KuppingerCole Report

LEADERSHIP COMPASS

By Paul Fisher
February 11, 2021

Privileged Access Management for DevOps

Privileged Access Management (PAM) is an important area of access risk management and identity security in any organization. Privileged accounts have traditionally been given to administrators to access critical data and applications. But, changing business practices, hybrid IT, cloud and other aspects of digital transformation has meant that users of privileged accounts have become more numerous and widespread. One area in sharp focus is DevOps support which has become essential to many organizations looking to become more responsive and innovative. Application developers and other agile teams increasingly need privileged access to essential tools, and several PAM vendors are responding to this demand.

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

Content

1 Introduction 4

1.1 Market segment 4

1.2 Delivery models 8

1.3 Required capabilities 8

1.3.1 Toolchain support 8

1.3.2 Runtime support 9

1.3.3 Finished application support 9

1.3.4 Certificate support 9

1.3.5 Base PAM support 9

1.3.6 High Availability (HA) 10

1.3.7 Non-human user support 10

1.3.8 Shared account support 10

1.3.9 Just in Time (JIT) 10

1.4 Other capabilities to support DevOps 10

1.4.1 Privileged Account Data Lifecycle Management (PADLM) 11

1.4.2 Controlled Privilege Elevation and Delegation Management (CPEDM) 11

1.4.3 Endpoint Privilege Management (EPM) 11

1.4.4 Session Recording and Monitoring (SRM) 11

1.4.5 Privileged Single Sign-On (SSO) 12

1.4.6 Privileged User Behaviour Analytics (PUBA) 12

2 Leadership 13

3 Correlated View 21

3.1 The Market/Product Matrix 21

3.2 The Product/Innovation Matrix 23

3.3 The Innovation/Market Matrix 25

4 Products and vendors at a glance 27

5 Product/service evaluation 30

5.1 BeyondTrust 31

5.2 Centrify 34
5.3 CyberArk 38
5.4 EmpowerID 41
5.5 HashiCorp 44
5.6 SSH Communications Security 47
5.7 STEALTHbits Technologies 51
5.8 Symantec 54
5.9 Thycotic 57
6 Vendors and Market Segments to watch 60
6.1 Remediant SecureONE 60
6.2 Saviynt 60
6.3 Venafi 61
7 Related Research 63
Methodology 64
Content of Figures 70
Copyright 71

1 Introduction

This report is an overview of the market for Privilege Access Management (PAM) solutions and provides a compass to help buyers find the solution that best meets their needs. KuppingerCole examines the market segment, vendor functionality, relative market share, and innovative approaches to providing PAM for DevOps solutions. This follow up to the larger Leadership Compass PAM 2020 (published May 2020) concentrates on those vendors we believe are best addressing the challenge of managing PAM within DevOps environments. Many vendors have yet to consider DevOps and agile environments, or believe their solutions cover this adequately, hence a smaller report.

However, the view of KuppingerCole is that the 10 vendors featured are currently doing most for DevOps by adding special technologies and capabilities that address the operating environments and pressures that DevOps teams tend to work in.

1.1 Market segment

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

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

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

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

In recent years, Privileged Access Management (PAM) has become one of the fastest growing areas of cyber security and risk management solutions. KuppingerCole estimates that the number of major vendors in the space is around 40 with a combined annual revenue of around $2.2bn per annum, predicted to grow

to $5.4bn by 2025 (see Figure 1).

That growth has largely been driven by changes in business computing practices and compliance demands from governments and trading bodies, as well as increased levels of cybercrime. The growth of Advanced Persistent Threats (APT) and the ability of hackers to access service accounts is a threat PAM can help with. Protecting admin and service accounts can make it more difficult for state actors and corporate espionage agents to abscond with data. PAM controls create additional hurdles for would-be attackers to pass as well as potentially more indicators of compromise (IoC) and thus opportunities for being discovered earlier in the process.

Digital transformation, regulations such as GDPR, the shift to the cloud and, most recently, the growth of DevOps in organizations looking to accelerate their application development processes are all adding to the growth.

The reason for this mini boom is that these trends have triggered an explosion in data and services designated as business critical or confidential, and a concurrent rise in the number of users and applications that need to access them. IT administrators realised that without dedicated solutions to manage all these, the organizations would be at great risk of hacks and security breaches. Hackers and cyber criminals have long targeted unprotected privileged accounts as one of the easiest routes to get inside an organization.

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

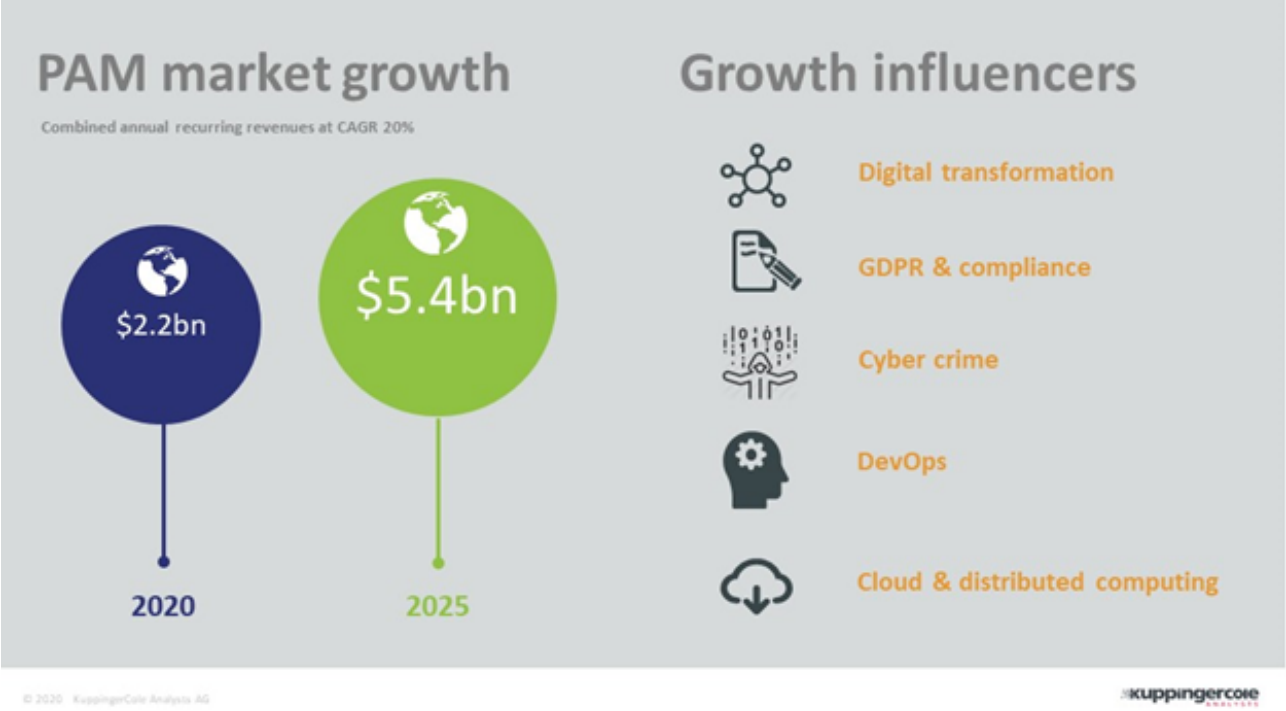


Figure 1: The PAM market is seeing dynamic growth as vendors seek to add better functionality to meet security challenges and more players enter the market.

The impact of agile development and DevOps on PAM

The pressure on organizations to develop their IT infrastructures within an automated Continuous Integration and Delivery framework (CI/CD) is increasing. The directive is from senior management who wish to see improvements in competitiveness through IT, and IT team leaders looking for boosts in software productivity and efficiency to meet the demands of senior management. Modern organizations are an unwieldy mixture of interconnected code and applications including microservices, APIs, desktop apps and mobile apps and to keep all these up to speed requires a constant stream of updates and patches – not to mention the roll out of brand-new software projects. It is not uncommon today for applications to be updated many times a day.

Today, the CI/CD trend impacts as much on third party and customer facing, software driven products as it does on internal IT projects. In a world seeking perfection, nothing is ever finished. At the heart of this process is the DevOps IT team culture which emerged to break down the traditional engineering and operations silos that existed previously, and often stalled software development, and introduced errors. It was found that co-operation between the teams and the breakdown of traditional IT roles helped facilitate the desired CI/CD framework as developers became used to agile turnaround and rapid software delivery times.

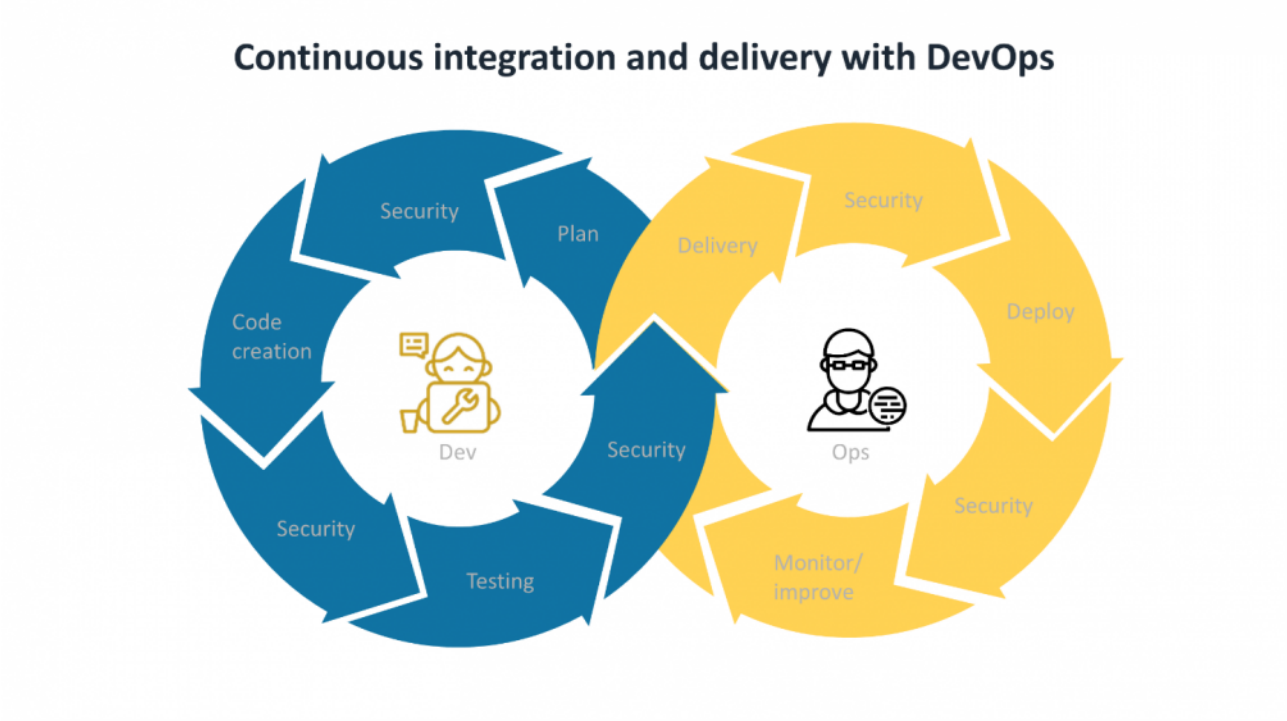


Figure 2: Transparent Security platforms including PAM must be embedded within the CI/CD lifecycle that DevOps teams work within.

Transparent Security platforms including PAM must be embedded within the CI/CD lifecycle that DevOps teams work within. A security feedback mechanism is also advisable to allow DevOps and other agile development teams to act quickly on vulnerabilities as they arise.

Why DevOps is now critical to managing privileged accounts in organizations

Those working in DevOps store, compile and test code that will involve privileged access to specific data sources, tools, applications and other resources that are classified as confidential, and must be kept secure. Today, this will include individual pieces of code, containers, and APIs as well as discrete data that relates to company projects or individuals.

DevOps will access and process privileged data and entities on a continuous basis. Without a platform to monitor, record and control this access, countless vulnerabilities will be introduced every day. For example, developers committed to their job, will often perform actions that make their operations quicker but introduce security risks. They may locally store or share credentials to privileged tools and data or embed them within an application or container they are working with. Developers may share passwords and code, and admins may allow privilege to users on an ad hoc bases – a process known as privilege creep.

The challenge is finding a PAM solution that can work at the pressure and speed that DevOps already work to and keep all secrets secure. It must not get in the way - it must be secure and accountable through integrated tools or via third-party integrations. In this Leadership Compass we assess those PAM vendors that are addressing the needs of DevOps and agile environments. Some are offering DevOps capabilities as

an add-on to existing suites, while others offer specific authentication toolsets that work well with providing privileged access to DevOps teams and non-human users. Currently vendors offer traditional vaults or certificates to authenticate users within the DevOps environment (see Figure 3).

1.2 Delivery models

This Leadership Compass is focused on PAM products for DevOps that are offered in on-premises, in the cloud or as-a-service (PAMaaS) by the vendor.

1.3 Required capabilities

At KuppingerCole we believe that the following capabilities are essential if PAM is to meet the demands of DevOps and other agile development environments.

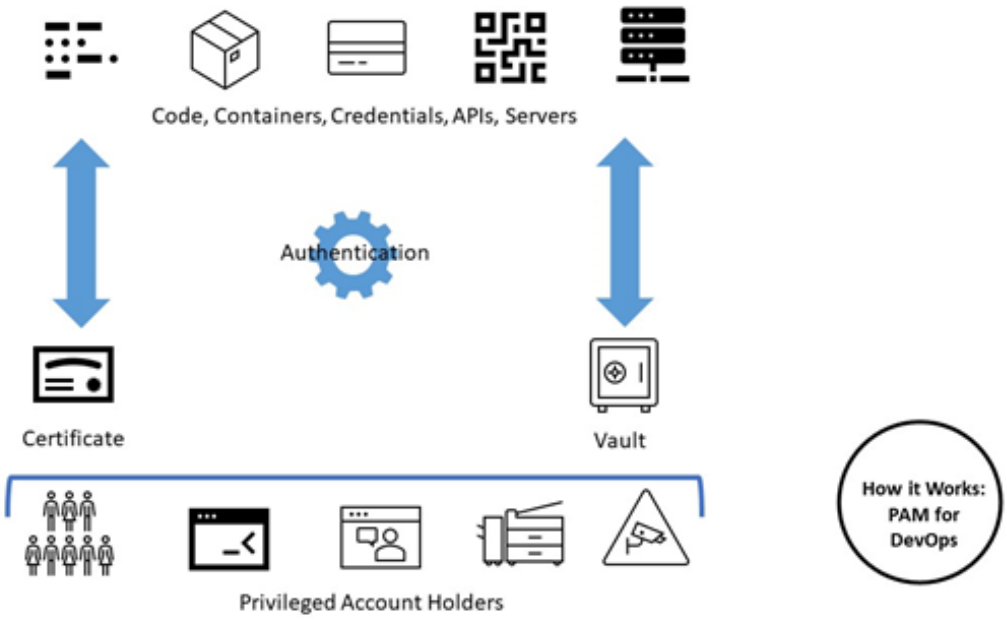


Figure 3: PAM for DevOps currently offers the choice of certificates or encrypted vaults to authenticate access.

1.3.1 Toolchain support

Efficient DevOps teams will want to use the most effective set of tools for developing and delivering applications. Such tools can comprise of code, artifacts, applications and other essential components. These are always likely to be components of strategic business value that qualify for privileged access only. Any PAM for DevOps solution should be able to provide fast and secure access to Toolchain components wherever they reside in the IT environment.

1.3.2 Runtime support

Developers who wish to run apps in containers and elsewhere may not always have written all the code to fully execute. Therefore, they need access to runtime code to compete the job, and PAM must provide and protect the access needed to runtime.

1.3.3 Finished application support

One of the guiding principles of DevOps is support for CI/CD and to provide fast updates to applications, particularly when bugs or vulnerabilities may arise after code hits production. The best people to fix code are those who developed it in the first place, but obviously access to live code must be on a strictly privileged basis. This can also work in conjunction with specialist application lifecycle applications designed to assist developers find and sort applications rapidly.

1.3.4 Certificate support

While PAM has traditionally relied on an encrypted vault to store and manage passwords for authentication and access to privileged data and tools, the more intense and ephemeral nature of the DevOps environment is leaning toward the issue of one time only public key certificates for authentication of privileged users (see Figure 3).

1.3.5 Base PAM support

While authentication of privileged accounts is of paramount importance within the DevOps environments to ensure users get access to the tools they need, this should also be backed up with the regular features of PAM such as session management and recording, therefore it is advisable to either add a PAM solution to

DevOps that can integrate with legacy PAM platforms or to buy PAM that does both from the same platform. (See Section 1.4 Other capabilities to support DevOps)

1.3.6 High Availability (HA)

Having a method of accessing vaulted PAM accounts in an emergency is important for all PAM deployments but in the high stress, high strategic value DevOps it is more so. Developers being locked out of tools and runtime support will result in lost revenue and expensive downtime. Tools should be in place to conduct break glass procedures without compromising the integrity of DevOps or wider organization.

1.3.7 Non-human user support

Integral to digital transformation is the communication between machines and applications, and to other applications, data centres and databases to get business-related information. This is a key part of the DevOps process as developers use automaton tools to complete tasks. Some will require privileged access but time constraints on processes means it needs to be seamless and transparent as well as secure.

1.3.8 Shared account support

Best practice demands that organizations switch to single identity privileged accounts, but shared privileged accounts still exist in many organizations and remain a risk to security if not monitored. Shared accounts are a feature of DevOps and until they can be safely eradicated it is important that PAM for DevOps can manage and record usage securely.

1.3.9 Just in Time (JIT)

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

1.4 Other capabilities to support DevOps

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

1.4.1 Privileged Account Data Lifecycle Management (PADLM)

The usage of privileged accounts must be governed as well as secured. A discovery mechanism to identify shared accounts, software accounts, service accounts and other unencrypted/clear-text credentials across the IT infrastructure is included in some PAM solutions. PADLM tools offer workflow capabilities to identify and track the account's business and technical ownership throughout its lifecycle and can detect changes in its state to invoke notification and necessary remedial actions.

1.4.2 Controlled Privilege Elevation and Delegation Management (CPEDM)

This is another important function related to the fluid and fast changing needs of digital organizations. As the name suggests it allows users to gain elevation of access rights, traditionally for administrative purposes and for short periods typically, and with least privilege rights. However, some vendors are adapting the traditional role of CPEDM to become more task focused and adaptable to more flexible workloads that modern organizations require – such as DevOps. This is known as Privileged Task Management (PTM), enabling least privilege access to resources to get things done. Such processes can be pre-assigned for distribution or may well be a response to a specific request. The challenge for all PAM vendors is to integrate CEPDM and PTM securely and transparently. Inevitably, some will do it better than others.

1.4.3 Endpoint Privilege Management (EPM)

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

1.4.4 Session Recording and Monitoring (SRM)

SRM enables more advanced auditing, monitoring and review of privileged activities during a privileged session, including key-stroke logging, video session recording, screen scraping, OCR translation and other session monitoring techniques.

1.4.5 Privileged Single Sign-On (SSO)

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

1.4.6 Privileged User Behaviour Analytics (PUBA)

PUBA uses data analytic techniques, some assisted by machine learning tools, to detect threats based on anomalous behaviour against established and quantified profile behaviour of administrative groups and users.

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

- Privileged IT task-based automation is a new feature that brings PAM to more granular level by combining JIT access to specific tasks, often one time only. While integration with existing PAM solutions is currently limited, this is likely to change.
- Remote access for end users to privileged accounts is more relevant in digital environments. PAM solutions will increasingly support this in the future to help secure access for third parties such as customers and vendors, as well as remote workers.
- Privileged Access Governance (PAG) deals with offering valuable insights related to the state of privileged access necessary to support decision making processes in the organization. PAG can include privileged access certifications and provisions for customizable reporting and dashboarding.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

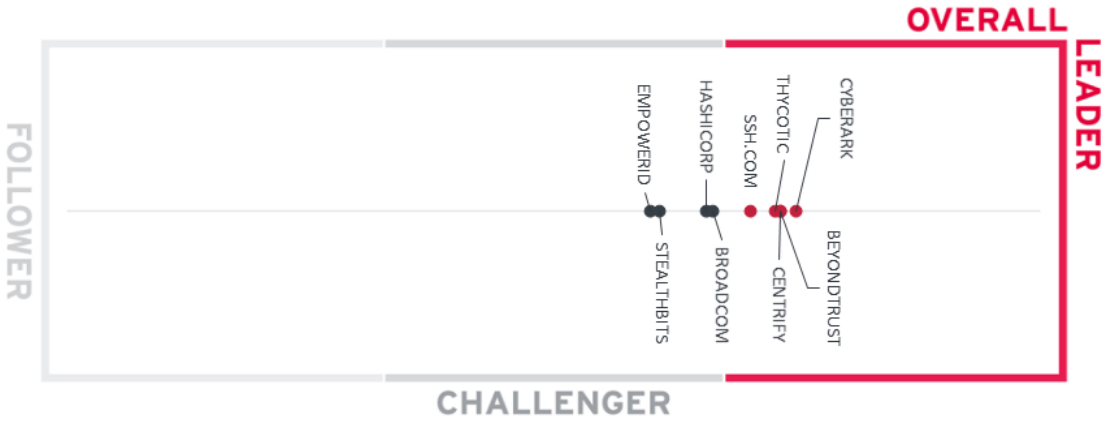


Figure 4: The Overall Leadership rating for the PAM DevOps market segment

The five vendors that comprise the Overall Leaders are well established brands: BeyondTrust, Centrify Corporation, CyberArk, SSH Communications Security (SSH.COM) and Thycotic Software, and it is no surprise that the same five that lead the PAM market generally are also leaders here. With the focus on DevOps the five are clustered much closer together and this demonstrates that the market leaders are actively investing in DevOps capability as part of their portfolio and are taking the demand seriously – but none yet has breakout technology. All five have ensured that this is not just marketing but of actual benefit

to DevOps people and environments. This is good news for the PAM market and for those organizations that may be looking for hybrid PAM deployments to cover DevOps or multi-cloud environments (or both) – as where the market leaders go, others are likely to follow. What all this means is that the PAM market is changing, and customers are starting to look for options that meet less homogeneous demands within their organizations.

Among the Challengers we see four vendors that are looking also to meet the demand for better privilege management in DevOps but in different ways: Broadcom, HashiCorp, Stealthbits Technologies, and Empower ID. Within this disparate group we find one company not traditionally considered a PAM vendor: HashiCorp, but like SSH.COM, it offers an individual, lean technology that suits DevOps well for certain applications.

Overall Leaders are (in alphabetical order):

- BeyondTrust
- Centrify Corporation
- CyberArk
- SSH.COM
- Thycotic Software

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

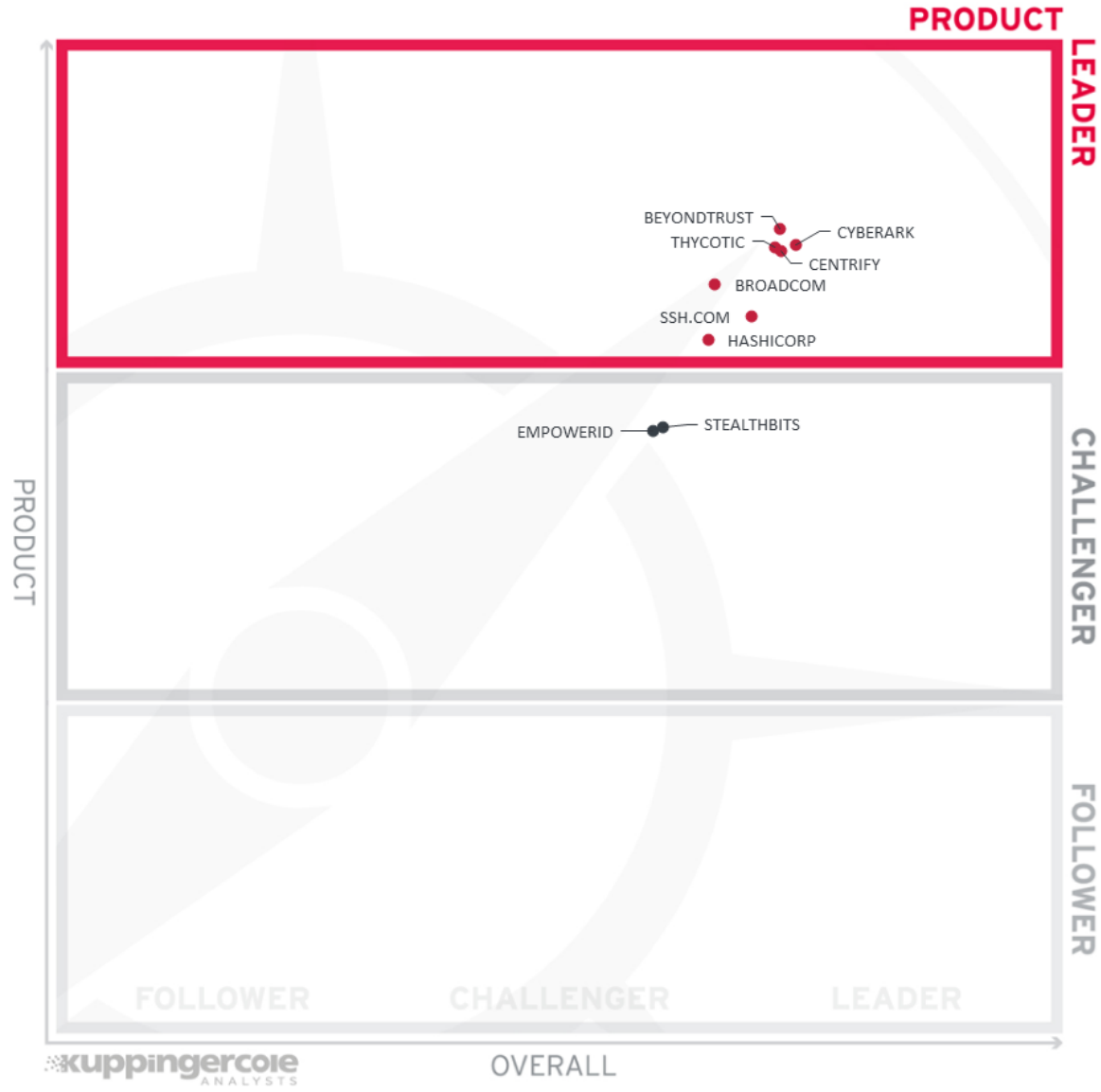


Figure 5: The Product Leadership rating for the PAM DevOps market segment

In the Product Leader category, we see the same five Overall Leaders joined by one giant, Broadcom, and one much smaller but innovative company – HashiCorp. Since Broadcom acquired CA Technologies' PAM platform the company has moved to consolidate and improve its market position. Its sheer size and financial clout make it a contender in the market, but it does offer some serious technical options to those looking for a PAM solution to assist with DevOps. HashiCorp is a very different company but HashiCorp Vault is now being slowly integrated into two new identity management platforms from the company, thus expanding its reach.

The Leaders are challenged by Stealthbits Technologies and EmpowerID. There are no Followers in this

category, which suggests that customers can buy with confidence that all these solutions will offer some form of DevOps capabilities that may meet individual needs.

Product Leaders (in alphabetical order):

- BeyondTrust
- Broadcom
- Centrify Corporation
- CyberArk
- HashiCorp
- SSH.COM
- Thycotic Software

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

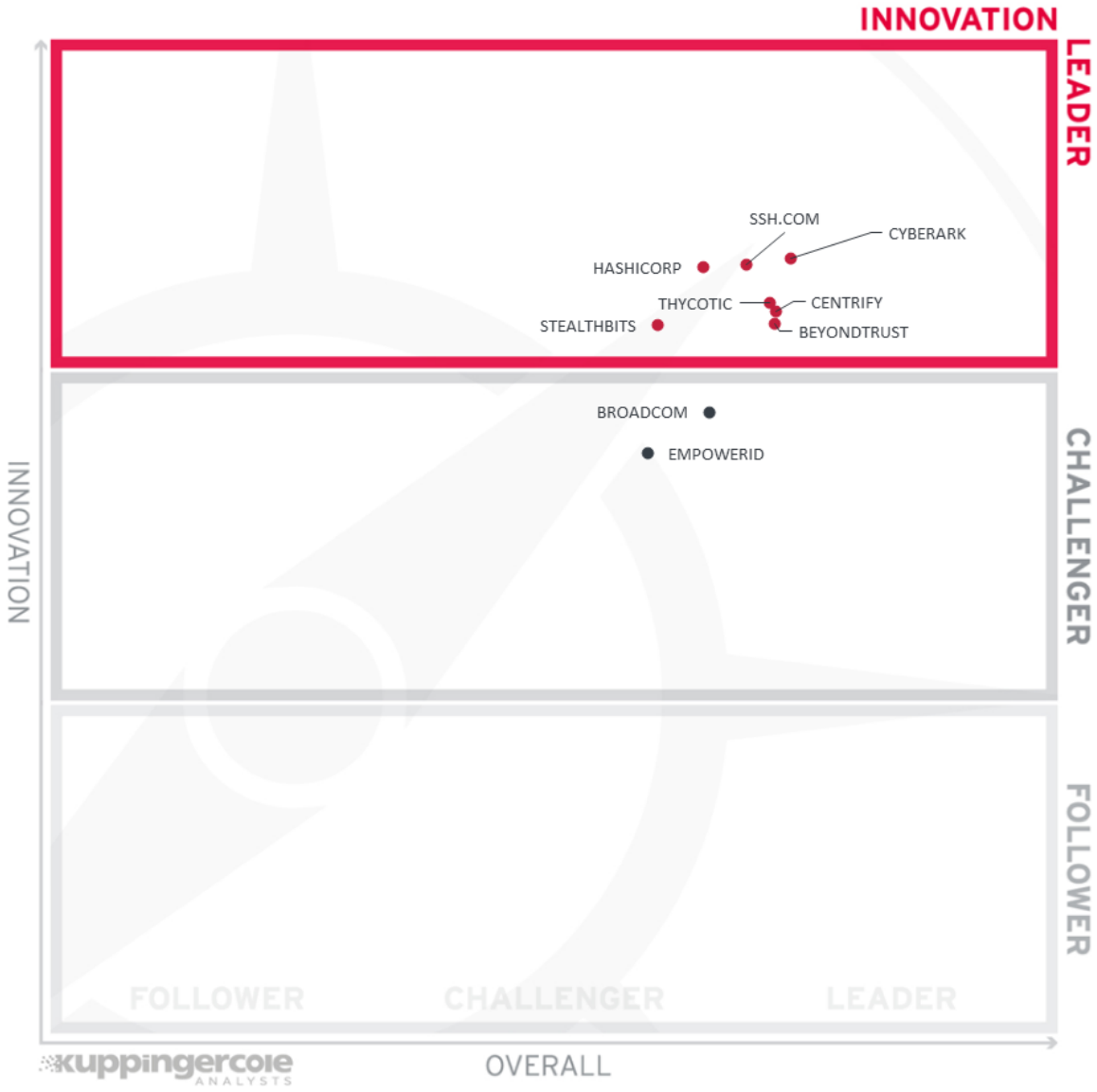


Figure 6: Innovation Leaders in the PAM DevOps market segment

This section is most interesting as Innovation is key to creating PAM that works well in DevOps environments. We have seven Leaders now: CyberArk, BeyondTrust, Centrify Corporation, HashiCorp, SSH.COM, Stealthbits Technologies, and Thycotic. The positioning is narrow, suggesting no vendor has the edge in innovation but the presence of traditional players is another sign that market leaders are taking the right steps to ensure their platforms can meet emerging challenges for PAM. The presence of Stealthbits Technologies and HashiCorp among the Leaders shows that they cannot afford to rest on their laurels, however.

There are no Followers again, demonstrating that all vendors in this Leadership Compass are there for a

good reason – they have indeed innovated to stay ahead. The Challengers are Broadcom and EmpowerID.

Innovation Leaders (in alphabetical order):

- BeyondTrust
- Centrify Corporation
- CyberArk
- HashiCorp
- SSH.COM
- Stealthbits
- Thycotic

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

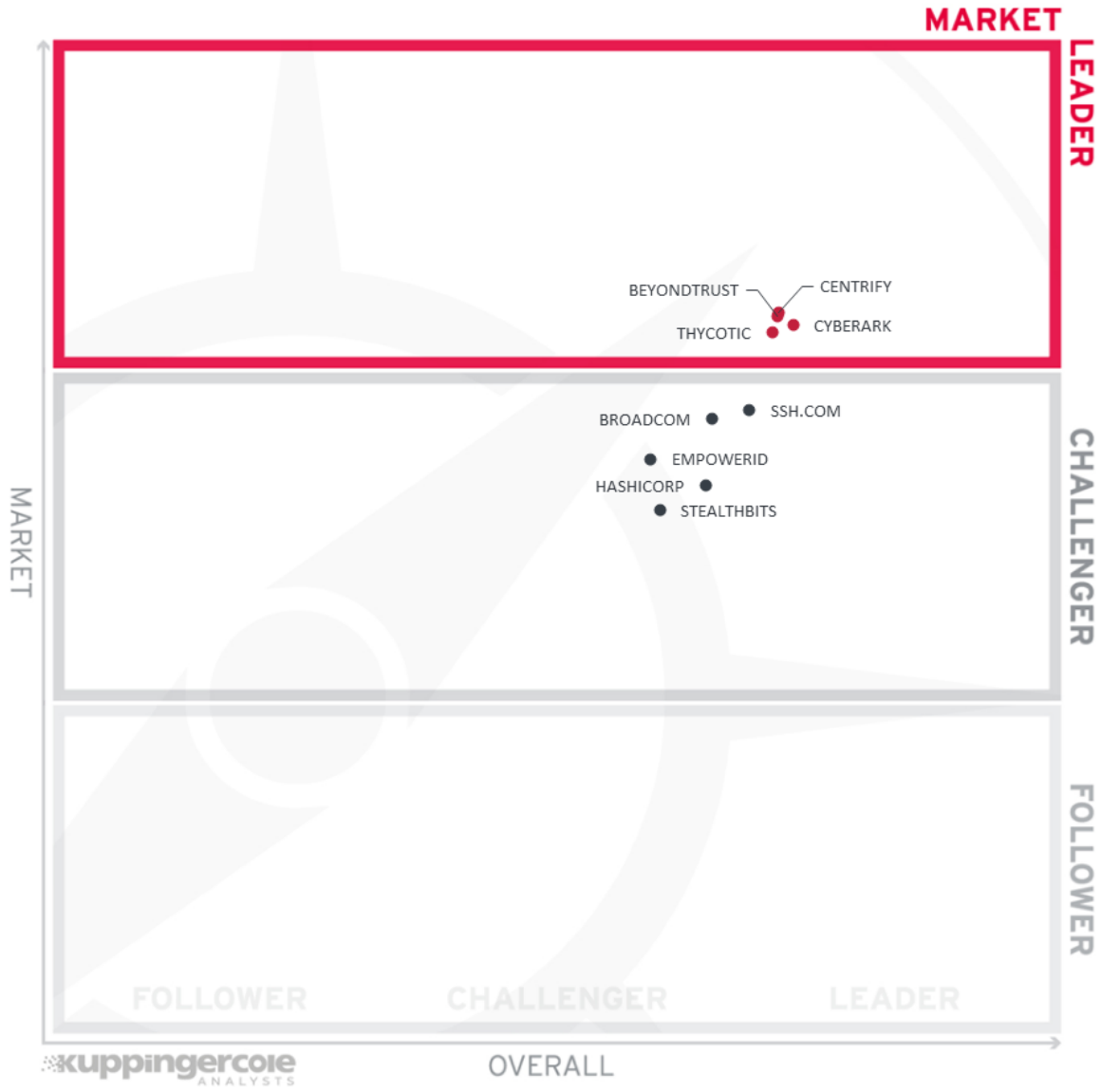


Figure 7: Market Leadership in the PAM for DevOps Leadership Compass

The results of this section are unsurprising. Centrify, BeyondTrust, CyberArk and Thycotic form a tightly knit group which accurately reflects their market reach and number of customers and identities managed. Such tight positioning reflects the competitiveness among the four that have added DevOps capabilities in recent years. In the Challengers section we see Broadcom, EmpowerID, HashiCorp, Stealthbits Technologies, and SSH.COM evenly spaced. While Broadcom has the resources of a global IT vendor, its presence in the PAM market is yet to match the market leaders.

Market Leaders (in alphabetical order):

- BeyondTrust
- Centrify Corporation
- CyberArk
- Thycotic Software

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 8: 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 “overperformers” when comparing Market Leadership and Product Leadership.

The results in this sector need some explaining in the light of PAM for DevOps. The Market Champions are the familiar Big Four of CyberArk, Centrify Corporation, BeyondTrust and Thycotic but below them is where the interest begins. Broadcom, HashiCorp, Stealthbits Technologies and SSH.COM are all underperforming in the market for PAM for DevOps which suggest they need to do more to market or package their innovative efforts to manage privileges in DevOps environments. HashiCorp is already making progress in this area, Broadcom is busily repackaging its PAM solution under the Symantec brand. We expect

SSH.COM, EmpowerID, and Stealthbits to also do more as the market matures.

3.2 The Product/Innovation Matrix

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

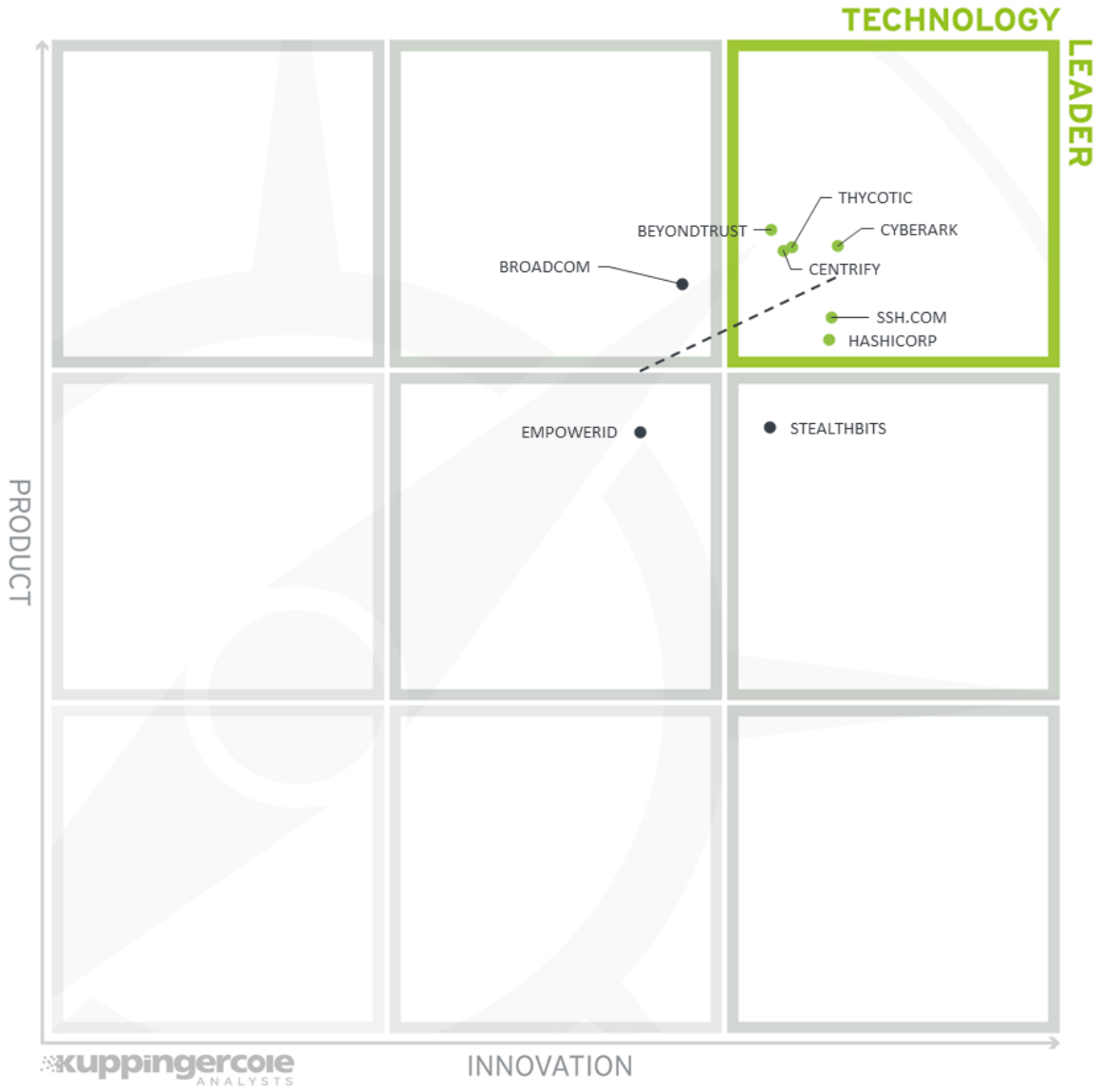


Figure 9: The Product/Innovation Matrix

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

In this matrix we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find the leading vendors in the upper right corner, clustered quite closely together but joined by Broadcom in the top center. The remaining vendors both fall within the following two middle squares. Therefore, customers can be confident that any of these may be a good choice depending on the level of DevOps privilege that needs managing.

3.3 The Innovation/Market Matrix

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

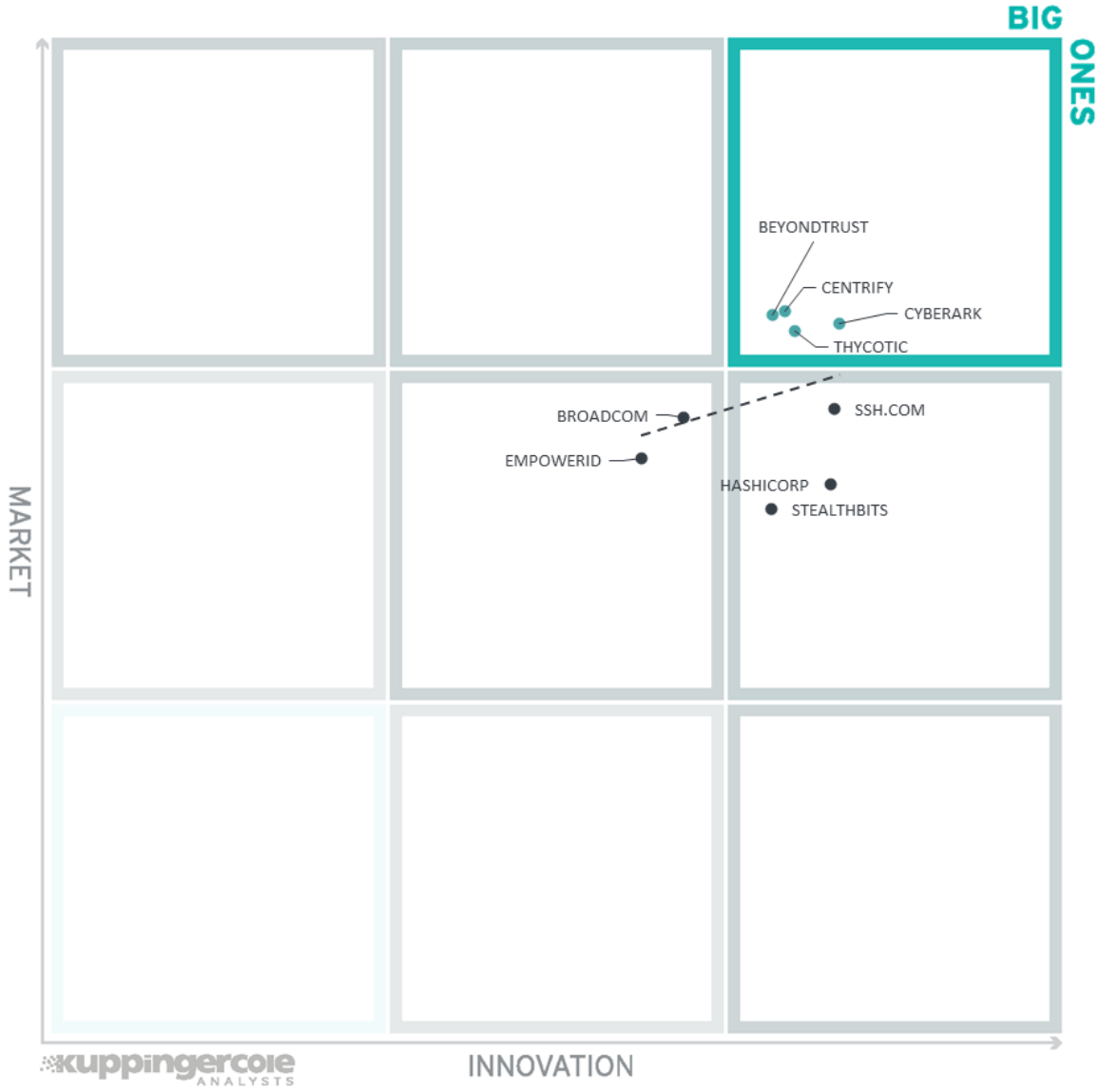


Figure 10: The Innovation/Market Matrix

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

The breakdown here shows that the smaller vendors SSH.COM, HashiCorp and Stealthbits are outperforming bigger rivals in absolute innovation for DevOps. However, the established leaders are innovating too – especially CyberArk – and that innovation is backed up by strong, fully loaded PAM platforms with proven base technology including Session Management, CPEDM and other tools.

4 Products and vendors at a glance

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

Ratings at a glance

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

Product	Security	Functionality	Interoperability	Usability	Deployment
BeyondTrust PAM	●	●	○	●	●
Centrify Zero Trust Privilege Services	●	●	○	●	●
CyberArk PAM	●	●	○	●	●
EmpowerID PAM	●	○	●	●	●
HashiCorp Vault	○	○	○	●	○
SSH.COM PrivX	●	○	○	●	●
STEALTHbits Privilege Activity Manager	●	○	○	●	○
Symantec Privileged Access Manager	●	○	○	●	○
Thycotic Secret Server	●	●	○	●	○
Legend		● critical	● weak	● neutral	○ positive	● strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
BeyondTrust	strong positive	strong positive	strong positive	strong positive
Centrify	positive	strong positive	strong positive	strong positive
CyberArk	strong positive	strong positive	strong positive	strong positive
EmpowerID	positive	positive	positive	positive
HashiCorp	strong positive	positive	positive	positive
SSH Communications Security	strong positive	neutral	neutral	positive
STEALTHbits Technologies	positive	positive	positive	neutral
Symantec	positive	strong positive	strong positive	strong positive
Thycotic	positive	strong positive	positive	positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/service evaluation

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

Spider graphs

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

- Toolchain support
- Runtime support
- Finished app support
- Certificate support
- Base PAM support
- High availability
- Shared accounts
- Non-human user support

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

5.1 BeyondTrust

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

BeyondTrust's main suite of products is now streamlined for Privileged Password Management, Endpoint Privileged Management and Secure Remote Access. Password management is provided by two key solutions: Password Safe (formerly PowerBroker), and DevOps Secrets Safe.

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

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

BeyondTrust is aware of the need to support PAM for DevOps. However, its approach has gone beyond paying lip service with existing functionalities and it offers a whole new vault dedicated to DevOps and agile environments. DevOps Secrets Safe goes beyond securing passwords and stores secrets used by applications, tools and other non-human identities such as Kubernetes service accounts. BeyondTrust also supports native integration with DevOps tools such as Jenkins, Puppet, and Chef, while Password Safe now supports better protection for shared credentials for DevOPs and QA teams with a view to improving productivity in agile environments. These are all good developments.

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

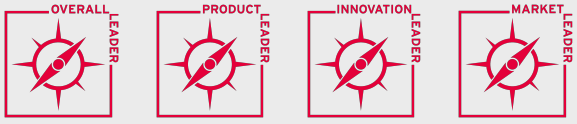
Strengths

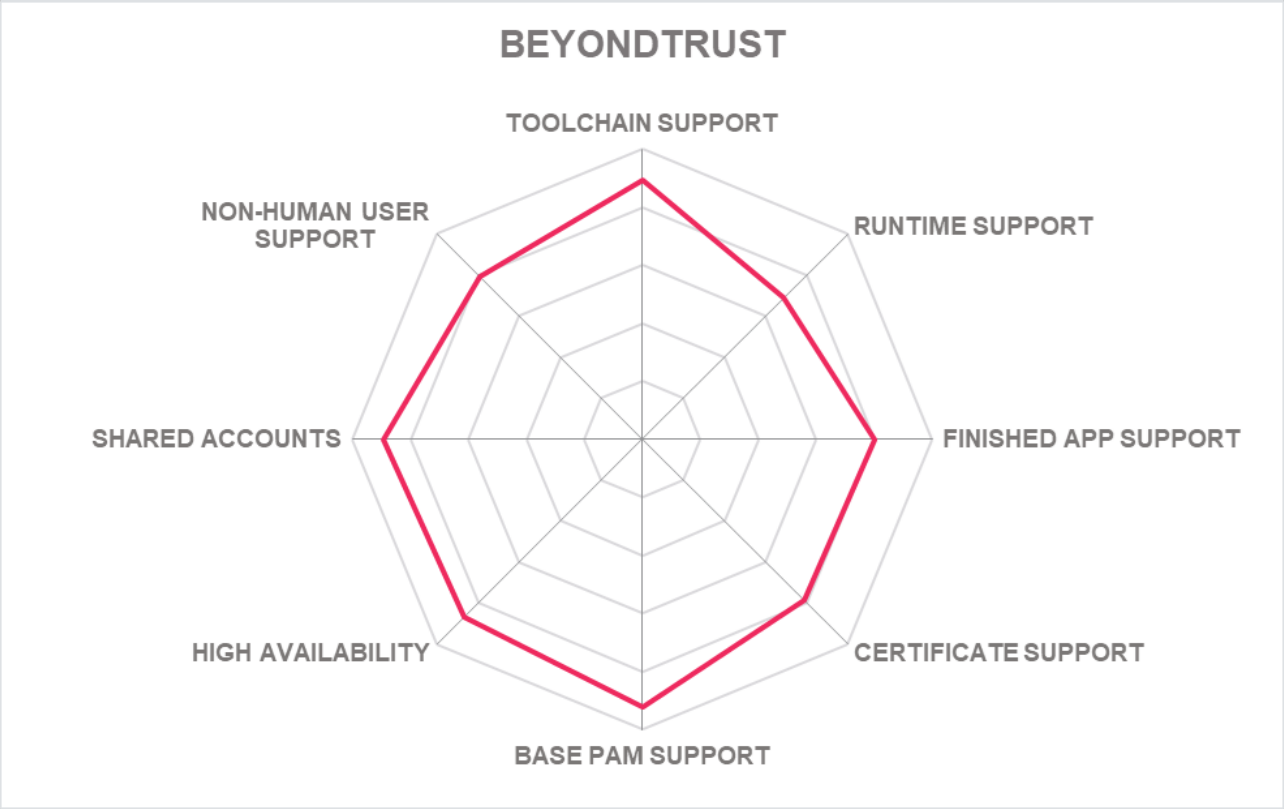
- Acquisitions now much better integrated making this a viable joined-up PAM suite
- Has taken support for DevOps further than some rivals
- Host-based approach for CPEDM delivers strong and granular command control for privilege elevation
- Ability to mix and match solutions across three main categories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

Challenges

- BeyondTrust dedicated vulnerability management tool has now gone EOS
- Much improved but vendor website can still make it hard to find specific products for PAM challenges
- DevOps Secrets Safe available as SaaS would be a plus for BeyondTrust

Leader in




BEYONDTRUST
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.2 Centrify

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

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

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

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

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

Centrify has strong DevOps credentials. It already gives DevOps tools direct access to the Centrify vault to retrieve credentials or ephemeral tokens, but the company has embraced the challenge of infrastructure as code environments. Centrify Delegated Machine Credentials allows developers to utilize trusted ephemeral tokens to lower the total amount of service accounts thereby decreasing risk and easing manageability for developers. Centrify also supports DevOps deployment operations (Cookbooks and playbooks for Ansible, Chef, Puppet, Salt, and Terraform) for all Centrify components.

There is strong integration into the DevOps pipeline and SSH key management is now included. Centrify can remove Secrets/Keys/API keys with JIT-focused ability to automate identity-centric PAM and machine credentials instead of stored secrets. Uniquely, Centrify has a helper program to accelerate scripting and access to end-to-end API capabilities without a deep understanding of Centrify APIs needed by the user. Finally, there is tooling for PowerShell, Python, Java, C/C++, C#, Node, Ruby, and JS interfaces further extending into the DevOps tool chain using native languages.

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

Centrify
ZERO TRUST PRIVILEGE

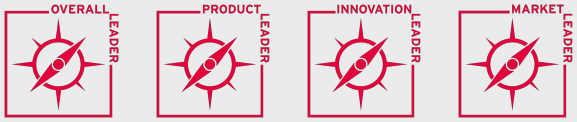
Strengths

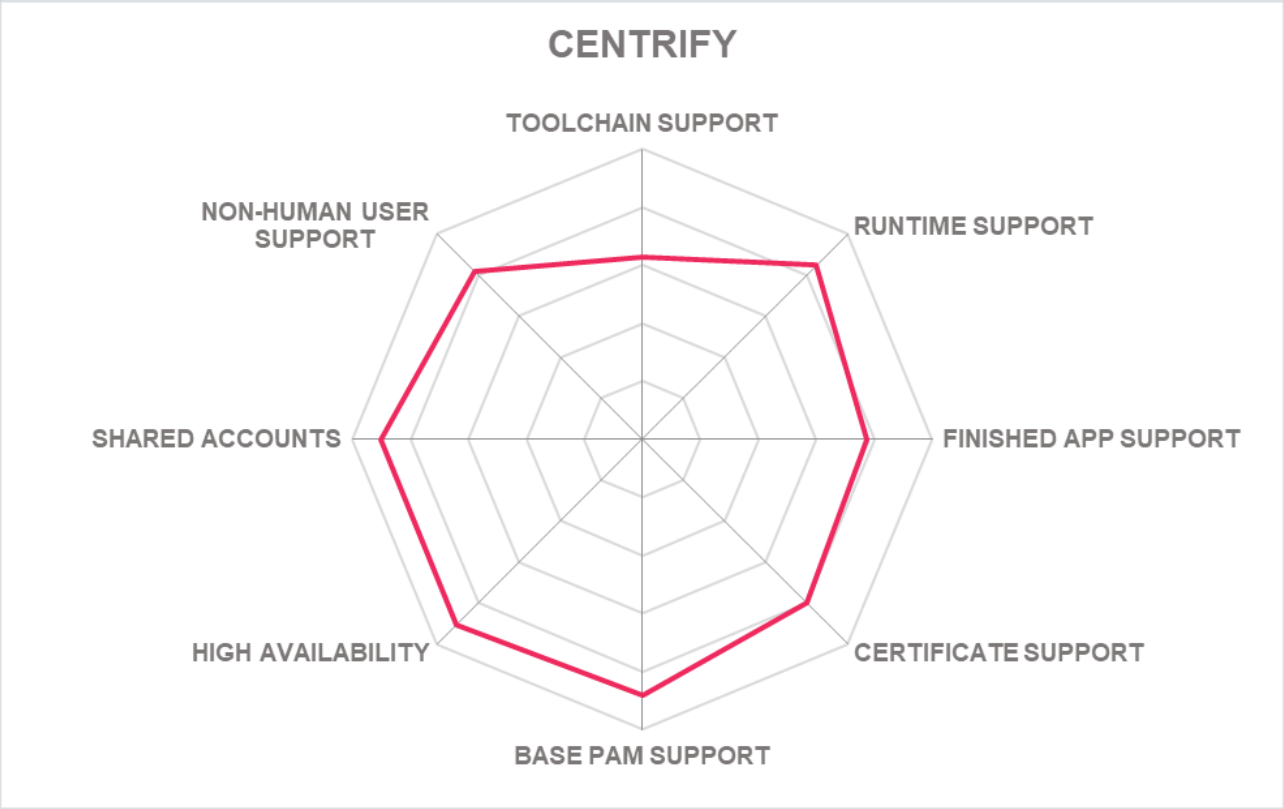
- Deep AD integration supporting complex multi-domain/ forest configurations
- Strong MFA and identity federation support with risk adaptive capabilities
- Strong CPEDM support
- Mature PAM as a Service offering in addition to a managed, on-premises delivery
- Strong privileged analytics with advanced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

Challenges

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

Leader in




CENTRIFY
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.3 CyberArk

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

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

CyberArk says that buyers often start off with its basic PAM module and then move onto more advanced solutions as needs change – while this enables customers to use a single solution to centrally manage privileged credentials across the entire enterprise, it also locks buyers at an early stage into one PAM ecosystem making it harder to change the more you invest.

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

CyberArk has made advances in providing PAM for new agile environments and DevOps. CyberArk Conjur provides secrets management across native cloud, DevOps, containerized and other dynamic environments enabling developers to secure and manage secrets used by users, applications, microservices, containers, automation tools and APIs etc. throughout the DevOps cycle. CyberArk continues to offer in-depth analytics, session management, elevation management and AAPM technologies across its suite of products. It also offers integrations for a wide range of third-party applications, DevOps tools and container platforms. CyberArk is doing much to ensure its solutions are ready for the next set of privileged access challenges related to digital transformation across many organizations. There is now an open-source version of Conjur along with technical content for the developer community.

CyberArk is also working on expanding PAMaaS for DevOps -- future versions of Conjur will offer a hybrid SaaS approach to centrally manage credentials in the cloud, while ensuring credentials, such as Kubernetes Secrets are locally available to ensure high availability in the event of a network or cloud failure.

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

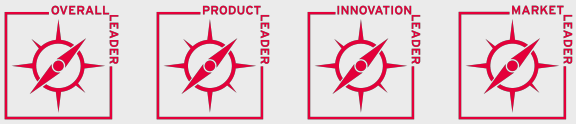
Strengths

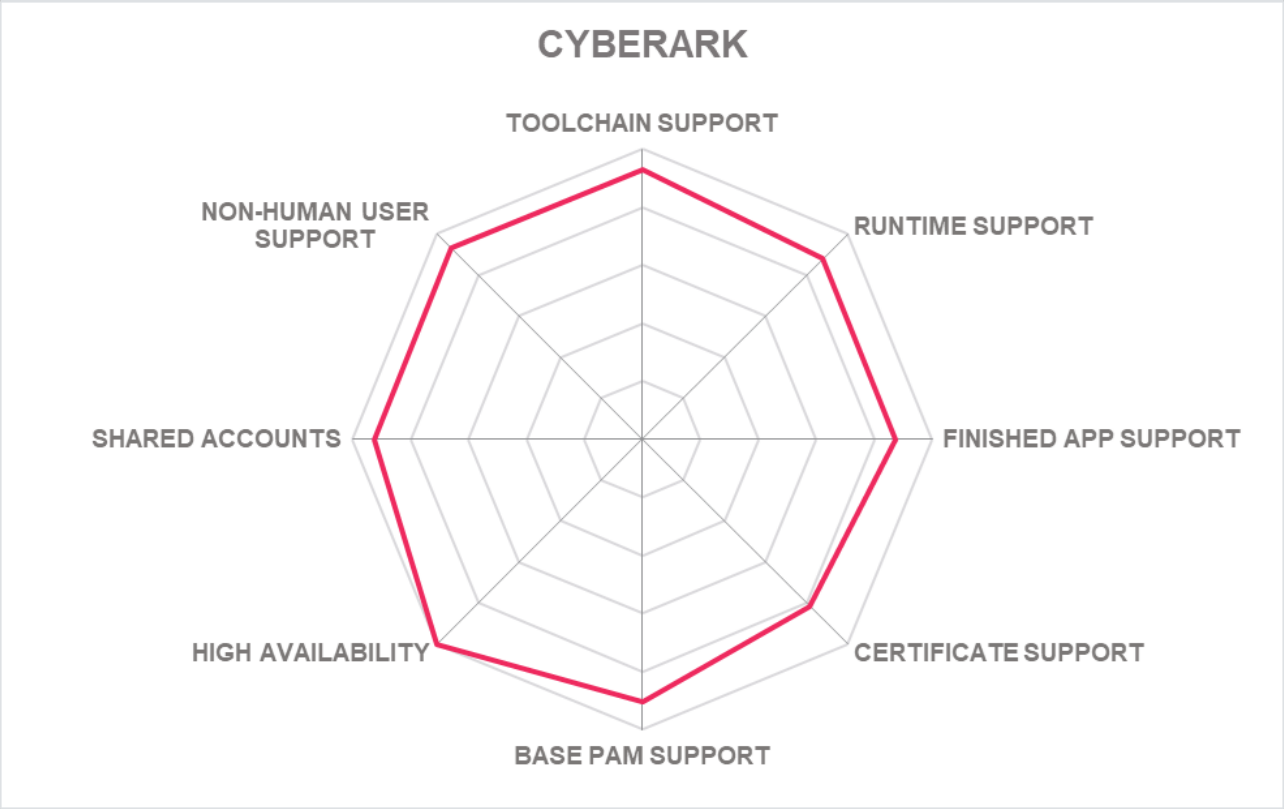
- One of the widest support levels for platforms and deployments
- Has continued to add features in the last year
- Intuitive and robust UI design
- Strong threat analytics capabilities offering real time threat detection and remediation
- Effective and clearly thought-out DevOps support
- Broad support for cloud applications and infrastructure
- A strong and functional partner ecosystem

Challenges

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

Leader in




CYBERARK
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.4 EmpowerID

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

The product is completely workflow based which EmpowerID claims is unique. It has a drag and drop creation of forms capability and 1,000 ready-made workflows ship with the product to get started. It uses conventional vault technology which hides passwords from users in RDP, SSH or web browser SSO. All privileged sessions are recorded. However, as a complete PAM solution, it only really lacks PUBA as one of the key functions and has good support for AAPM and JIT which is of use to agile environments but not yet DevOps or microservices specific.

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

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

Reporting is good with real-time alerts inform key personnel of critical activities such as privileged account usage, password changes, lockouts, and changes to sensitive group membership. Advanced analytics is less sophisticated although security admins and auditors can view actionable intelligence on the go from their mobile devices or subscribe to reports. EmpowerID is adding DevOps capability by extending the Policy Based Access Control (PBAC) authorization engine integration with the Open Policy Agent for Kubernetes and enabling microservices policy decisioning and enforcement using its KONG-based Application Gateway. The company is also extending its integration with microservices "secret" vaults in line with a projected shift to microservices where machines and identities are ephemeral and distributed, with limited inbound access to those systems. The product does a good job of complementing EmpowerID's existing IAM products and adds PAM to those. It is basing its development roadmap on Kubernetes and microservices which should make for an interesting development in our next assessment.

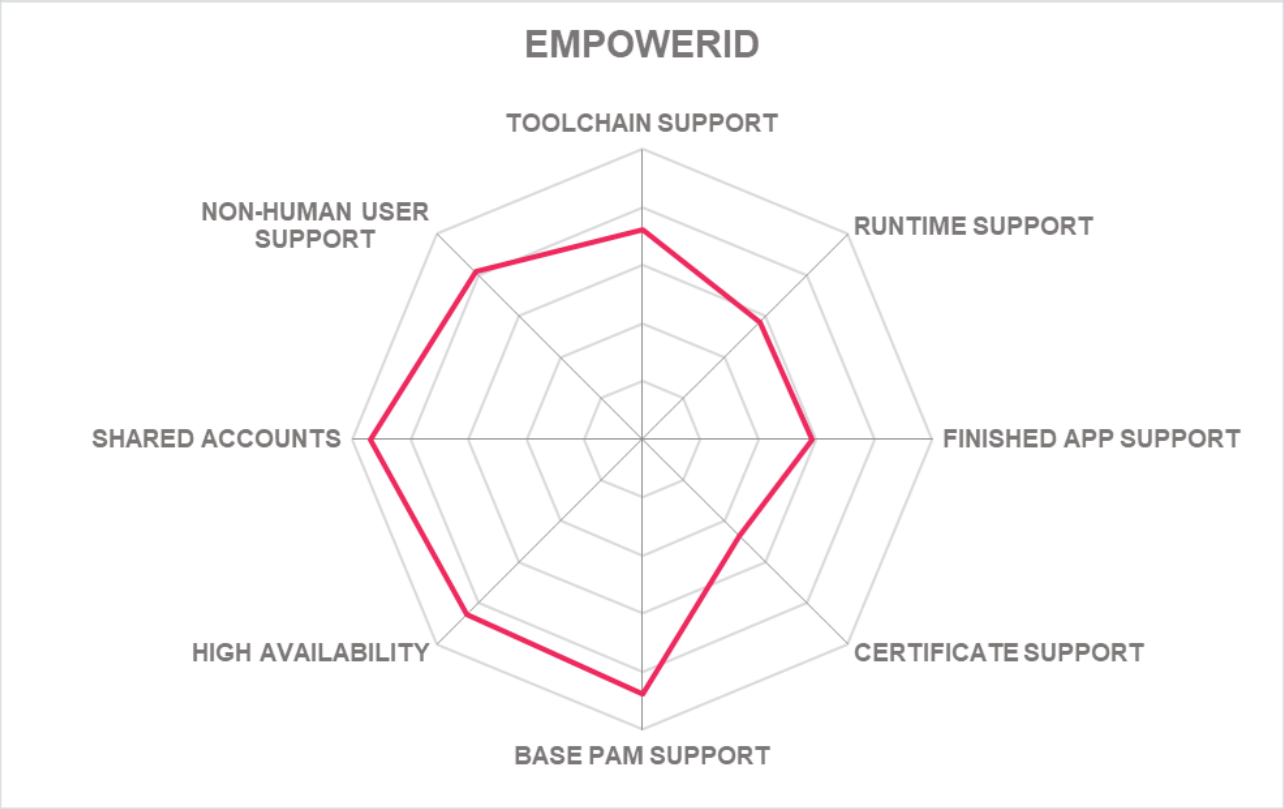
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●○○

Strengths

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

Challenges

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


EMPOWERID
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.5 HashiCorp

HashiCorp is a provider of multi-cloud infrastructure automation software for cloud and on-premises environments. Built on an open-source foundation, HashiCorp Vault securely manages secrets and protects data for both open-source users and enterprise customers. Vault is part of the HashiCorp product suite built around infrastructure automation and secure workloads across on-premises and public and private clouds and provides a tightly integrated DevOps platform based on the principle of Zero Trust. HashiCorp Vault secures, stores, and tightly controls and monitors access to tokens, passwords, certificates, and encryption keys. It saw almost 16 million downloads in 2020.

HashiCorp Vault is offered in three variants aimed at individuals, teams, and enterprises. While the core features such as dynamic secrets, encryption, secure storage, key rotation, vault agent, access control policies and credential checkout workflows are included in all the three vault variants, MFA, governance and features necessary to support multi-datacenter environments such as disaster recovery and replication are only available as part of team and enterprise versions — which makes sense. For those looking for a traditional PAM platform, in October of 2020, HashiCorp launched Boundary, a new open-source product that focuses on simple and secure remote access, allowing users to access any system from anywhere. Boundary integrates with Vault for secret injection, so users don't have to manage or be exposed to credentials and sensitive data.

However, HashiCorp is now offering HashiCorp Vault as part of its wider HashiCorp Cloud Platform introduced in June 2020 and designed to offer an easy to deploy cloud security platform that incorporates PAM. The platform is initially available directly on AWS. As part of this platform, HashiCorp Consul helps make sense of machine communications and workflows on Service Mesh architecture.

HashiCorp Boundary offers identity-based secure, remote access controls across the kind of environments that DevOps people will need such as Kubernetes, cloud resources clusters and on-prem data centers. There is also session management and auditability built in. While HashiCorp Vault already offers a viable and lean solution for DevOps, the entry of the new platforms should give bigger rivals pause for thought. HashiCorp has addressed one of the key challenges of PAM for DevOps – maintaining speed of access for agile teams within secure workflows and a platform base can only enhance its appeal.

HashiCorp Vault offers secrets management and secure Application to Application Password Management (AAPM) capabilities to support enterprise DevOps initiatives. While several other PAM vendors are now offering similar capabilities to suit DevOps, HashiCorp offers a good start for organizations looking to onboard PAM with the application development and deployment processes and addressing those workflow issues so critical to DevOps.

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

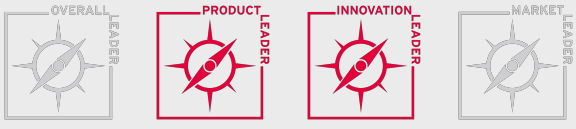
Strengths

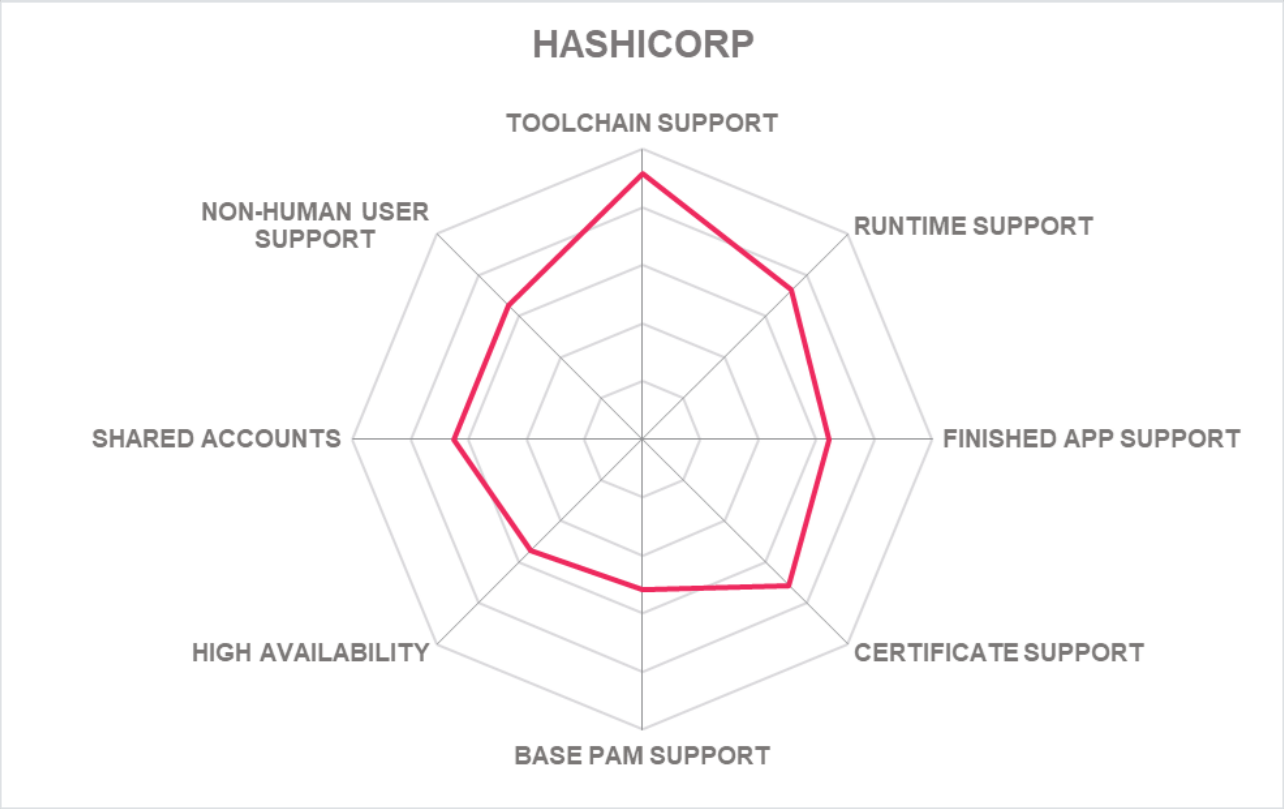
- An understanding that DevOps needs speed of access and simplified workflows as much as secure secrets
- Lean, easy to deploy and use
- HashiCorp adding Vault to a wider product platform will widen its appeal and gain new customers
- Can fill the workflow gap that some more conventional PAM platforms leave
- Wide support for SSO and MFA tools
- Allows customers the choice of passwords, keys and certificates or a combination
- Designed for multi-cloud environments

Challenges

- Still lacks many components to make it a full PAM platform but Boundary is a good start
- Some crucial features only available in Team and Enterprise editions
- Open-Source basis may impact on some enterprise security policies and governance rules

Leader in




HASHICORP
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.6 SSH Communications Security

Based in Helsinki, Finland, SSH.COM offers PrivX as its primary product in the PAM market. PrivX is a relatively new offering in the market by SSH.COM that attempts to offer an alternative to conventional shared account password management technology by providing a certificate authority based Just-In-Time access for SSH and RDP. Instead, PrivX by default dispenses with the need for a vault full of credentials and issues short-lived, or ephemeral, certificates for on-demand access.

It is an innovative approach (on the market since 2017) but one that does bring functional and security advantages – access is faster, onboarding and offboarding of privileged users is quick and there are no passwords to issue or lose, since there are no permanent left-behind credentials. Furthermore, users never handle or see any credentials or secrets at any point when accessing servers. Access is also based on roles to further restrict access to only those authorized.

SSH.COM has now introduced Secure Information Storage (vault) for customers that want it. Secrets are stored in JSON formatted data, and based on their role, users get access to the secrets. With HTTP(S) Web Gateway it is possible to manage access to critical web resources, including admin consoles of network devises, admin portals to a company's SaaS services or internal web tools, like Salesforce or Twitter.

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

While the core product is deliberately lean, it integrates with third parties to add functionality for SIEM ticketing systems and HSM. There is support for session recording and compliance, and recordings are encrypted. All SSH/RDP/HTTPS sessions are audited and logged and can also be recorded if needed for compliance, forensics or training purposes. PrivX also offers accountability of user activities even if admins are using shared accounts, since PrivX associates a user ID to every session. PrivX integrates with SIEM, and UEBA systems. Other important areas of functionality covered include SAPM, AAPM, PADLM, PUBA and CPEDM but traditional endpoint privilege management is missing here.
However, PrivX should reduce the need for traditional endpoint security. It completely isolates the user from the target – the user's own browser never touches the target system, minimizing the need for endpoint security. This applies to RDP, SSH, and HTTP(S) access.

PrivX is by its nature ideal for DevOps teams looking for privileged access with ephemeral certificate delivery at its core. Accounts are not accessible by any other means as there are no credentials available. Additionally, there is no need to make run-time changes in target hosts (immutable infrastructure). PrivX also supports integrations and plug-ins for different DevOps CI/CD pipelines and role-based access controls for container orchestration platforms. PrivX is available as Infrastructure as a Code (IaC) on AWS for fast deployment, natively taking advantage of the elements of cloud environments (scalability, backups, etc.).

With PrivX, SSH.COM presents a unique approach for managing certificates based SSH and RDP access

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

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

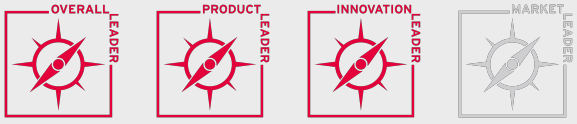
Strengths

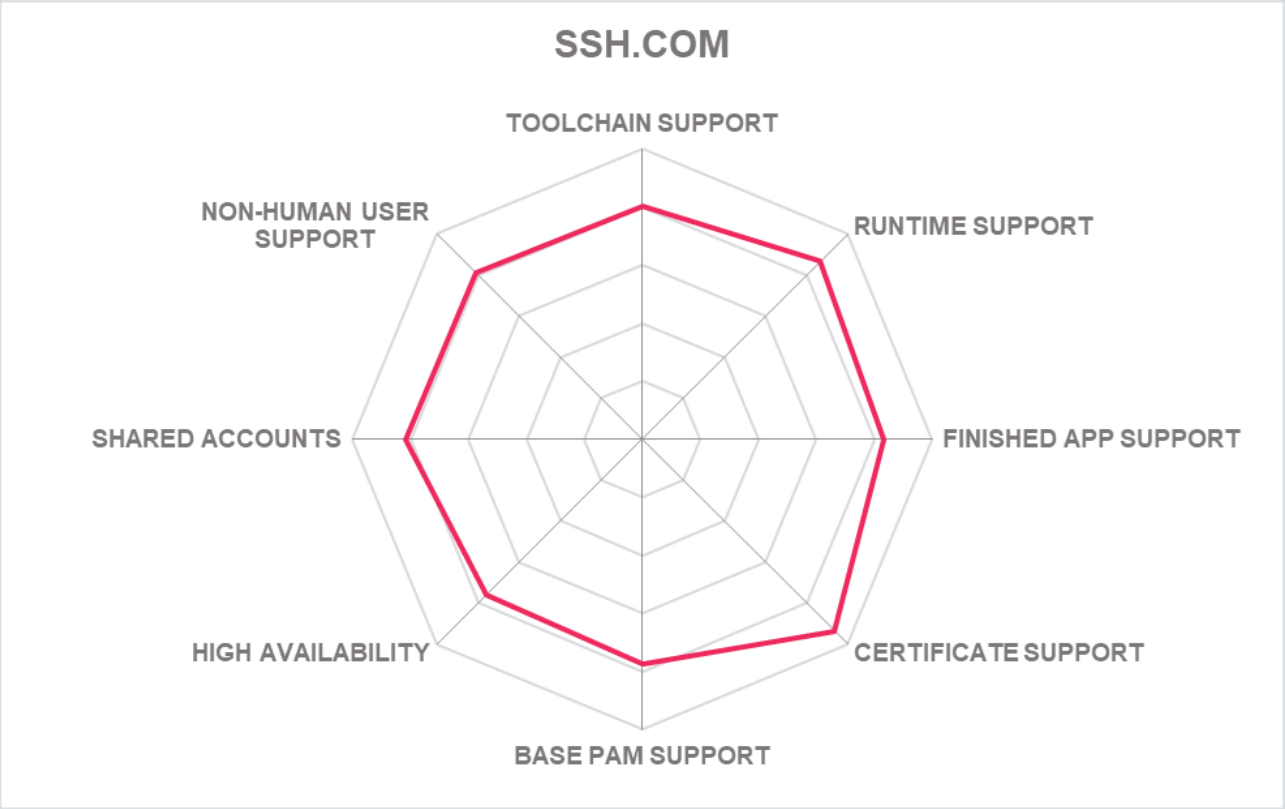
- Lean footprint and rapid access make it ideal for DevOps and agile environments
- Reduces one level of vulnerability by eliminating static passwords and vaults
- Eliminates the risk of redundant credentials being stolen or misused
- Quick deployment enhanced by the PrivX extender tool and IaC
- For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

Challenges

- Absence of traditional endpoint privilege management keeps the solution lean but may be missed by some
- Agentless approach may deter some buyers but good for DevOps applications in a multi-PAM environment
- Would like to see the SSH delivered SaaS version go beyond trial

Leader in




SSH.COM
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.7 STEALTHbits Technologies

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

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

The key is BYOV or Bring Your Own Vault. Customers have the option to integrate a third-party vault with a REST API, from several leading PAM providers including CyberArk, Symantec, BeyondTrust, HashiCorp (it also supports Microsoft LAPS).

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

The integrated JIT approach is well suited for DevOps. It creates accounts on the fly for any development lifecycle environment as applications move from dev to unit test, for example. The application needs only to request an account alias and SbPAM will create an account with just the right amount of permission at exactly the point it is required. This works for both application testing and orchestration integration into tools such as Ansible. Stealthbits plans to add scalable components to deliver credentials on the fly to CI/CD departments and add improvements to how containers and applications need to authenticate to release credentials.

The downside of this is that the product lacks some key capabilities that many organizations still need such as EPM, CPEDM and PADLM, especially for DevOps environments. But its task-based approach can work well with the traditional features of other PAM solutions, and it may well find a home in specific DevOps environments. In line with its DevOps targeted suitability, Stealthbits promises new releases of the product every three months.

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

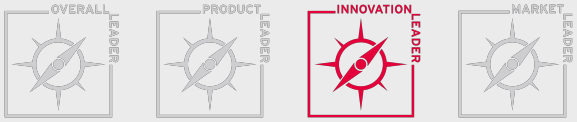
Strengths

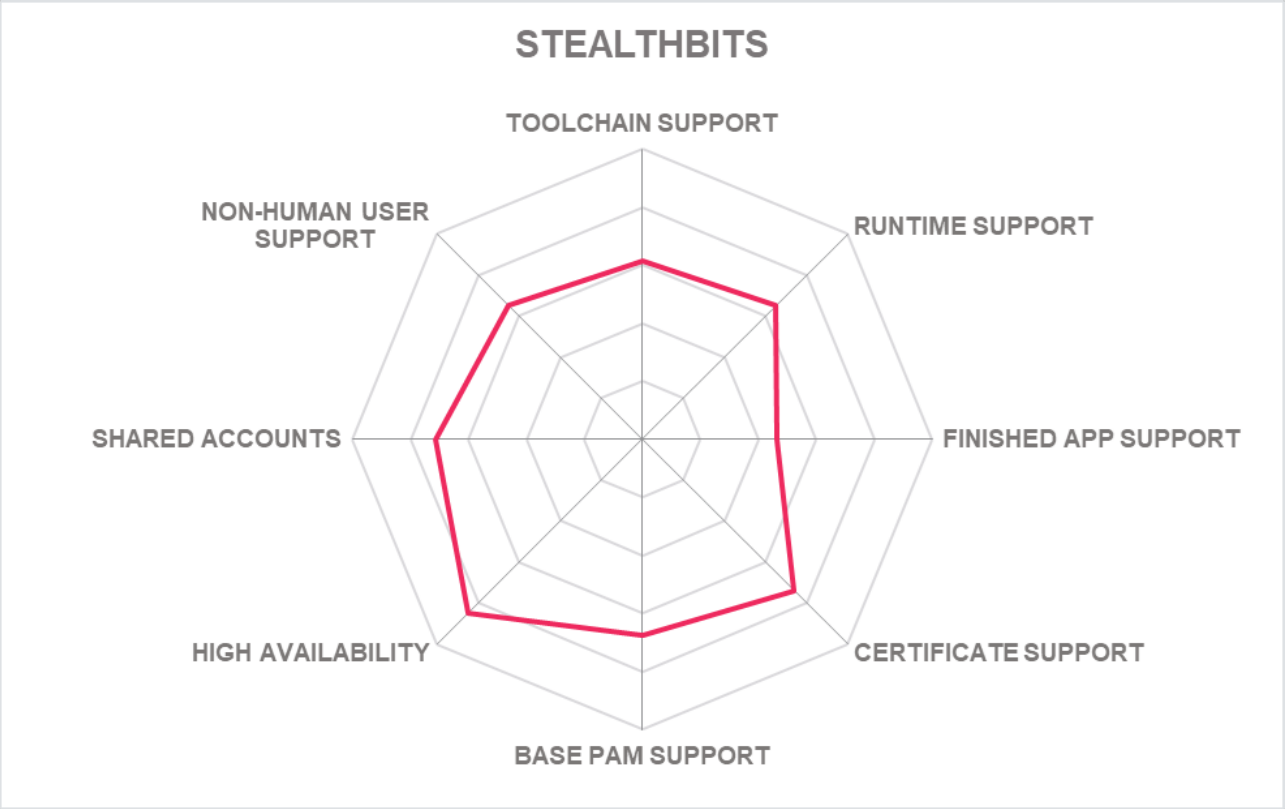
- Potentially the future of PAM in terms of ease of use and ephemerality
- Highly suitable for DevOps environments
- Easy to use and administer, very rapid deployment
- Ephemeral approach means a reduced attack surface
- Would work well with smaller, less legacy encumbered organizations

Challenges

- Lacks some advanced PAM capabilities that DevOps may need
- BYOV approach may be tricky for some organizations looking for an integrated solution from a single vendor
- Needs to do more to effectively market this approach to PAM

Leader in




STEALTHBITS
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.8 Symantec

A new name for PAM but one borne by the acquisitions by US chip giant Broadcom of CA Technologies and subsequently, Symantec. Having digested the former CA collection of IAM technologies, it now intends to market its PAM solution under the Symantec brand, well known in cyber security.

Symantec is a brand known for its sturdy endpoint protection products and Broadcom obviously hopes the brand will work well for what was CA's PAM suite. It may play well in the SMB market where Symantec has always been strong. Certainly, Symantec's PAM solution should have some investment dollars behind it with Broadcom's $5.6bn annual revenue from software. The new business will be run as a subsidiary which potentially allows Symantec to focus and compete more effectively with the PAM leaders.

As the acquisition is still not fully bedded in there is no great technical leap forwards from the CA platform of 2019 but there are changes in presentation. Symantec talks of a "OnePAM" solution which will incorporate an access manager including a vault and PAM Server control, giving agent-based control of servers and a threat analytics module. The solution is designed for hybrid environments with AWS and Azure support, and Symantec claims its appliances can be stood up very quickly, with auto discovery of privileged accounts getting basic PAM up and running in 2- 3 days. Symantec supports different form factors for on-premises, public and private cloud; thus, useful for agile environments.
Given that competitors are now happily marketing PAM suites with optional modules available off the shelf this fully integrated approach could be risky, however modules can still be purchased individually. In terms of technology then not much has changed. There are still robust SAPM, AAPM and PSM capabilities in the solution. The Threat Analytics engine delivers advanced threat analytics leveraging machine learning techniques for automated detection of risky privileged behaviour. The PAM Server Control offers an agent-based architecture to intercept control and restrict commands at OS Kernel level enabling a fine-grained command control and privilege elevation while enabling authentication of UNIX and Linux users using AD and Kerberos credentials for Unix-AD bridging. The affinity with CA's former IAM product remains.

DevOps support is good but not yet fully-fledged. Customers can leverage the Privileged App-to-App Manager to create a stub integration to any third-party DevOps tool, allowing developers to leverage PAM's credential vault at run time, ensuring no hard coded passwords or SSH keys are required. The product also supports extensible secrets types and the Target Connector Framework which allows users to create custom connectors for homegrown applications. This approach is clearly on the right lines and demonstrates an operational understanding of DevOps environments.

Symantec has several pipeline features to address further challenges from DevOps and Containerization which are promising. These include a Secrets Management tool that runs within an ephemeral environment – and micro-segmenting Symantec PAM modules for container deployments. We look forward to those.

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

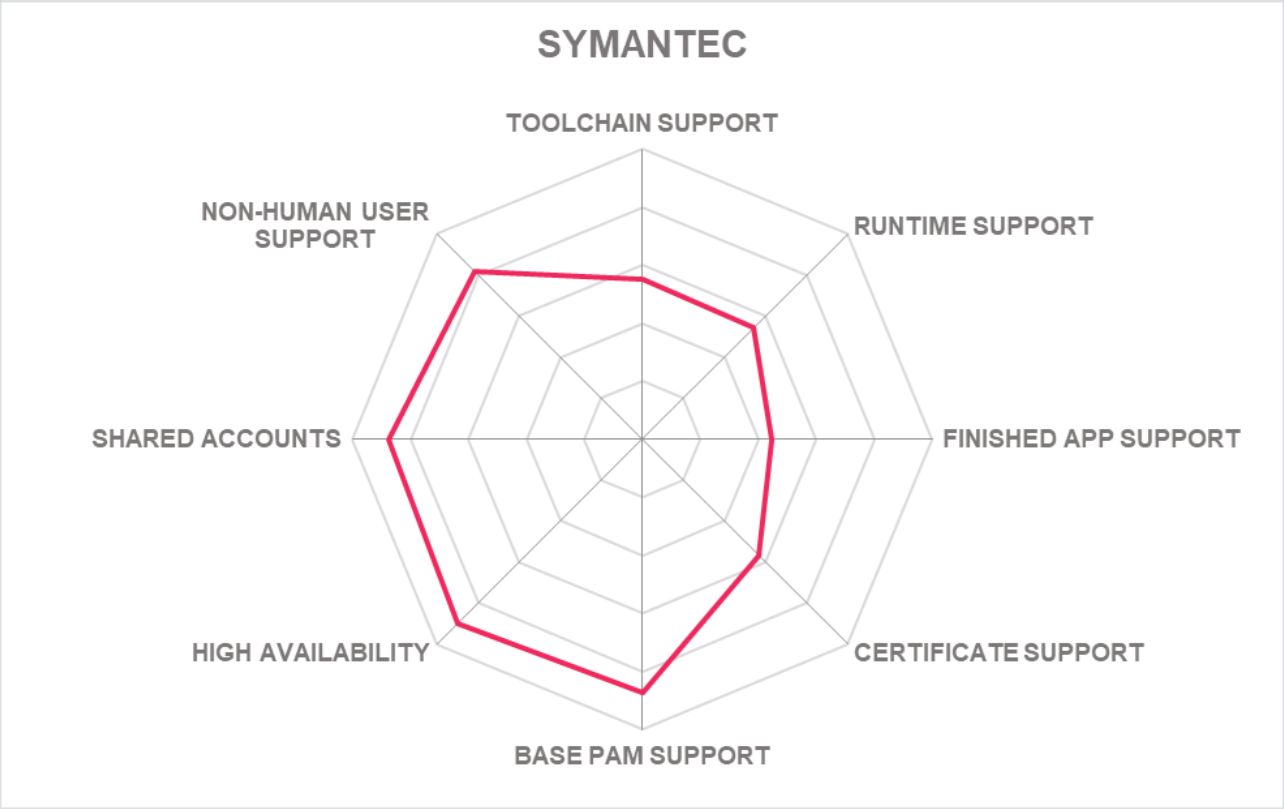
Strengths

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

Challenges

- Support for DevOps will be significantly improved with the arrival of new capabilities – but must come soon
- Product needs renewed marketing commitment under Symantec brand
- Lack of focus on mid-market segments may now be helped by Symantec's experience here

Leader in


SYMANTEC
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

5.9 Thycotic

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

Thycotic remains one of the well-known names in PAM, and while it has benefited from the "blue labelling" of its product by IBM, it has remained very much its own company and able to reach big corporate customers of its own. Thycotic's platform consists of four PAM modules: Secret Server itself, Privilege Manager, Account Lifecyle Manager, DevOps Secrets Vault plus the Connection Manager (its RDM product).

Privilege Manager is Thycotic's agent-based EPM solution for Windows and Mac endpoints that supports extensive EPM capabilities including application control and privilege elevation (available on-premises or as a SaaS-hosted solution in Azure). The Thycotic Privilege Behaviour Analytics solution monitors user activities across Secret Server deployments. It can alert upon detection of anomalies based on thresholds, or automatically respond to threats with customer-configured response actions.

Secret Server is launched from a browser with a brand-new user interface as of 2021, but may also be launched from an SSH terminal for those who prefer a command line interface (CLI). Connection Manager is another alternative for hard-core Secret Server users that runs natively on a PC and enables the management of multiple simultaneous privileged sessions. For MFA it supports all the standard mechanisms including FIDO2, has a strategic partnership with Duo Security, and supports SAML and OpenID Connect to delegate authentication to an external identity provider. JIT functionality includes credential check-out and workflow support. Workflows allow if-then functionality based on numerous triggers and resulting actions. Scalability and fast deployment are also strengths. Thycotic also offers browser extensions and a mobile app.

DevOps Secrets Vault automates secrets management in applications and DevOps CI/CD pipelines, and is capable of high-speed secrets creation, archiving, and retrieval. It supports SDKs and DevOps plug in tools including Java, Python, .NET, Go, and Ruby; and for DevOps, Jenkins, Kubernetes, Ansible, Chef, and more. DevOps Secrets Vault is specifically designed to handle high velocity automation through CLI and API interfaces. IaaS federation is enabled so that, for example, AWS IAM users may authenticate to DevOps Secrets Vault. Additionally, AWS roles may be assigned to AWS assets and they in-turn can authenticate to DevOps Secrets Vault. DevOps Secrets Vault also enables TLS and SSH certificate signing, enabling the automation of short-lived certificates for JIT access to machines.

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

thycotic

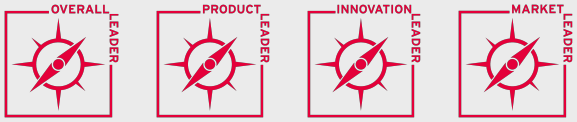
Strengths

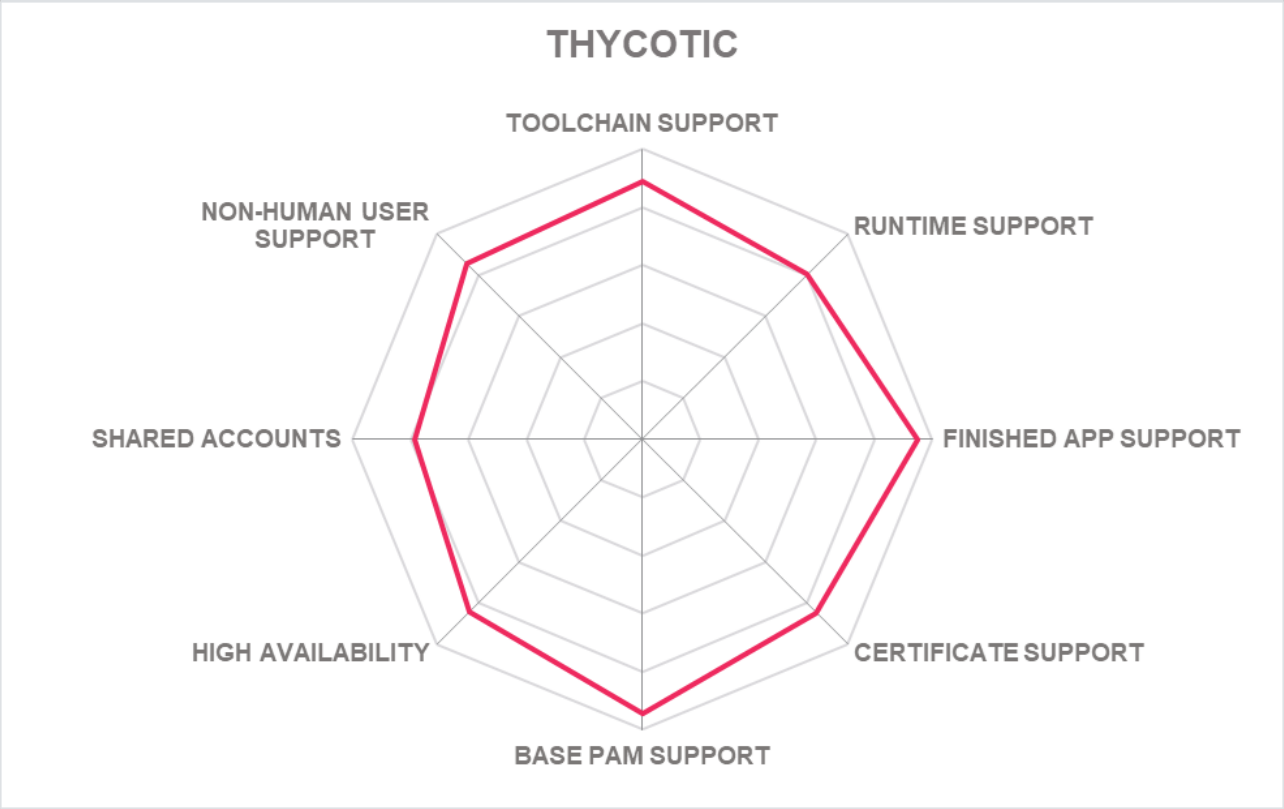
- Solid and well-known brand that has used its relationship with IBM to its advantage
- Ongoing product development and frequent updates show commitment
- Thycotic understands that DevOps for PAM needs to take account of unique coding environments and secrets management
- Good new user interface leverages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

Challenges

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

Leader in




THYCOTIC
TOOLCHAIN SUPPORT
RUNTIME SUPPORT
FINISHED APP SUPPORT
CERTIFICATE SUPPORT
BASE PAM SUPPORT
HIGH AVAILABILITY
SHARED ACCOUNTS
NON-HUMAN USER SUPPORT

6 Vendors and Market Segments to watch

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

6.1 Remediant SecureONE

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

Currently SecureOne has limited support for DevOps teams but does offer Zero Standing Privilege for Cloud Workloads. This should enable DevOps teams privileged access to cloud, ephemeral and on-premises workloads. These capabilities allow users to log into cloud hosted Linux systems using their directory credentials – without having to bind the Linux systems to the directory. According to the company this will allow cloud developers to seamlessly integrate Remediant into their CD/CI pipeline and enforce Zero Standing Privilege as part of their default container images.

Why worth watching: While Remediant are some way off the leaders currently, broader development of its JIT technology would lend it well to DevOps environments.

6.2 Saviynt

Saviynt is a US-based company founded in 2010 that specializes in IGA and Identity solutions. It has recently entered the PAM market with a new cloud-only PAM platform, with HashiCorp vault technology to store secrets – generation of new keys, rotation and check in/check out are performed within Saviynt Cloud PAM, however. The solution is designed to run on all major cloud platforms including AWS, Google, Azure,

SAP 4 Hana, and Oracle. It is also compatible with Workday and Salesforce platforms. While no PAMaaS option is offered directly by the company, in theory it could be deployed as a service by third party managed service providers (MSPs) or as an option within large enterprises.

Saviynt's API integration provides the tool for developers to make a programmatic call to the Saviynt vault to request access permissions and check out a key at the time of code execution. This creates a more secure environment, less subject to key exfiltration and compromise.

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

Why worth watching: Saviynt's major proposition is a secure environment for developers that puts secrets management at the heart of code execution.

6.3 Venafi

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

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

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

Venafi continues to develop expertise in enabling access for machine identities and its DevOpsACCELERATE solution uses advanced certificate-based authentication techniques to speed access for DevOps teams to the resources they need. It is conceivable that the combination of this along with the company's existing SSH-based authentication services may deliver secure access to privileged accounts for DevOps, machines, and other entities.

Why worth watching: Venafi's development of SSH key management is exciting and we think that it will soon make an impact on the PAM for DevOps market.

7 Related Research

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

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

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

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

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

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

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are

understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

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

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

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

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.

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

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

Vendor rating

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

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

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

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

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

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

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

Rating scale for products and vendors

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

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

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

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

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

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

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

Figure 2: Transparent Security platforms including PAM must be embedded within the CI/CD lifecycle that DevOps teams work within.

Figure 3: PAM for DevOps currently offers the choice of certificates or encrypted vaults to authenticate access.

Figure 4: The Overall Leadership rating for the PAM DevOps market segment

Figure 5: The Product Leadership rating for the PAM DevOps market segment

Figure 6: Innovation Leaders in the PAM DevOps market segment

Figure 7: Market Leadership in the PAM for DevOps Leadership Compass

Figure 8: The Market/Product Matrix.

Figure 9: The Product/Innovation Matrix

Figure 10: The Innovation/Market Matrix

Copyright

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

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

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