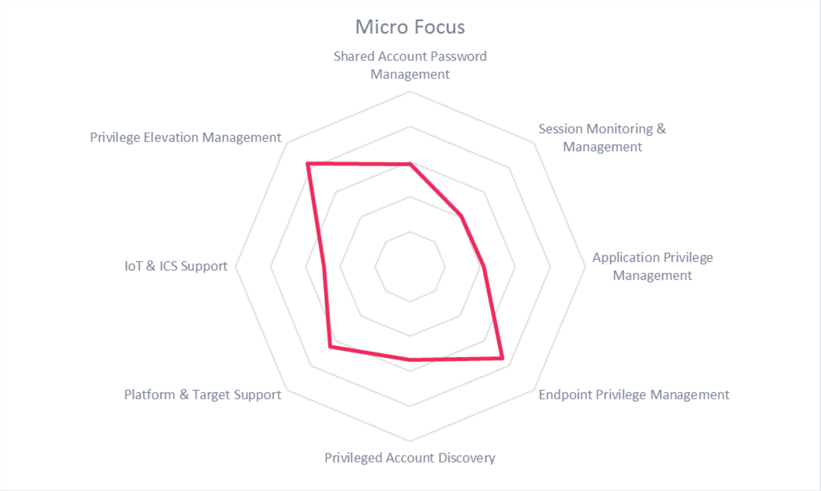
Strengths	Challenges
● Significantly extended feature set and well-thought-out roadmap ● Strong support for database Privilege Management ● Support for SIEM integration and alerting & monitoring ● Integration with provisioning systems ● Support for virtualised platforms	● Broad support for common Privilege Management features, but partial lack of depth of capabilities, e.g. analysis of recorded sessions ● Limited Privileged SSO features ● No Privileged Behavior Analytics

Table 25: Micro Focus's major strengths and challenges

Micro Focus offers the standard feature set associated with traditional Privilege Management, but lacks some of the modern features such as Privileged Behavior Analytics. They repositioned the product recently, supporting a standard feature set including a password vault, risk-based session monitoring, and a variety of other features. Furthermore, they have strong support on supporting privileged access to databases, currently supporting Oracle and Microsoft. However, while Micro Focus has significantly increased the breadth of functionality, there still remain areas with limited depth of features.

Security	strong positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 26: MicroFocus rating



From an architectural perspective, Micro Focus is moving from a purely host-based approach towards a mix of proxy and host-based architecture, which allows for deep integration on certain target systems, while other capabilities such as the password vault are run centrally.

Micro Focus' Privileged Account Manager is an overall good offering, with most features that you would expect from a vendor in the Privilege Management space. Micro Focus has made significant progress in that area and is continually improving their offering. In combination with their other products they have a decent overall customer base with a good partner ecosystem. Despite the progress made, there still is considerable opportunity for Micro Focus to innovate and further strengthen their offering. Their current updates and the roadmap plans make Micro Focus a vendor to take into account when looking for a Privilege Management offering.

5.13 MT4 Software Studio

MT4 Software Studio is a Brazilian software vendor, providing a series of IT Security products. Among these products is their flagship product Senha Segura, which is a comprehensive, well-integrated offering in the area of Privilege Management.

Strengths	Challenges
● Overall comprehensive product offering with good UI, covering most major areas of Privilege Management ● Proven performance and scalability ● Well-integrated solution, good and efficient UI ● Focused provider of IT Security solutions	● Limited support for multiple languages ● Some gaps in breadth of session recording ● Small vendor with limited global scale and small partner network ● No full support for Privileged Behavior Analytics, but good risk-oriented reporting

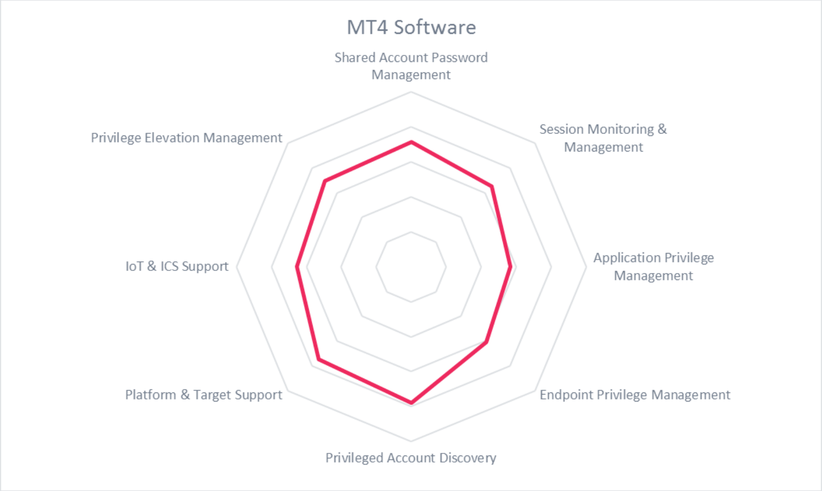
Table 27: MT4's major strengths and challenges

The overall product feature set is astonishingly broad and deep. In core areas such as Shared Account Password Management, the offering provides a comprehensive feature set, delivered via a well thought-out and efficient to use UI. Senha Segura is more than just an entry-level offering, but an already mature product.

However, there are some gaps in functionality. Application Identity Management is supported, but, e.g., the interfaces to databases are rather weak. In the area of Session Recording, baseline support is provided for both text-based and graphical sessions, however some of the other offerings in the market offer more breadth than Senha Segura, e.g. in OCR analysis and meta data collection. Also, Privileged Behavior Analytics is still missing.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 28: MT4 rating



But in sum, Senha Segura is, from a feature perspective, an enterprise-level offering that is competitive with the established products in the market. Thus, particularly for organizations having a strong footprint in their local markets in South America, the product is an option to the more well-known competitors.

While the product offering of MT4 Software Studio is surprisingly strong for a small vendor, their obvious challenge is delivery on global scale. As of now, the company is lacking a global partner ecosystem. Building such an ecosystem and adding broad support for other languages appears to be the main task for now, so that Senha Segura becomes a real option for customers in other geographic areas than South America. It definitely has the potential for doing so.

5.14 One Identity Privileged Management Solutions

One Identity is part of Quest Software, which became independent again after being part of Dell for some years. The solution consists of a number of components, which are referred to as One Identity Privileged Management Solutions.

Strengths	Challenges
● Strong feature set for both Unix/Linux and Windows environments ● Enterprise ready and proven ● Global presence of and strong partner ecosystem ● Tight integration with One Identity Manager and other One Identity products	● Limited customization possibilities particularly of Privileged Password Manager ● Limited Support for Cloud Infrastructures ● Major update planned

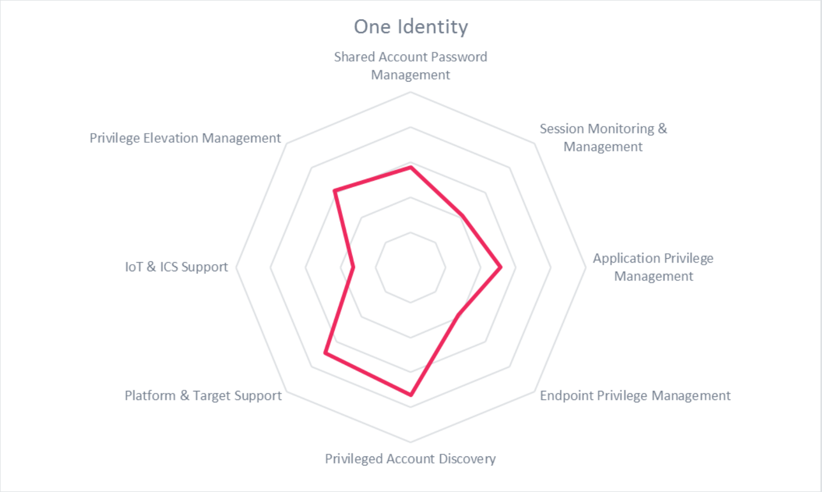
Table 29: One Identity's major strengths and challenges

The main products of One Identity Privileged Management Solutions are Privileged Password Manager, Privileged Access Suite for UNIX, and Privileged Session Manager. These are well integrated with other product offerings provided by One Identity.

Privileged Access Suite for UNIX is targeted towards UNIX based systems including Linux and Mac. As also seen from other providers, the approach to managing privileged accounts is by using the capabilities of Active Directory and integrating UNIX authentication into Active Directory. The tool also supports various options for delegating root privileges.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 30: One Identity rating



Privileged Password Manager is a full-featured Privilege Management solution offering all the features that could be expected such as password repository and extensive logging and monitoring capabilities. This product can be supplied as a hard appliance. There is also integration to One Identity Manager, One Identity's Identity Provisioning and Access Governance solution.

One Identity solutions cover a wide area, based on two main products, which are integrated into a hard appliance. Notably, One Identity is in the progress of moving to a largely rearchitected solution, thus we recommend customer checking back with the vendor on the current status and roadmap plans.

5.15 Osirium

Osirium is a UK-based provider of a Privilege Management solution. The product differs from most other offerings in certain areas. On the one hand, this makes comparison to other vendors' offerings difficult; on the other hand, the differences might be exactly what customers are looking for, in particular the task-based approach and the "gateway" concept Osirium has implemented.

Strengths	Challenges
● Task-based approach allows restricting privileged access to pre-defined tasks, with a wide range of preconfigured tasks ● Support for downstream target systems through "gateways" ● Password never touches administrative workstations ● Support for Privileged Behavior Analytics	● Lack of Application Privilege Management ● Small vendor with a rather limited global scale and lack of a global partner ecosystem ● Overall broad coverage of capabilities, but lack of depth in certain areas

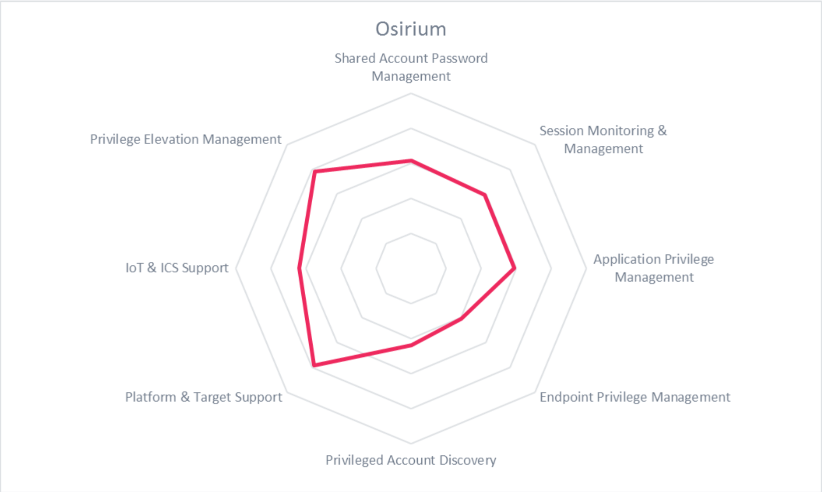
Table 31: Osirium's major strengths and challenges

While offering support for common feature sets such as Shared Account Password Management or Session Management including Session Recording, there are some gaps, both in supporting specific areas such as Application Privilege Management and in depth of features, compared to the market leaders. On the other hand, Osirium already supports the new area of Privileged Behavior Analytics.

However, more importantly, Osirium is taking a different approach in certain areas, which is a challenge in a feature list comparison but might result in a better solution to customers. One is their task-based approach, which allows assigning restricted tasks to users. Thus, instead of granting full access to privileged accounts, customers can assign task sets to their administrators and operators, which allows for implementing a real least privilege model. Osirium provides a broad range of pre-configured tasks across a variety of systems.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 32: Osirium rating



Another area where Osirium differs significantly from other vendors is their approach of using sort of "gateway" systems, which can be based, e.g., on rather old operating systems. These are accessed and managed remotely, allowing the running of old software stacks that are still required for managing certain environments. Particularly with respect to the emerging demand in Operational Technology Security, e.g. for managing ICS (Industrial Control System) environments, this approach appears to be very valuable.

From our perspective, Osirium is an interesting alternative to the established players in the Privilege Management market and thus a strong contender, particularly because they opted for new, innovative approaches in certain areas instead of following a "me-too" approach. Despite their rather small partner ecosystem, they might be considered in evaluations to have an option for an alternative approach to Privilege Management, which might be the better fit for some customers.

5.16 SSH Communications Security

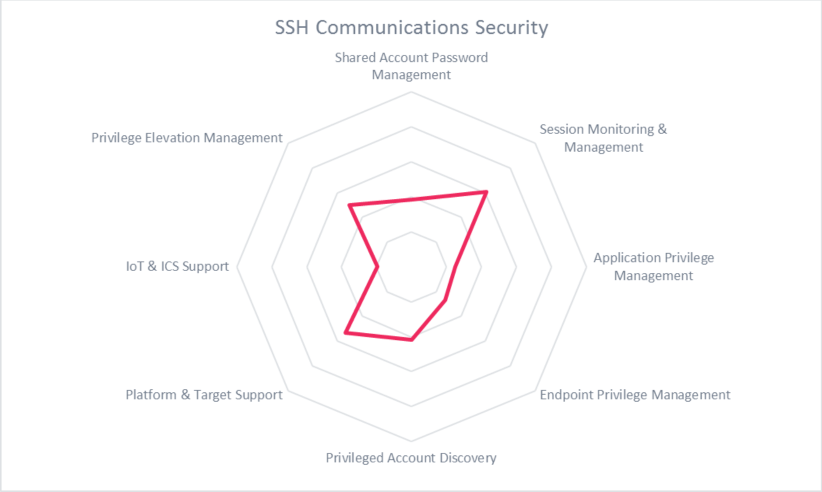
SSH Communications Security Corporation is a publicly traded company based in Helsinki, Finland. The company develops a number of products around the SSH protocol, including Tectia SSH - a multiplatform SSH client/server solution, CryptoAuditor for monitoring and managing privileged user activities, as well as the Universal SSH Key Manager, which is covered in this review. Currently, SSH Communications Security has a team of around 110 employees led by Tatu Ylönen, and over 3000 customers around the world.

Strengths	Challenges
● Unified automated solution for all aspects of SSH infrastructure management and good Session Monitoring features ● Non-intrusive operation, does not require changes in existing processes ● Large number of supported platforms, SSH servers and clients ● Real-time alerting and remediation actions, integration with most SIEM solutions ● Global presence with multiple offices in the US, Europe and Asia	● Functionality limited to SSH keys and Session Monitoring, not a full-featured Privilege Management Solution ● No vault, but indirect approach of authenticating privileged session access also by shared accounts

Table 33: SSH's major strengths and challenges

For Privilege Management, two solutions are of relevance. One is Universal SSH Key Manager is a unified solution covering all aspects of discovery, monitoring and management of SSH infrastructures across multiple platforms, both on-premise and in the cloud. It’s a mature feature-rich product backed by the expertise of the original developer of the SSH protocol. Designed to be non-intrusive, it can be deployed quickly without changes in existing network infrastructures or business processes.

The other is CryptoAuditor, which analyzes privileged sessions via different protocols, including RDP and SSH. It can monitor sessions, block sub-protocols such as file transfer or clipboard access, authenticate users, and block access and distribution to various types of content.



Security	strong positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 34: SSH rating

Universal SSH Key Manager can be recommended for any organization using SSH within their IT infrastructures. That is, for every organization in the world. However, it is not a complete Privilege Management solution. CryptoAuditor, the other offering, provides the same look and feel but it not fully integrated yet. Together, these two offerings provide a good baseline-level of Privilege Management capabilities, while not yet being feature-complete.

5.17 Thycotic Secret Server

Thycotic is a Washington DC based software vendor, incorporated in May 2000. Thycotic provides password and Active Directory Group management solutions. Their approach is similar to most of the other vendors in this space, and they offer a full featured Privilege Management Product. The company is privately held and recently funded by Insight Venture Partners. Thycotic might be considered the underdog of Privilege Management, coming from the lower end of the market and steadily making their way into enterprise level clients.

Strengths	**Challenges**
● Supports a broad number of systems ● Automatic password rotation of system accounts ● Simple implementation & user friendly ● Historical Auditing ● Web and mobile access ● Robust application to application password management	● Still limited partner ecosystem ● Can only be implemented on a Microsoft Stack ● New capabilities for Privilege Behavior Analytics not yet feature-complete, lacking full integration into Secret Server

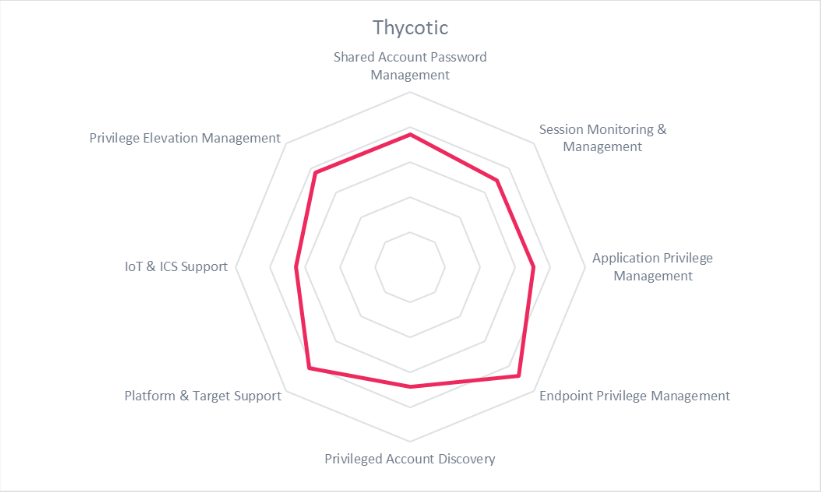
Table 35: Thycotic's major strengths and challenges

Thycotic is a very interesting and "young-minded" vendor, in that they focus very much on features supporting the emerging platforms such as support for REST and cloud services. This has earned them a place as a Leader in innovation from our point of view. They have gone from being a pure password management software vendor to now offering a full-fledged Privilege Management platform ready for global enterprises.

Features that should be noted are their large and growing support for cloud infrastructures and mobile applications. The real-time management of passwords is also a nice feature, where you can setup real-time alerts when and if passwords are changed. As you would expect, Secret Server supports RBAC – which is more or less the standard now for Privilege Management – for management of access to systems.

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

Table 36: Thycotic rating



Thycotic have numerous high-profile clients, and their product has proven to be a mature enterprise class solution. Thycotic Secret Server would fit well into any organization looking for a good, reliable and comprehensive Privilege Management solution. A particular strength of the product is support for rapid deployment, based on the long-standing experience of Thycotic with a very large number of smaller customers where complex deployments involving professional services will not work. Recently, they added Privileged Behavior Analytics capabilities which, however, aren't yet feature-complete and not fully integrated with Secret Server.

5.18 Wallix AdminBastion Suite

Wallix is a French provider of software and services in the Privilege Management market. Their product Wallix AdminBastion (WAB) Suite is at the core of their offerings, as they fully focus on managing privileged users, providing password management, implementing access control and maintaining traceability to secure access to Systems. Wallix has a fairly large installed base along with a fair number of customers. Wallix has virtually no presence in the USA with over 90% of its customer base in the EMEA region.

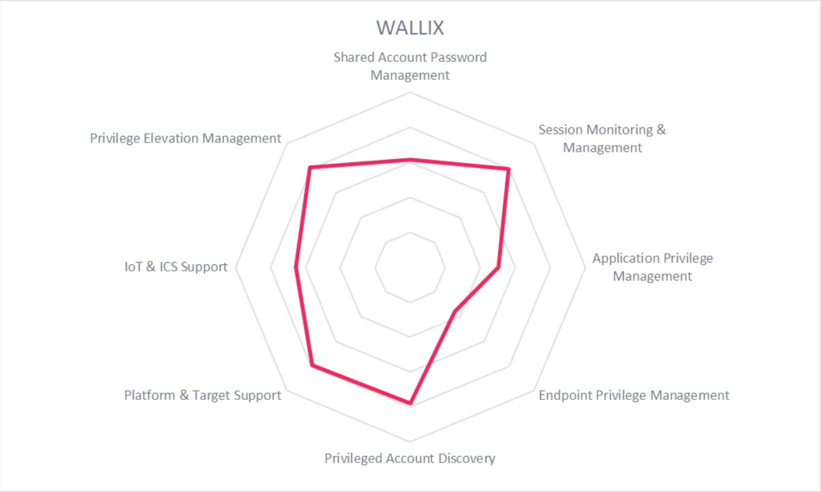
Strengths	Challenges
● Supports a broad number of systems ● Leading-edge session logging and recording capabilities ● Full support for multi tenancy ● Well thought-out roadmap, becoming increasingly feature-complete	● Relatively limited reach outside EMEA ● Limited partner ecosystem, but started alliance program ● No support for threat analytics yet, but partnerships with vendors such as Splunk and IBM

Table 37: Wallix's major strengths and challenges

Wallix AdminBastion (WAB) suite is a single access web portal for multi-bastion and/or multi-tenant organizations. It includes user and session management, password management and built-in access request and approval capabilities. It provides Single-Sign-On to connected systems, session auditing and recording, real-time supervision of sessions, and scheduled reports. In the area of session monitoring and recording, Wallix clearly is among the leading-edge vendors in the market.

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

Table 38: Wallix rating



Over time, enhancements for providing robust and unified Privileged Password Management have been implemented with the overall strategy aiming at positioning the WAB suite as a general Privileged Access Management system, including unified password management, privileged single sign-on and basic automated real-time session analytics.

Wallix is one of the few vendors that focus on supporting protocols rather than platforms making it an easier choice in some environments. We like the fact that it has adopted a pure web based user interface approach. However, the solution lacks some key features in terms of interoperability and integration, one of the more noteworthy missing features being the lack of support for integration with Identity Provisioning solutions beyond baseline Active Directory integration. However, with a well-thought-out roadmap and the various innovations provided in recent releases, Wallix is making its way from a specialized session management provider towards a strong contender of established solutions for the overall Privilege Management market.

6 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on Privilege Management, there are several other vendors which either declined participation in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document, or are not (yet) mature enough to be considered in this document.

6.1 AppleCross Technologies

AppleCross Technologies provides their Privileged User Manager (PUM) tool. The tool is targeted at Shared Account Password Management and Privilege Elevation Management for Windows and Linux/Unix platforms. The software might be an alternative for entry-level requirements in the Privilege Management space.

6.2 Arcon

Arcon is based in India and is fast emerging as a strong Challenger (still a relatively unknown player) in the Privilege Management field with its biggest presence in APAC, and a smaller European presence. Its product is Arcos Privileged Identity Management. Our analysis has uncovered a product with a strong feature set that is constantly being improved and is ready to play on an enterprise level. We are very excited to see how that will evolve over the next months and years.

The suite, built on the Windows platform only, is feature-rich, with features that are to be expected from top-of-class products such as integration to ticketing systems and several SIEM systems while offering support for session invocation and recording, Application Identity Management and support for RBAC (Role Based Access Controls) for product features. The offering delivers rich interfaces for programming, but not a complete REST-based set of APIs yet. While this allows for flexible integration, integration efforts can become significant. Furthermore, while there is a broad range of supported features, some areas such as discovery functions still lack some depth in functionality.

Arcon Arcos Privileged Identity Management, which supports one of the most fine-grained SoD policy sets we have seen in that market segment, can be deployed in a number of different ways both as a hard or a soft appliance. It is tested to work in Amazon’s AWS. We would have liked to have seen support for a few more languages, as at the time of writing only English, French and Spanish are supported. Arcon has demonstrated success with some large-scale deployments. On the other hand, deployment commonly requires professional services and might require coding for integrations, which can lead to longer timelines for running projects. The company has a small partner ecosystem, however with some partners operating at global scale. Overall, ARCOS is an interesting alternative to the established products particularly from its breadth of features.

6.3 Firmus

Firmus is another player in the market. While they act as a system integrator, they also offer MasterSAM, a suite of products targeting Privilege Management, User Activity Monitoring, and Access Control for users. With the overall feature set, the tool is considered to be an alternative to established players, however the main emphasis of the vendor appears to be on the system integrator business.

6.4 Fox Technologies/FoxT

Fox Technologies delivers a product targeted at managing servers. The product, named FoxT BoKS ServerControl, covers both Shared Account Password Management and Privilege Elevation Management, based on centralized security policies and covering various types of server operating systems. Fox Technologies counts among the more established players in the market and is an option particularly for Privilege Management targeted at large data center environments, with focus on the traditional requirements such as Shared Account Password Management.

6.5 NRI Secure

NRI Secure Technologies is primarily a system integrator. However, they also provide a software solution targeted at administrator access to server environments, fitting into the Privilege Management market. The main emphasis is on Shared Account Password Management and logging of access of privileged users.

6.6 ObserveIT

ObserveIT provides a comprehensive solution for monitoring user activity across the enterprise. The product operates primarily based on agents that can be deployed across a variety of platforms. It provides detailed user behavior analysis and live session response.

ObserveIT is one of a few specialized vendors that started in the area of Privileged Session Monitoring. Like all players in that particular niche of the Privilege Management market, ObserveIT extended its portfolio gradually to provide a more comprehensive feature set. The company now focuses on User Activity Monitoring for all types of sensitive users, including three major capabilities:

- Monitoring and recording of sessions in visual form, both command line and GUI sessions, and the creation of user activity logs from the recorded data;
- User behavior analytics, that detect and alert about abnormal or illegitimate activities of users or hijacked accounts; and
- Live session response, allowing interception and alteration of sessions at runtime based on both information collected with user behavior analytics or through external products such as SIEM (Security Information and Event Management) tools.

Additionally, their focus has extended from solely the traditional coverage of administrators and operators to also supporting use cases of other application users of systems such as SAP and external service providers that operate applications.

In the area of session monitoring and recording, or – to use the term ObserveIT introduced – 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 variant, SSH, Telnet, direct logins to consoles etc.

Due to the fact that ObserveIT works with an agent-based approach, information can also be collected locally, in contrast to a number of other solutions that are network- or gateway-based.

ObserveIT's agent-based approach not only allows monitoring and session recording, it also creates user activity logs that translate all user actions into logs. These logs allow meaningful and efficient searches; thus customers can quickly jump to the right section in a recording when doing forensics. ObserveIT delivers a strong implementation in that feature area, allowing for efficient analysis of recorded sessions.

Based on the wealth of information collected, ObserveIT further provides the ability to run rule-based user activity analytics and generate alerts in case of rule violations. Such rules can be configured to, e.g., identify access to uncommon applications, systems, or other resources; identify the execution of an unusual number of activities; or alert on activities outside the normal work hours. There is a broad variety of criteria available for such analysis.

Based on the rules, alerts can be created at runtime, notifying defined individuals about rule violations, so that they can take action. These actions include access to the video recordings of sessions, but also access to the detailed user activity log.

ObserveIT has a well-defined partner program for various groups of partners, including alliance and technology partners for technical integration, resellers and distributors, and managed service and consulting partners. With its approach, ObserveIT can be an interesting addition to other Privilege Management solutions as well as a standalone solution for the use cases such as privileged session management addressed by that company.

6.7 Oracle

California based Oracle is another one of the old-time giants in the software industry, and with the acquisition of Sun back in 2009 now also in Hardware. When it comes to IAM, Oracle has always been leading edge in most segments.

OPAM (Oracle Privileged Account Manager) is one of these products. It focuses on managing passwords for privileged users, in particular shared accounts such as Unix/Linux or database administrators. It also supports auditing of the use of such accounts.

The product is becoming increasingly integrated with the overall Oracle IAM suite of products, which allows comprehensive lifecycle management for privileged accounts. This is on the one hand a clear strength of the Oracle solution, enabling an integrated approach on Privilege Management, in contrast to relying on specialized tools. On the other hand, customers looking only for Privilege Management are challenged with the need of acquiring a broader suite of products to achieve the Privilege Management functionality.

6.8 Wheel Systems

Wheel Systems provides an appliance-based solution for managing privileged access, covering Shared Account Password Management, Application Privilege Management, and Session Management. Their offering, named FUDO PAM, provide a good level of features and can become an option to established systems in the market.

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 particular 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.

7.1 Types of Leadership

We look at four types of leaders:

- 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 area, we distinguish between three levels of products:

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

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

7.2 Product rating

KuppingerCole as an analyst company regularly does 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 on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole 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. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and

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

password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to 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 which the vendor has provided is of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

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

7.3 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.

7.4 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.

7.5 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 Privilege Management, we look at the following seven areas:

Shared Account Management

Capabilities for managing shared account passwords, providing single sign-on access to privileged accounts, and related capabilities.

Session Monitoring & Management

Features in Session Monitoring and Session Management, including recording of both text-based and graphical sessions and the capability of finding relevant events in such recordings.

Application Privilege Management

Managing application privileges, e.g. by identifying privileged accounts and passwords in scripts, replacing these, managing these, etc.

Endpoint Privilege Management

Management of privileged accounts on endpoints, including identification of such accounts, application whitelisting, and other capabilities targeted at endpoint systems.

Privileged Account Discovery

Discovery capabilities for privileged accounts, including grouping of such accounts, interfaces to CMDBs, and other related capabilities.

Platform & Target Support

Breadth and depth of target platform support for the various feature areas.

IoT & ICS Support

Capabilities targeted at IoT environments, in particular IIoT (Industrial Internet of Things), and ICS (Industrial Control Systems), both areas where we observe a strong demand and need for Privilege Management solutions.

Privileged Elevation Management — Limiting elevation of access rights for privileged accounts, supporting enforcement of least privilege principles; frequently enforced through platform-specific agents.

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 other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Privilege Management.

7.6 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 Privilege Management offerings in chapter 6, “Vendors and Market Segments to watch”. In that chapter, we also look at some other interesting offerings around the Privilege Management market and in related market segments.

8 Copyright

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

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**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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