KuppingerCole Report

LEADERSHIP COMPASS

By Paul Fisher

August 23, 2022

CIEM & Dynamic Resource Entitlement & Access Management (DREAM) platforms

This report provides an overview of the market for platforms that support CIEM and DREAM environments and provides you with a compass to help find the solution(s) that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing solutions that increase security in these business application environments for managing cloud entitlements.

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

Content

1 Introduction/Executive Summary

The complexity of cloud architectures and design – Kubernetes alone has enough mind stretching concepts, permissions, building block terms to service a cottage industry of self-help books – means that trying to manage these environments, particularly in dev environments is not just about Privileged Access or CIEM. It's kind of another level of cloud security in itself which some of these platforms can assist with to different levels.

Cloud access is managed by the developers who have little time for IAM + Security - according to one vendor, so there is a fork in the road emerging – one way is to persevere with the top down (PAM) method of controlling access centrally – or by opening up identity and security to individual departments within organizations – i.e., developers, operations, HR, etc.

Dynamic cloud environments require dynamic access. Dynamic cloud architecture is coming to dominate enterprise networks and operations, as business leaders and IT vendors understand a paradigm shift is necessary for organizations to compete as fully digital enterprises.

This new architecture incorporates multiple instances of cloud services including IaaS, PaaS and SaaS, as well as hybrid combinations of cloud and on-premises installations and within it all, clusters of teams using and running these clouds.

This new IT architecture has become essential to organizations seeking the speed and dynamism essential for organizations to run the applications and tools needed for fast changing markets and challenging operating conditions. DevOps and other agile teams within organizations have come to rely on dynamic clouds to complete workloads on a Just In Time (JIT) basis, in response to demands from internal customers (LoBs). All the while, networks are much more open to employees, third party users, suppliers, and customers; what was once considered "privileged" is becoming the norm as collaboration and data sharing become ubiquitous. The emergence of non-human identities gaining access to cloud-based resources is also an important part of the new environment.

The speed at which these environments operate has put severe pressure on the capabilities of traditional access management platforms such as role-based IGA, IAM and PAM. While workloads have long been present in servers and private clouds these tended to be static and not time critical. What has changed is the breadth of access, but primarily the dynamic/agile/volatile nature of what needs to be managed. It is not about setting up a server on a physical machine that runs for years anymore, but about constantly changing workloads.

Hence the need for our new Dynamic Resource Entitlement & Access Management (DREAM) classification for access management and entitlement platforms that can manage the challenges in the computing environments mentioned above. Fundamentally, DREAM based platforms must operate at the speed of the cloud and grant access based on tasks, toolchains, and workloads rather than roles – or only permission

access to static resources such as servers or vaults.

These platforms include those categorized as CIEM (Cloud Infrastructure Entitlement Management) platforms that offer rapid access to cloud infrastructure itself and in some more advanced examples, offer granular control of cloud-based resources. Also included within DREAM are the newer PAM for DevOps tools that extend the traditional functionality of PAM for toolchain focused access for DevOps teams. It's an emerging market but one that is attracting significant attention, not least from some of the biggest names. Microsoft acquired CIEM vendor CloudKnox in 2021 and has now relaunched the technology as Microsoft Entra Permissions Management as part of a wider sweep into cloud security management. Unfortunately, the package arrived too late for this Leadership Compass but there are more details in the Vendors to Watch section.

All included platforms must address the protection of the clouds themselves, the assets held in the cloud, and include those assets which remain on-premises but are needed to connect to the cloud. We are addressing such common components as VMware, Linux/Windows Servers, Web Servers, SaaS, IaaS, databases, containers, code, confidential data, secrets, credentials and privileged accounts. Finally, certain IGA products will contribute to a DREAM based architecture for compliance purposes.

1.1 Highlights

- The IT environment has become complex, but this will not stop as more technologies such as Edge Computing start to take hold.
- New technology, business practices, and cultures are arising that will further put a strain on traditional Identity and Access Management (IAM) solutions for multi-hybrid environments.
- KuppingerCole has identified the Dynamic Resource Entitlement and Access Management (DREAM) classification to measure the increasing number of platforms that address cloud entitlement challenges.
- The Leadership Compass analyses platforms from established CIEM and PAM vendors that offer components to manage privileged access in the cloud.
- DevOps and developer environments are a key focus for DREAM but increasingly other lines of business are creating and using cloud services.
- Reporting and discovery are key capabilities for CIEM and DREAM.
- While most CIEM and DREAM platforms support AWS, Azure and GCP as standard, the market is looking for wider cloud support to include Oracle, OVH, IBM, etc.
- Some vendors have designed fully cloud native packages that also support open source and API

customization by customers.

- The CIEM and DREAM sector is impacting on classical PAM; its vaults and standing privilege architectures are increasingly too slow for dynamic cloud workloads.
- Overlapping technologies may have different buyers now. DevOps security and access management often bought by engineering depts, while infrastructure designers look to PAM.

1.2 Market Segment

This Leadership Compass looks at currently available platforms that fall under the KuppingerCole DREAM classification and add value to business. Such platforms will include Privileged Access Management (PAM) for DevOps (PAM/DevOps), Cloud Infrastructure Entitlement Management (CIEM) platforms, and certain Identity Governance and Administration software for compliance purposes.

Thus, solutions must not only deliver functionality and support for all types of identities, but also meet our requirements regarding the architecture, deployment model, and their interoperability with traditional applications, cloud services, and new digital services.

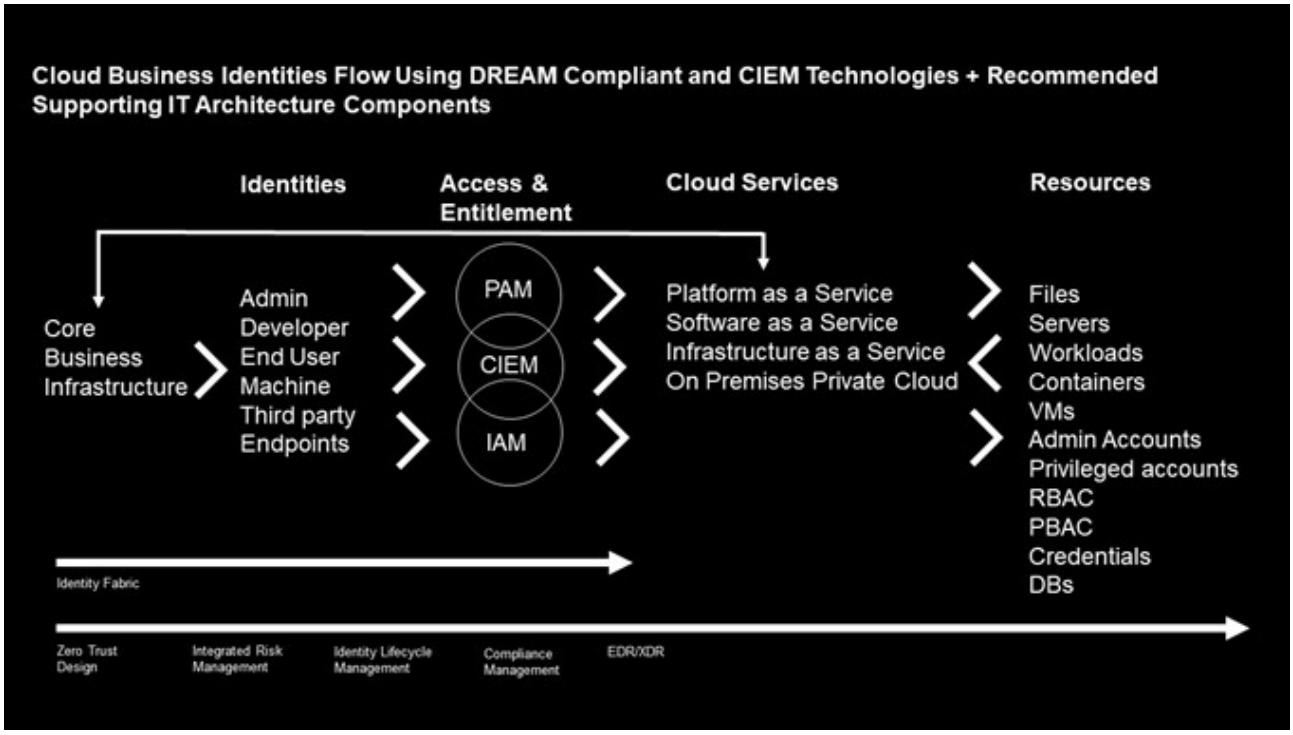


Figure 1: How DREAM and CIEM platforms facilitate access to cloud resources. (KuppingerCole)

1.3 Delivery Models

DREAM compliant platforms will run as a service from the cloud; cloud native platforms are obviously technically suited to orchestrating other cloud applications and all cloud-based entities as well as marshalling identities. This would not rule out platforms that have some on-premises component, however but the core capabilities must run in the cloud. All platforms must be deployed in such manner to enable integration will legacy cloud and legacy non-cloud infrastructures.

Delivery of cloud services must meet the expectations regarding licensing models (pay-per-use) and elasticity and scalability, i.e., flexible scaling of the service. Beyond that, as mentioned above, we expect modern SaaS architectures, which are anyway the foundation for flexibility in deployment today.

Thus, solutions must not only deliver functionality and support for all types of identities, but also meet our requirements regarding the architecture, deployment model, and their interoperability with traditional applications, cloud services, and new digital services.

1.4 Required Capabilities

This report describes the basic capabilities that all solutions should support in terms of use cases, which are:

- Native Support for Tier 1 CSPs – AWS, GCP, Azure,
- Agentless deployment
- Just in Time (JIT) access for users, machines, and service accounts
- Cross-cloud/multi-cloud discovery tools
- Least privilege enforcement
- Privilege Right Sizing
- Integration with UEBA/SIEM platforms
- Centralized and easy to read dashboarding
- Alerting and reporting mechanisms
- AI-powered analysis and assessment tools
- Enforcement of Least Privilege
- Automated discovery of privileged accounts
- Connectors to both cloud services and on-premises applications
- API based toolkits for customizing connectors
- Local caching for intense workload support in cloud
- Entitlement Management, including Role Management
- Native Orchestration Tool support e.g., Kubernetes
- Privileged User Behaviour Analytics (PUBA)
- Workflow and task-based authentication
- PAM Session Recording and Monitoring
- Rule based privileged escalation
- API Authentication support

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in 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
- Innovation
- Market

2.1 Overall Leadership

Figure 2: The overall leaders in CIEM and DREAM

This is the first Leadership Compass KuppingerCole has produced on CIEM and DREAM and the results here are in line with what we might expect in terms of maturity (it applies to other charts as well). While cloud infrastructures are not new , we are now witnessing the second stage of cloud adoption in which the

demands of multi cloud and dynamic access and authentication processes are needed to get the best from cloud – and businesses are realizing that. So currently we only have three leaders: CyberArk, EmpowerID and SSH.

Apart from CyberArk these are not the names that normally dominate PAM Leadership Compass – and the reason is that while DREAM and CIEM solutions require some heritage capabilities of PAM to work well, they also need more and the three leaders here have, in different technical ways, responded well to the new paradigm – particularly for those areas of Cloud Entitlement Management that need fast, secure and credible access such as Developers – probably the most challenging and demanding users of cloud. They have also thought about putting entitlement management closer to where it is needed by a process of decentralization.

Behind the Leaders we have a cluster of leading Challengers who are close to the standards set at the top. These are (in alphabetical order) Britive, HitachiID, NextLabs Palo Alto Networks, Senhasegura, SailPoint and Saviynt – all of which would be worth investigating by potential customers to see if they fit the desired outcome. Behind them we see our remaining vendors: StrongDM, BeyondTrust, Ermetic, Sectona, Attivo Networks, Remediant, ObserveID and HashiCorp.

The fact there are no Followers on Overall Leadership suggests this market is already starting to mature.

Overall Leaders are (in alphabetical order):

- CyberArk
- EmpowerID
- SSH

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is based on the analysis of service features and the overall capabilities of the numerous services. Product Leadership is where we examine the functional strength and completeness of services.

Figure 3: The product leaders in CIEM and DREAM

Here, things have opened a little bit where we see six vendors sharing the Leadership placings. These are (in alphabetical order) BeyondTrust, CyberArk, EmpowerID, Saviynt, Senhasegura and SSH. These have done well for providing more complete products in term of services which also extend into other supporting areas such as analytics and credential management.

SailPoint and HitachiID come closest to the Leaders among the Challengers and they are joined by strongDM, Sectona, Palo Alto Networks, Britive, NextLabs, ObserveId, Remediant, Ermetic, Attivo Networks and HashiCorp. Here is a good mix of vendors known for traditional PAM or IGA and those younger vendors that have focused on CIEM. Plenty to choose from for buyers at all levels among the capabilities of the

vendors here.

There are no Followers on Product Leadership which is reassuring and shows a fast developing market with vendors responding well to capability demands from the market.

Product Leaders (in alphabetical order):

- BeyondTrust
- CyberArk
- EmpowerID
- Saviynt
- Senhasegura
- SSH

2.3 Innovation Leadership

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

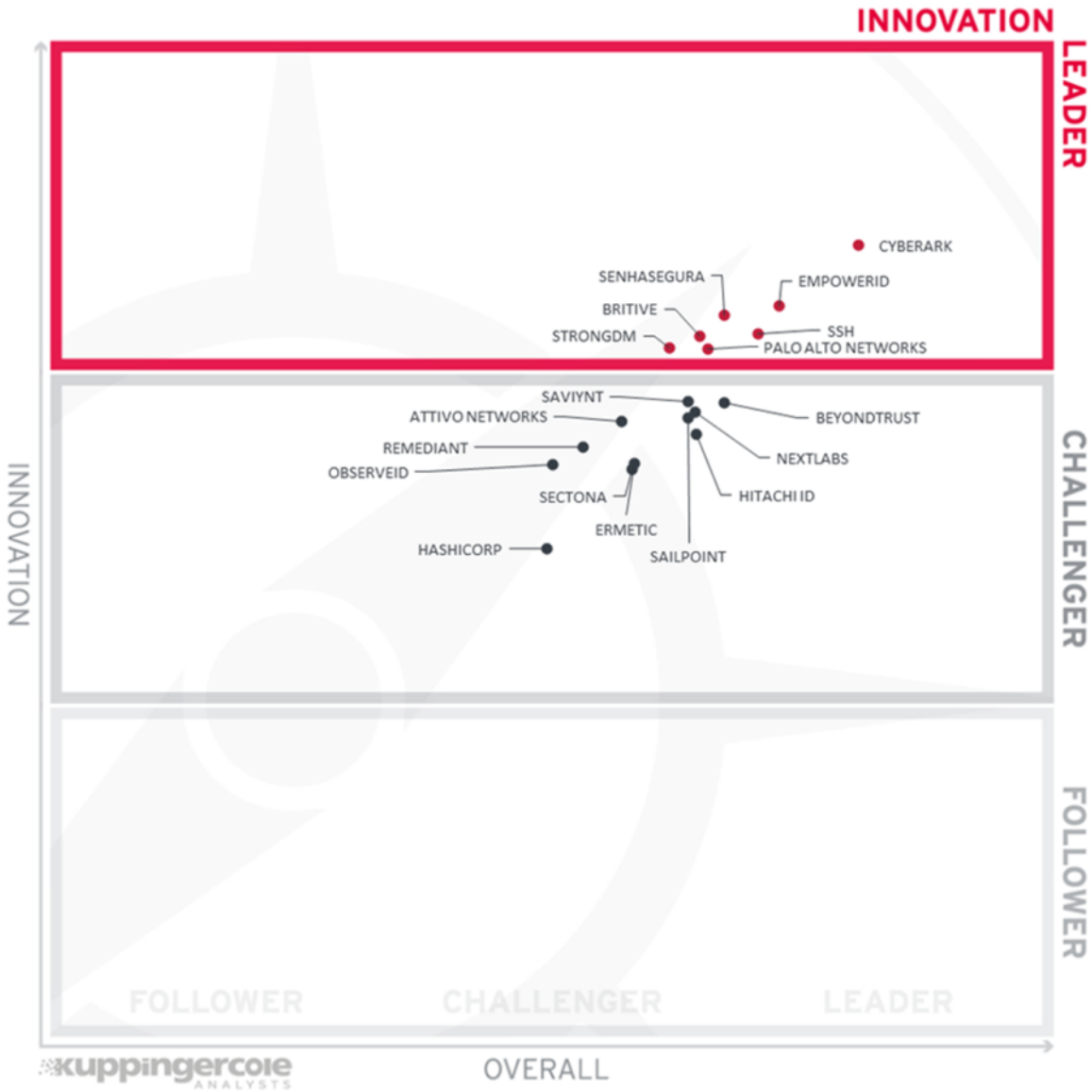


Figure 4: The innovation leaders in CIEM and DREAM

Vendors in this measurement have been assessed critically on the customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions. Britive, CyberArk, EmpowerID, Palo Alto Networks, Senhasegura, SSH and StrongDM have fulfilled this by developing their platforms to embrace the new worlds of CIEM and DREAM capability.

Therefore we have a majority of vendors listed as Challengers: they represent a fertile mix of new capabilities, new ways of managing entitlements while also developing existing products. It is also why we see a mix of traditional PAM/IGA players competing with newer CIEM players. By carefully reviewing any of these options, buyers should be able to make a sensible choice to match requirements on DREAM

environments and cloud entitlement management demands. The Challengers are Saviynt, NextLabs, SailPoint, Attivo Networks, HitachiID, Remediant, BeyondTrust, ObserveID, Ermetic, Sectona and HashiCorp.

Innovation Leaders (in alphabetical order):

- Britive
- CyberArk
- EmpowerID
- Palo Alto Networks
- Senhasegura
- SSH
- StrongDM

2.4 Market Leadership

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

Figure 5: The Market Leaders in CIEM and DREAM

In this section we see a not untypical spread of vendors that have scored well on the number of installations and managed identities. So, we see some traditional big names, in terms of turnover and size etc, but also smaller vendors that are still pushing the envelope in terms of customers reached. This is well demonstrated in the Leaders which are, in alphabetical order, BeyondTrust, CyberArk, EmpowerID, HitachID, NextLabs, Palo Alto Networks and SSH – a good mix of big and small, and up and coming.

Behind this group is another healthy mix of vendors that are starting to approach the right mix of market presence and identities managed, along with new capabilities that are focusing on the DREAM and CIEM demands. We believe that good choices can be found among SailPoint, Ermetic, Britive, Sectona, Saviynt,

Attivo Networks, strongDM, Senhasegura and Remediant.

Market Leaders (in alphabetical order):

- BeyondTrust
- CyberArk
- EmpowerID
- HitachiID
- NextLabs
- Palo Alto Networks
- SSH

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

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

3.1 The Market/Product Matrix

Figure 6: The Market/Product Matrix for CIEM and DREAM

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

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

In the upper right segment, we find the "Market Champions" leading in both the product and market ratings. This segment contains CyberArk, SSH, EmpowerID and BeyondTrust.

In the top middle box, we see NextLabs, HitachiID, and Palo alto Networks with leading products but missing out on some market share

In the middle of the chart, we see the rest of the vendors providing good but not leading-edge capabilities and therefore are not Market Leaders yet. They also have average market success as compared to market champions

3.2 The Product/Innovation Matrix

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

Figure 7: The Product/Innovation Matrix for CIEM and DREAM

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.
Here, we see a good correlation between the product and innovation rating. Most vendors are placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most of the leading vendors near the centre of the box. The top-notch vendors are CyberArk, Senhasegura, and EmpowerID with vendors placing closer to the axis depicting a better balance of product features and innovation.

There are three vendors in the top middle box, SSH, BeyondTrust and Saviynt who are offering less

innovation but good product capabilities, including some more traditional capabilities.

In the centre and centre left box of the chart, we see the majority of vendors who offer a media mix of innovation and product leadership.

3.3 The Innovation/Market Matrix

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

Figure 8: The Innovation/Market Matrix for CIEM and DREAM

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position. In the upper right-hand corner box, we find the "Big Ones" in the WAF market: CyberArk, Palo Alto Networks and EmpowerID.

NextLabs, SSH, HitachID and BeyondTrust are in the top middle box, showing a strong market position but less innovation than those in the Big One's category. SailPoint, Ermetic and Sectona appear in the middle-right box, indicating stronger innovation than market presence – with HashiCorp in the Left Middle Box.

The segment in the middle of the chart contains the vendors rated as Challengers both for Market and Innovation Leadership, including Britive, Saviynt, Attivo Networks, Senhasegura, strongDM, and Remediant.

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 DREAM Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

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

Product	Security	Functionality	Deployment	Interoperability	Usability
Attivo Networks IDEntitleX	positive	neutral	neutral	neutral	neutral
BeyondTrust Cloud Privilege Broker	strong positive	positive	positive	positive	positive
Britive PAM Platform	positive	positive	neutral	positive	strong positive
CyberArk Cloud Entitlements Manager	strong positive	positive	strong positive	positive	strong positive
EmpowerID	strong positive	positive	positive	strong positive	strong positive
Ermetic Cloud Infrastructure Security	positive	positive	positive	neutral	positive
HashiCorp Boundary	neutral	neutral	neutral	neutral	positive
Hitachi ID Bravura Security Fabric	strong positive	positive	neutral	positive	positive
NextLabs Control Center	positive	positive	positive	strong positive	neutral
ObserveID Platform	strong positive	positive	neutral	positive	neutral
Palo Alto Networks Prisma Cloud	strong positive	positive	positive	strong positive	positive
Remediant SecureOne	positive	positive	neutral	neutral	positive
SailPoint Cloud Access Manager	strong positive	positive	positive	strong positive	positive
Saviynt Enterprise Identity Cloud	strong positive	positive	positive	positive	positive
Sectona Security Platform	strong positive	positive	neutral	positive	positive
Senhasegura Platform	strong positive	positive	strong positive	strong positive	strong positive
SSH PrivX	strong positive	positive	positive	strong positive	strong positive
strongDM Infrastructure Access Platform	positive	positive	positive	strong positive	strong positive
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
Attivo Networks	positive	neutral	neutral	positive
BeyondTrust	neutral	positive	positive	positive
Britive	positive	neutral	positive	positive
CyberArk	strong positive	strong positive	strong positive	positive
EmpowerID	positive	neutral	neutral	positive
Ermetic	neutral	positive	neutral	positive
HashiCorp	weak	weak	neutral	strong positive
Hitachi ID Systems	neutral	positive	neutral	strong positive
NextLabs	positive	strong positive	positive	strong positive
ObserveID	neutral	critical	critical	positive
Palo Alto Networks	positive	neutral	positive	strong positive
Remediant	neutral	weak	weak	strong positive
SailPoint	positive	neutral	strong positive	strong positive
Saviynt	positive	strong positive	strong positive	strong positive
Sectona	neutral	neutral	neutral	strong positive
Senhasegura	positive	weak	neutral	positive
SSH Communications Security	positive	positive	positive	positive
strongDM	positive	neutral	neutral	positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

- Reporting
- Identity Governance
- DevOps Tools
- Extended IaaS support
- Dashboard
- PAM
- SIEM support
- Application Dev Tools

5.1 Attivo Networks

Attivo Networks is based in California. In May 2022, Attivo Networks was acquired by SentinelOne, a leading Endpoint Protection Detection & Response vendor. The Attivo Networks IDEntitleX product reviewed here is part of the wider Attivo Networks suite of Active Directory security applications. It is offered for SaaS deployment only – and focuses on protecting access for Active Directory identities and entitlements to AWS and Azure cloud services.

The product has a central dashboard to monitor and assess entitlements and splits identity types into Users, Groups and applications. Built-in analysis tools assign a risk score to identities based on their entitlements and can detect excessive access to resources (known as Objects by Attivo) and over entitlement.

The graphical tool available offers an “explorer" view with graphical attack path mapping and search against identities, resource, and entitlements. There is full integration of entitlement analysis across cloud with Active Directory. OKTA and Ping Identity federation tools detection supported.

The dashboard is highly functional and includes comprehensive visibility into identity and resource permissions gaps, cross-account access visualization, risk scoring, privileged account discovery for both machines and non-machines identities, and alerting to possible security risks (not suspicious activity however).

This is not a PAM tool so there is no credential management, session monitoring or privileged analytics but it can discover privileged accounts and offer privilege escalation. Attivo Networks IDEntitleX can be integrated with XDR and SIEM tools; currently supporting Splunk and QRadar. There is a good deal of automation in the product; entitlement configuration, permission management, identity risk assessment, alerts for unused permissions, excess privilege and excess permissions detection are all supported.

Attivo Networks is committed to developing IDEntitleX with GCP and greater Kubernetes support is coming – but more support for container technologies beyond Azure and AWS is needed for developer environments to significantly increase its range in DREAM environments. Least privilege control will be enhanced with granular AWS policy generation, remediating unused Cloud Access keys, Users, etc.

Overall this is a powerful CIEM tool for Azure and AWS environments needing better control over access and entitlements. Its ease of use and features will be welcome as it embraces wider cloud and DevOps compatibility. Stronger support for authentication protocols beyond passwords, SSH keys OAuth 2 and SAML is desirable too.

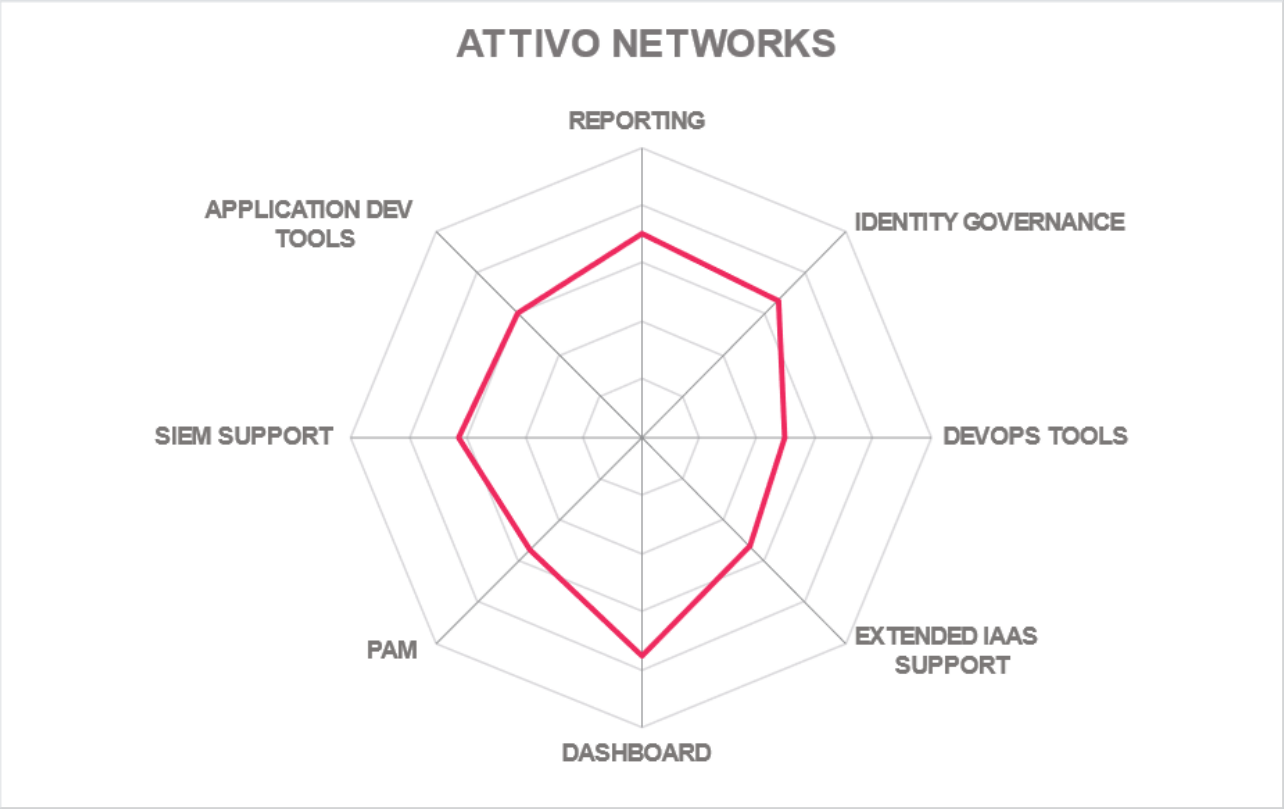
Security	●●●●○
Functionality	●●●○○
Deployment	●●●○○
Interoperability	●●●○○
Usability	●●●○○

Strengths

- Strong focus on Active Directory suggests deep knowledge of Microsoft identity structures and anomalies which will suit many organizations
- Easy to understand dashboard with single pane of glass eases pressure on admins and IT managers
- Easy deployment
- Compliance tools are welcome
- Strong on automation capabilities

Challenges

- Wider authentication protocol support needed
- While Microsoft cloud focus makes sense, the company would do well to widen IaaS support
- We would like to see development in areas that are designed for DevOps
- Currently lacks JIT functionality which it badly needs
- Lack of PAM oriented capabilities


ATTIVO NETWORKS
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.2 BeyondTrust

BeyondTrust is one of the best-known PAM vendors and it has continued to refine a portfolio of identity products bracketed into Privileged Password Management, Secure Remote Access, Endpoint Privilege Management, and Cloud Security Management in which sits the BeyondTrust Cloud Privilege Broker product. Released in December 2021, BeyondTrust Cloud Privilege Broker is sensibly built on cloud native code.

Deployed as SaaS only, BeyondTrust Cloud Privilege Broker is a cloud entitlements management solution for AWS and Azure that enables users to visualize and manage cloud access risk in multi-cloud environments, from a single pane of glass dashboard. BeyondTrust Cloud Privilege Broker is 100% cloud native built using the open-source service mesh Istio as part of BeyondTrust's own micro services architecture

Cloud Privilege Broker provides recommended steps for enforcement of least privilege and enables the rightsizing of entitlements, to reduce risk and meet compliance goals. The Dashboard is configured out of the box to get started, but can be modified by customers to fit specific environments. A risk assessment tool is available to test IaaS platforms and entitlement policies can be configured within that tool. There is wide integration with third-party IDP authentication platforms. Coming soon is auto-discovery for up-to-date inventory of user and machine principles, policies, and entitlements. As soon as resources appear, or changes to an existing resource occur, they are detected, evaluated and assessed for risk.

Cloud Privilege Broker centralizes usage data with purpose-built dashboards for the cross-cloud visualization and management of entitlements. The dashboard helps administrators detect and review anomalies in account permissions, ensure access from only trusted sources, and provide easily deployable recommendations for enforcement of least privilege policies. These recommendations are a key component of the platform and are based on discovery, tasks, and existing policies. A typical recommendation from the dashboard would be to deploy Multi-Factor Authentication, or simply remove permissions from an individual. Other important metrics displayed on the various dashboard modules are an overall risk score, risk-over-time, Top 10 recommendations for improving security access, discovery results, and more.

The discovery process is comprehensive. It can find users, groups, roles, and service principals in IaaS platforms. Further, auto-classification will rate risks of access permissions into high, medium, and low, bringing a welcome element of risk management to the platform.

More granular audit information is also provided about the health of connectors, completed actions, and recommended mitigation steps. Reporting also includes a User Activity report, such as new users granted access or new cloud connectors, and data on users who may have ignored a recommended course of action, to reduce and document exposure to risk. The user interface of BeyondTrust Cloud Privilege Broker is easy to understand and meets the demands of delivering data quickly to enable better decision-making. The Administrator Dashboard will highlight actions that need immediate attention.

BeyondTrust has already provided a DREAM focused tool for developers with DevOps Secrets Safe. This

features built-in support for Docker, Kubernetes, and microservices and is database agnostic. BeyondTrust Cloud Privilege Broker fits well with the existing DevOps tools and the drive to streamline all its other products into a single cloud native platform. This should enable BeyondTrust to elevate beyond its legacy PAM roots into a full-featured, DREAM compatible platform, suitable for many organizations. But it has work to do on the roadmap before that is quite ready.

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

BeyondTrust

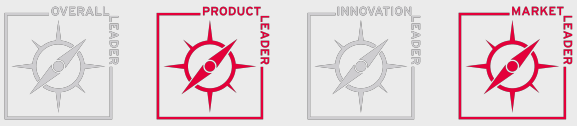
Strengths

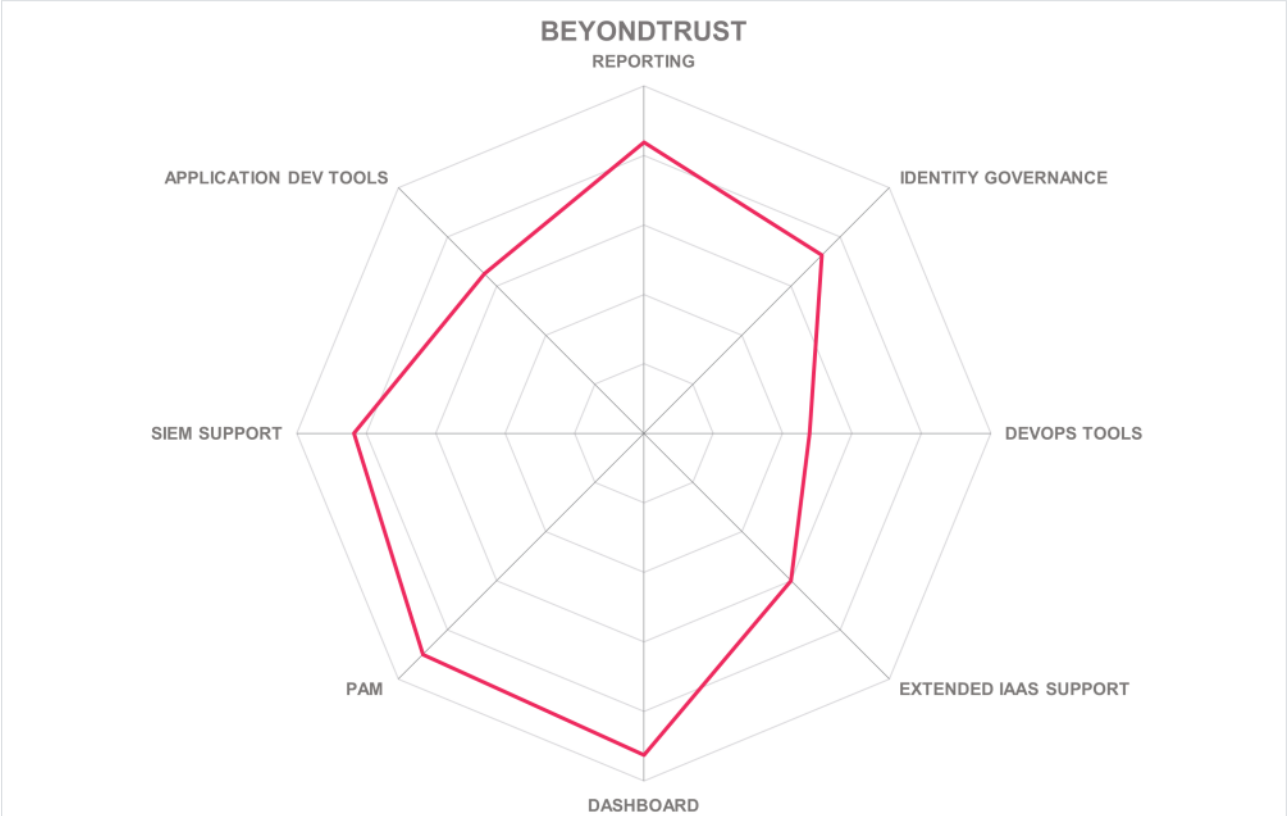
- Platform extends BeyondTrust's expert and trusted knowledge of PAM to deliver least privilege access to multi-cloud IaaS
- Cloud Privilege Broker is deployed on BeyondInsight, providing a familiar user interface
- Centralized dashboard provides key metrics and recommendations in a single UI
- Provides continuous discovery of users, groups, roles, and policies
- The Recommendations section is an easy way for admins to discover, analyse, and limit access

Challenges

- Currently limited to AWS and Azure but further support for CSPs and SaaS applications are in the pipeline
- This product provides familiarity to existing BeyondTrust customers to a good degree but those looking for a standalone CIEM may be harder to satisfy
- There may be integration possibilities by adding the BeyondTrust DevOps Secrets Safe vault product as DevOps are typical users

Leader in




BEYONDTRUST
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.3 Britive

Britive was founded in 2018 and based in California. It develops access and entitlement management solutions for IaaS platforms deployed in multi-cloud environments. It added CIEM capabilities and security governance tools to the platform in 2021. It's raison d'etre is ephemeral JIT access for all types of identities to all resources - data, servers, CSP, SaaS applications - in DREAM environments. In scenarios when ephemeral access is not feasible, Britive has introduced a cloud vault for static secrets and keys, which can also be accessed JIT. Due to Britive platform acting as an abstraction layer, machine and non-machine identities never see or have standing access to the application, cloud, or server layer. Britive leverages an API-first approach to grant users access to the target cloud platform or application with the level of privileges authorized for the user.

In the DevOps environment the API-first architecture is used for containers and orchestration services typically used in modern organizations. Britive is extended to sit inside containers creating a temporary service account for developer access. This is to prevent hard-coded credentials being placed inside the containers – a known security risk and one that DevOps people often use. A temporary service account is instead created.

Deployment is agentless which simplifies set up and is in line with the stated goal of making installation, management, and usage easy for non-traditional admins and less experienced IT security people to use. Instead, it encourages those directly involved in DevOps or other development environments to apply security controls themselves.

The platform is API driven, nominally for third-party IAM, SIEM, SSO, usage analytics but it also readily integrates with common CI/CD automation and data warehousing investments. For developers it supports a range of DevOps automation tools (Terraform, Ansible, AWS Cloud Formation, Kubernetes tools for GCP, and Azure) as part of the CI/CD Build and Operate functions.

Britive has one of the widest compatibilities for JIT machine and non-machine access cloud services including IaaS, DaaS, PaaS, and SaaS solutions including less obvious provisioning for cloud services such as Snowflake (DaaS), Workday, Okta Identity Cloud, Salesforce, ServiceNow, Google Workspace and others – some following specific requests from customers. This extends its reach into the cloud beyond many rivals, out of the box.

While this is undoubtedly a lean cloud first entitlement platform, it retains several classical PAM capabilities such as automated account discovery, rule-based privileged escalation, and onboarding of privileged accounts, which will be useful to many potential customers.

Britive Advanced Data Analytics enables organizations to automatically uncover and monitor all human and machine identities and privileges (including overly broad and misconfigured privileges) and privilege related risky behaviour (including privilege drift and abuse) cross-cloud.

The class-leading modern user interface allows for quick onboarding and offboarding of users, and self-

service privilege check-out, and the learning curve – given the focus of the platform - should be less than most similar applications.

In the pipeline are developments in Identity Lifecycle Management (ILM) for machine, service, and non-machine identities as well as moves to incorporate HR and ITSM cloud support areas. It is ambitious to turn all identity access into JIT and embrace Zero Standing Privilege (ZSP) across all environments – but this is seemingly an achievable target with Britive, for those environments that wish to (and can) follow that path.

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

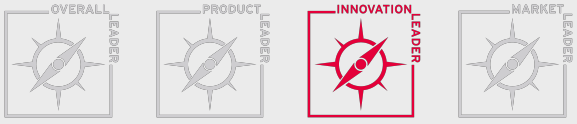
Strengths

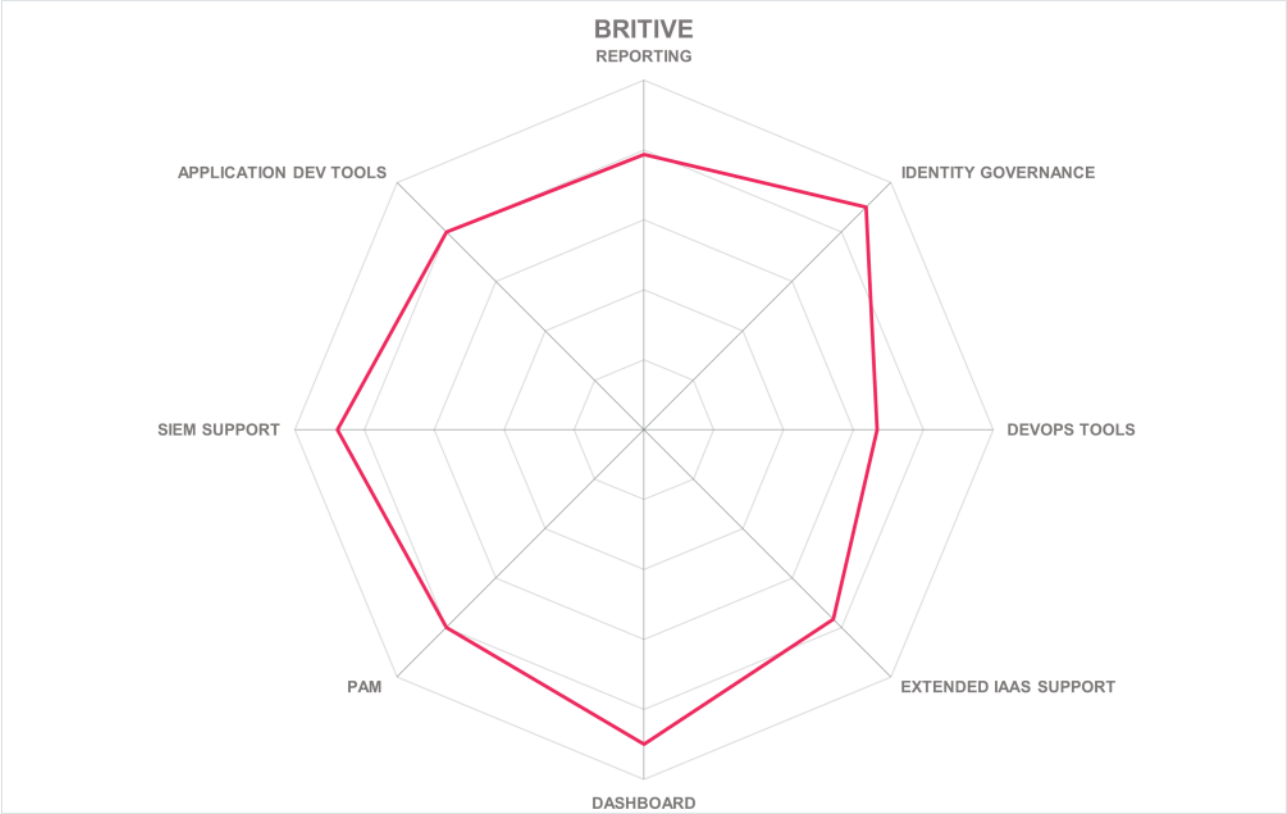
- Supports Data-as-a-Service (DaaS) applications as a bonus for developer environments
- Quite eye opening in the way it supports multi-cloud access especially in high-risk developer environments
- Wide and deep support for IaaS, microservices and containerization architectures
- Retains several classical PAM capabilities to round out its appeal
- Strong support for DevOps tools

Challenges

- In many ways, Britive is anticipating the future with the focus on 100% JIT access, but some organizations may find this a challenge with current infrastructures
- Focus on non-traditional IT experts having admin access in DevOps may be too much for some
- PAM features could potentially be improved in future releases

Leader in




BRITIVE
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.4 CyberArk

CyberArk is a major PAM vendor based in Israel and the United States. It is currently realigning its portfolio of products around the CyberArk Identity Security Platform branding, in a further push away from a market focus on PAM. Within this setup is the new CyberArk Cloud Entitlements Manager, a CIEM based product fully compatible with existing CyberArk applications.

The arrival of CyberArk Cloud Entitlements Manager is preceded by three years development in the CyberArk research labs. It can discover and manage entitlements for machine and non-machine identities as well as service accounts and APIs across AWS, Azure and GCP. Excess entitlements can be terminated, a process that benefits from automation while permissions in use, as well as entitlements that could provide Admin or even so-called Shadow Admin access (not sanctioned a properly sanctioned combinations of permissions that are toxic and could lead to surprise privilege escalation) are highlighted in the dashboard.

The dashboard creates a visual representation of entitlements across the specific Cloud platform that is being analysed. This will showcase what services and permissions that a user or any entity has access to. Recommendations to adjust excessive permissions are sorted by Predictive Risk Analysis and Threat Intelligence built into the platform. CyberArk Cloud Entitlements Manager creates deployable recommendations and remediation steps for an admin to utilize for reducing the risk level for an over-privileged entity. The new application integrates into CyberArk Privileged Access Manager to onboard credentials (if used) to the CyberArk Digital Vault.

Once set up, CyberArk Cloud Entitlements Manager continually scans an IaaS to search for anomalies in entitlements and permissions: Webhooks will be used to notify IT Admins or Managers of changes to items such as Shadow Admin or Admin creation.

Currently, the platform can run on SaaS or on-premises but a move to connector-less model is in the pipeline. Also, under development and mining CyberArk's long experience of managing Privileged Access is Secure Cloud Access and Secrets Hub which will enable connecting public cloud provider's native secrets management solutions, such as AWS Secrets Manager to PAM, either through Self-Hosted or Privilege Cloud environments.

With this new service, developers can continue using native solutions, while security can govern and manage secrets centrally across their hybrid and multi cloud environments using the CyberArk solution. This solution is being developed in close collaboration with AWS. However, this is well behind many smaller CIEM providers who already do this for AWS – and GCP and Azure. It is fundamental to DREAM.

In late 2021, CyberArk added Dynamic Privileged Access capabilities to allow for the brokering of access to ephemeral compute with both SSH certificate signing and as-needed provisioning/de-provisioning just-in-time using attribute and tag-based policies to broker access.

Meanwhile for future development CyberArk says it is moving towards JIT ephemeral access for all identities as standard. This is a good thing for CyberArk's many thousands of customers and for identity and access

management in general.

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

CYBERARK®

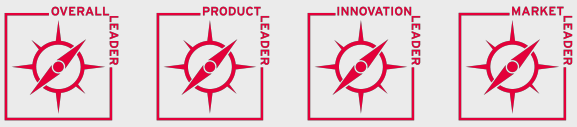
Strengths

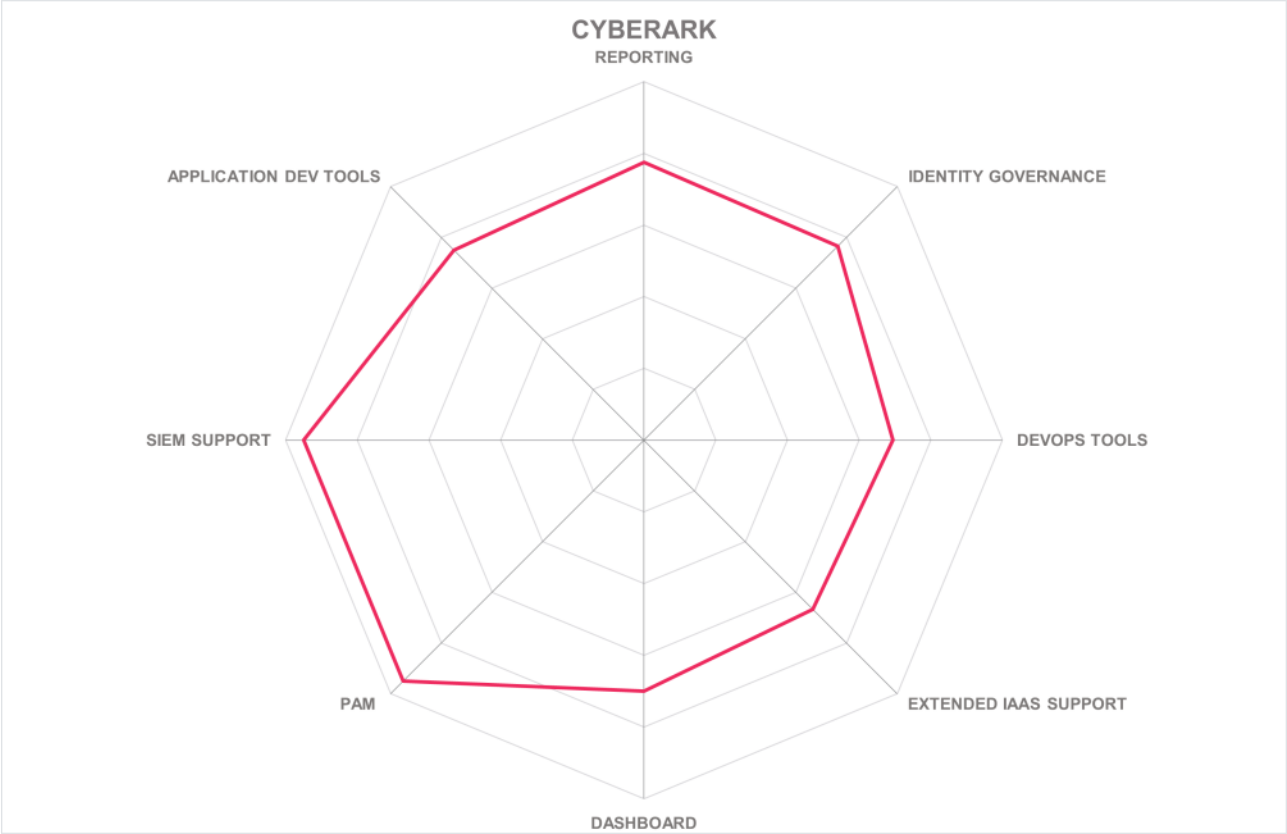
- As would be expected, a huge range of PAM capabilities that are instantly compatible by integrating existing CyberArk products
- Good partner for CyberArk Conjur Secrets Manager which is fully containerized across a good range of providers
- Good range of IaaS provider support including IBM, Oracle and OVH
- Creates deployable recommendations and remediation steps for an admin to utilize to reduce risk level of permissions
- Dynamic Privileged Access capabilities to allow brokering of access to ephemeral compute resources with SSH certificates
- Size and resources mean that CyberArk can fully reengineer its platforms for the new era

Challenges

- Some but not all of CyberArk's products are fully cloud native and support microservices and containers
- Does not yet support any CSP native Key Stores (AWS is coming) which is a major obstacle to seamless cloud management and entitlement
- CyberArk is doing more than its closest PAM rivals to embrace CIEM and DREAM but is already outperformed by smaller cloud native rivals in some key areas

Leader in




CYBERARK
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.5 EmpowerID

Based in Ohio (US), EmpowerID offers several products within its broader IAM portfolio, including EmpowerID Privileged Access Management (PAM). All applications within the portfolio run as SaaS, and EmpowerID software offers fully managed services. The only on-prem component is Cloud gateway on Win 10/11 - this creates the credentials and keys.

For the DREAM environment EmpowerID offers capabilities in Cloud Entitlement Management, some more advanced PAM tools and PAM for DevOps. It has wider than average support for IaaS including the big three providers and Alibaba, IBM, Oracle Rackspace, VMWare, and OVH. All components are offered cloud-native based on a microservices architecture. Container compatibility is also wide with support for Linux and Windows containers.

Full PAM is available for DevOps and the Session Manager Architecture is completely broken out into microservices and fully containerized. There is a standards-based native Identity Provider built into the platform that provides SSO to cloud applications directly from a menu in the dashboard. Other IDPs are supported, and multi- factor authentication can be configured in addition using Azure, Duo, OAuth and mobile-based MFA apps. EmpowerID's expertise in identity management make this a flexible access tool for DREAM.

The applications are also open to customer development with very broad API support and dev tools readily built-in to the platform. For example, there is a built-in tab for Postman, a relatively easy API platform for building and using APIs – a notable plus not just for development of CIEM and DREAM capabilities for EmpowerID software but also to elevate secure access and entitlement flows within DevOps environments. Furthermore, APIs can be used to provide RBAC JIT access to resources for individual entities which more often compute at endpoints in the post Covid eras

The dashboard at the heart of EmpowerID is comprehensive in scope and does more than just open access to cloud services. Other key capabilities include ML supported role mining with automatic clean-up of roles, display of rights granted to roles and the security impact these may have on the organizations. Business functions can be mapped to Azure Groups; for example, purchase Order functions. Whole groups can be switched to JIT access if the role is considered high-risk or optimised for Least Privilege Access.

EmpowerID also has integrated support for SAP which it can connect to directly and manage identities. Discovery tools provide data on standing privileges for identities and ZSP can be easily configured in a window with time restrictions defined. Conversely, end users can reuse JIT access under the same GUI.

Assigning roles across EmpowerID for Active Directory and other services is very clear and very graphical. The experience is the same for ServiceNow, SAP, and other integrations. The Risk Analysis Engine can scan entire stacks to reveal which identities and roles are at risk. An example would be machines which have too many admins. The whole ethos of EmpowerID is to hide the proprietary logistics and IAM tools of all CSPs – what it calls its semantic layer approach - and cloud-based applications and to provide seamless access and control of cloud services. It seems to work.

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

empowerID

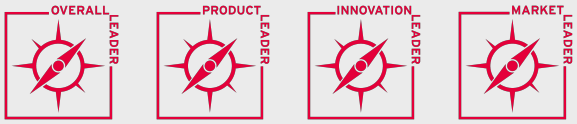
Strengths

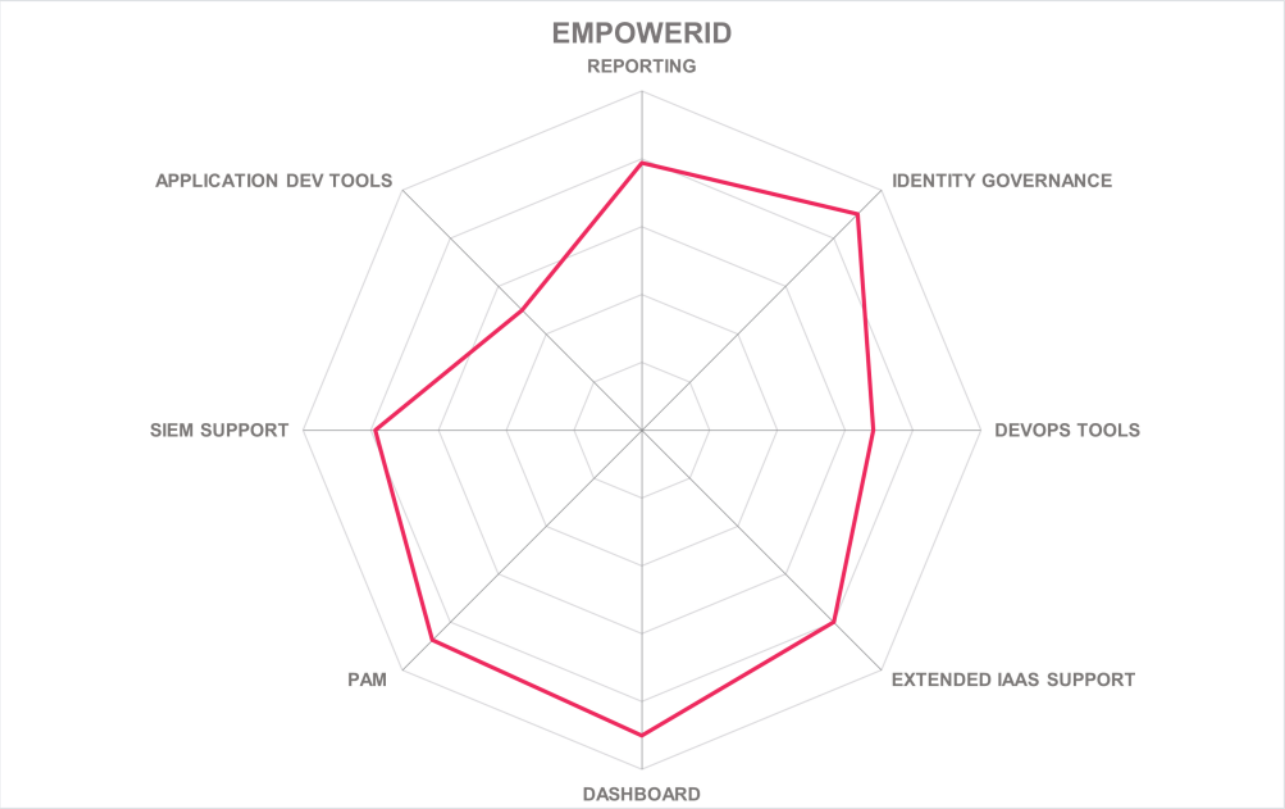
- EmpowerID is really thinking beyond the static nature of classical PAM and ID management with an abstracted layer approach to DREAM
- Excellent GUI out of the box
- Wide ranging IaaS support
- API support includes ability to use APIs to build new functions with built-in support for API development platforms

Challenges

- Needs to expand EPM and PRA support for the era of home working
- We would like to see PUBA and other advanced capabilities added to make this a more rounded option - but given the way market is heading this may not matter to some cloud native organizations
- Still heavily AD and Azure AD focused but EmpowerID is convinced that Microsoft has won the identity management argument in the cloud – others may differ

Leader in




EMPOWERID
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.6 Ermetic

Ermetic, based in Tel Aviv, Israel, was founded in 2019. The Ermetic Cloud Infrastructure Security (CIS) Platform monitors privileged access across AWS, GCP, and Azure clouds.

Ermetic Cloud Infrastructure Security platform is deployed as SaaS and can onboard cloud accounts for analysis within a central dashboard. It supports the three main major IaaS providers. It can list cloud resources and infrastructure using the proprietary terminology – for example it will list EC2 instances under AWS (an instance is a virtual server with different capacities and functions within the AWS universe). Such AWS instances are labelled as Public or Privileged and the associated identities with each type of access are further listed. There is also access to AWS S3 buckets to see who or what has access, and so on.

The platform can expose a full asset inventory across regions, accounts, and divisions across AWS/Azure/GCP – ideal for multi-cloud environments. It provides a granular, contextual visibility into all identities, configurations, permissions, and activities. It also displays publicly exposed (internet facing) publicly exposed resources.

A useful tool also displays the potential attack chain that attackers might use laterally if they were to hijack an identity with access to Private and Public Privileged Access. In this way Ermetic serves as an excellent discovery tool for exposing cloud access entitlements given to identities. This also allows Right Sizing to be adjusted for roles and identities in the different cloud services available.

Another key capability is exposure of over-permissioned identities – increasingly a problem in multi-cloud environments where machine and non-machine identities are granted privileged access on an ad hoc basis. The platform is fully compatible with Okta and other major IDP platforms.

One of the strengths of Ermetic is the ability to go beyond the limited granularity of the major cloud providers, and to overcome the incompatible methods used for IAM in each Cloud Service. There is also access to S3 buckets to see who or what has access.

A Cloud discovery tool is of little use unless you can do something about over privileges and authentication errors, so Ermetic Cloud Infrastructure Security can read/write and delete all permissions.

This can fix over privilege and over sharing of resources – all controlled from the IAM tab in the dashboard. Remediation is possible in the Findings Tab and can be based on the organization's specific security policies. Machine identities can be onboarded and set as Least Privilege before entering any production environment. This is a platform with great promise and worth investigation for specific applications in small and large organizations.

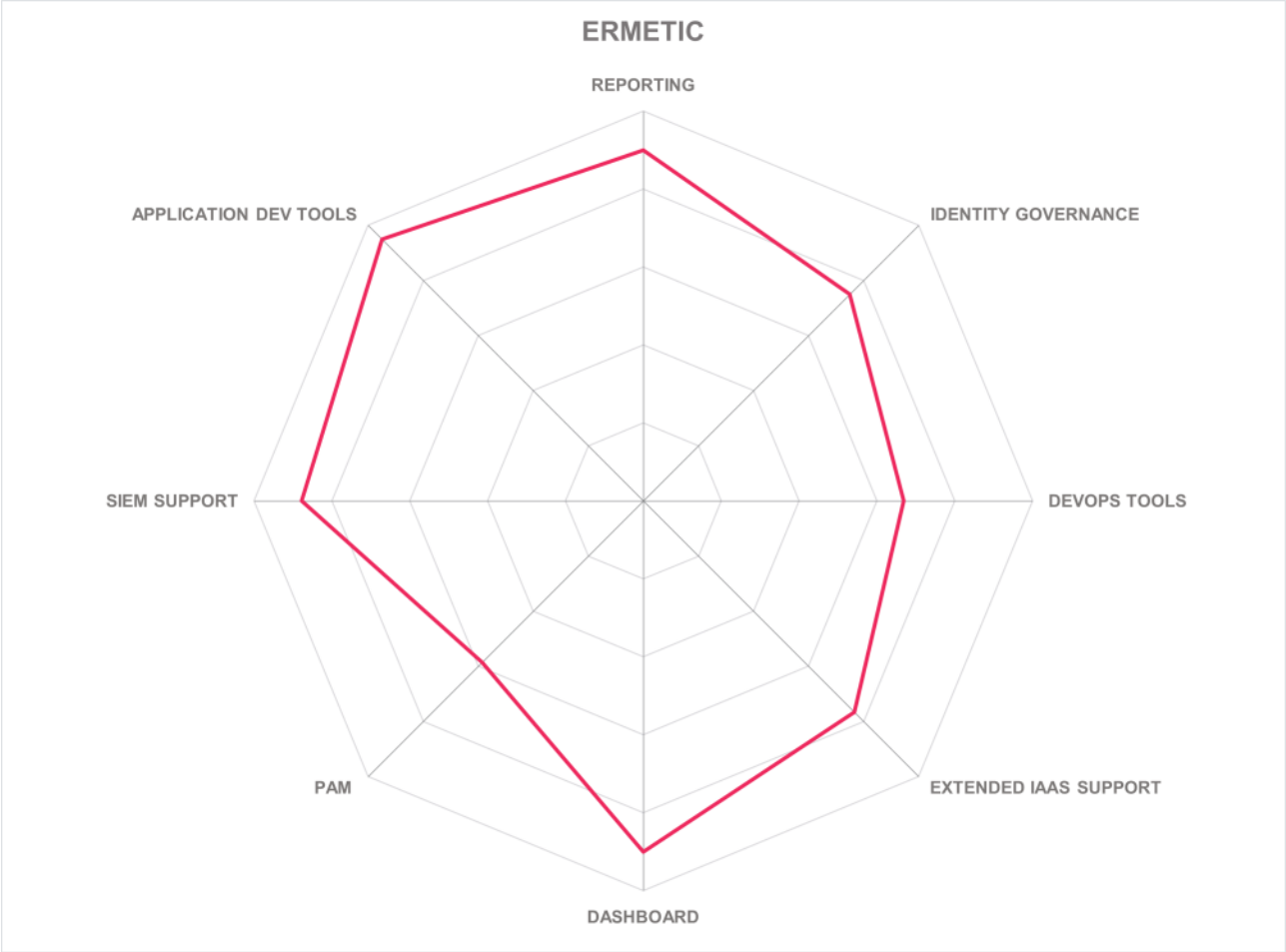
Security	●●●●○
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Does a good job for critical task for managing cloud access & entitlements
- Does well in supporting DevOps and developer needs in the cloud
- Simple to deploy, set up and use – makes good use of latest trends in dashboard and UX design. Tab based navigation a plus.
- Allows managers and admins to rectify over privilege and cloud entitlements
- Will appeal to those departments looking for segmented solutions to specific tasks

Challenges

- Should support more than just the three main Cloud Service Providers
- While supporting elements of PAM for cloud access it cannot compete with major PAM providers
- Ermetic may find it harder to compete if bigger players add similar functionality, but it does have lean cloud native architecture on its side


ERMETIC
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.7 HashiCorp

HashiCorp is a cloud security vendor based in San Francisco. HashiCorp Boundary is designed to improve Cloud Infrastructure Automation and to simplify access management in multi-cloud environments. The platform is currently available as open source, but a SaaS managed service version is in the pipeline, which will broaden its appeal across those organizations less inclined to use open-source components in their environments and wish to leave the running of the platform to other IaaS.

Currently the platform can be deployed on AWS, GCP, and Azure with yet no support for Tier 2 CSPs. But support for third party access where it matters is broad with 11 IaaS platforms including OVH, SAP, and Oracle included. Likewise, its support for container platforms is also wide, with 12 supported including the less ubiquitous such as Pivotal, Mesosphere, and SUSE. HashiCorp recommends that Boundary is not installed on any PaaS platforms.

Boundary itself runs on a microservice-based architecture with three runtime components: Workers, Controllers, and a Database. The Controller provides an HTTP JSON API for users to interact with Boundary and is responsible for all authorization of requests and for recording every change to resources. The Worker creates proxy connections between users and a target. The database provides persistent storage for the Controller. SSH keys, certs, and passwords are all options for authentication processes.

Boundary supports a just-in-time access model at multiple levels: at the network level, where sessions have a Time-to-live value; at the credential level, where Boundary can leverage dynamic credentials from a HashiCorp Vault; or at the RBAC level, giving a good deal of flexibility.
Two key DREAM compliant processes can be automated in the platform: entitlement configuration and enforcement of least privilege across the infrastructure. And privileged account discovery can be set to continuous.

The dashboard is limited in scope for wider analysis with only session monitoring and some analytics available but is not at the level of many PAM providers and needs integration with wider analytics or SEIM tools. Boundary currently integrates with any Identity Provider that supports OpenID Connect protocol (OIDC).

Boundary integrates with OIDC identity providers, SIEM/Analysis tools with Postgres integrations, common cloud providers like AWS and Azure for agentless service discovery, and HashiCorp Vault for integrated secrets management.

The focus of HashiCorp is very much on developer environments (aka App Development Cycle) that wish to spin up servers, apps, and other services across a chosen IaaS. Developers access to cloud infrastructure is via HashiCorp Terraform with no keys/credentials to manage and users never have direct access to target resources – it is always by a JIT proxy connection. Authentication is primarily granted at workflow level and supports API and MFA options. Boundary streamlines access workflows with a REST API for integration into existing workflows and to integrate with other vendors such as IGA. Overall, it is a well-engineered platform with potential for future growth in capability and management.

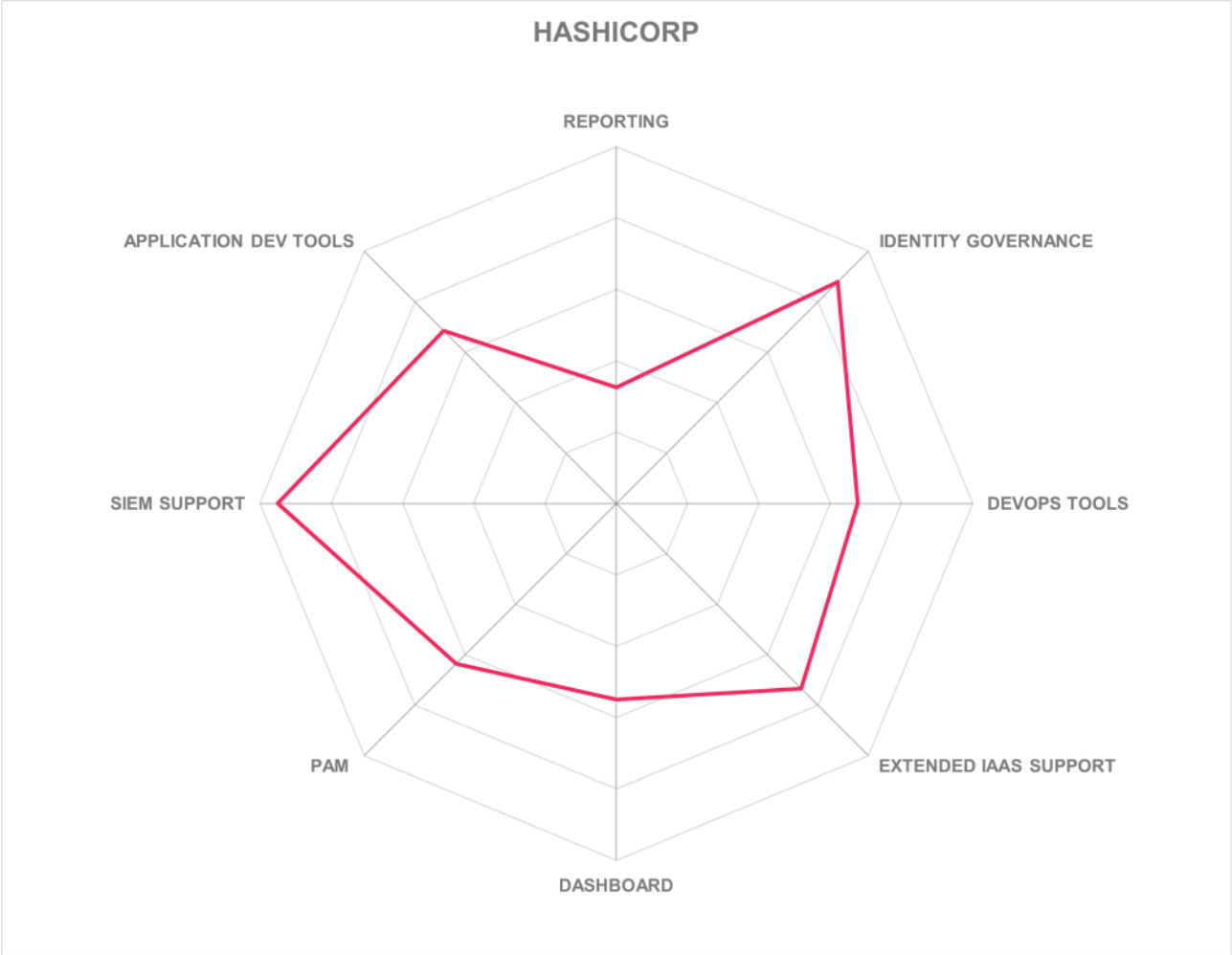
Security	●●●○○
Functionality	●●●○○
Deployment	●●●○○
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Highly focused to agile Dev environments and will accelerate access and entitlement in these
- Works well with other HashiCorp components including Terraform
- Allows fine-grained authentication and authorization secure access to systems in private networks without granting access to the larger network where those systems reside
- Automates significant portions of the secure access workflow with API-driven integrations and automated target discovery to ephemeral resources
- Can be used with HashiCorp Vault to allow isolation of credentials
- Cloud native and huge support for IaaS providers

Challenges

- Lacks extensive analytics and management options
- Is less of a management tool and lacks session management, recording, and forensics that PAM players can offer to this market
- Until the SaaS managed service arrives, some customers may be put off by the open-source origins of the platform
- For those that wish to keep focus on password management for cloud this may not be the right answer


HASHICORP
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.8 Hitachi ID Systems

Hitachi ID, headquartered in Canada, is a global IAM software provider that originated as MTech Information Technology and was acquired by Hitachi in 2008. Bravura Security Fabric components can be run as a service directly by Hitachi (under AWS) or run in the cloud on other CSPs by the customer if the cloud can support Windows and Linux virtual machines. Bravura Security Fabric connects to most target systems using their native APIs and protocols and thus requires no software to be installed locally on those systems.

The platform has extended JIT access capabilities for machine and non-machine identities. JIT access is available for basic Privileged Access to accounts for end users and Admins, and both identity types are shut down after a specified period – thus reducing standing privilege. Shared accounts can be assigned JIT workflow request approval and JIT group memberships can be assigned within the Bravura Privilege Dashboard. In addition, JIT access to federated SAML solutions is enabled.

This in effect allows a single identity access to a group or federate to a system, with elevated rights also an option. While such JIT capability is worthwhile and welcome, the whole platform is still highly reliant on traditional passwords and password management for access - even as HitachID introduces a new cloud native (AWS) secrets management application.

Hitachi ID Bravura Safe secret management is hosted in AWS ECS using serverless hosting strategies - targeted at DevOps types who keep and share secrets in cloud servers. It stores its data on geographically redundant AWS RDS databases and the AWS Elastic File System. High availability is ensured through multiple availability zone hosting within a single region – according to the company. This does indeed provide high availability and security for data in the cloud, but one feels it misses the point of access and entitlement in the cloud. More CIEM capabilities would be useful.

Traditional strengths of HitachiID remain intact. Dashboarding is a single pane, robust and easy to use, but focused on traditional PAM capabilities such as PUBA, session monitoring, onboarding of privileged accounts etc., rather than offering more concrete details on CIEM activities – apart from the provisioning and auditing of entitlement management. It does present cross-account access visualization, automatic discovery and remediation of over privileged accounts, risk scoring, etc.

Bravura Identity Fabric lacks API compatibility to authenticate users to cloud-based resources. While this is on the roadmap it puts it at a disadvantage compared to other platforms in this Leadership Compass.

There are ambitious plans on the horizon which may bring HitachiID Bravura more into contention here and make the wait worthwhile for existing customers. The company is committed to developing more flexible and rapid cloud entitlement and management with its technology partner Elastic – which may go some way to providing the traditional security strengths of HitachID PAM with modern cloud native CIEM type controls.

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

Hitachi ID

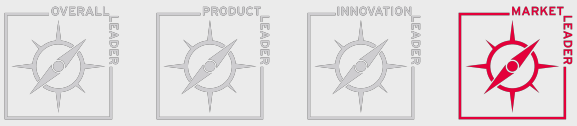
Strengths

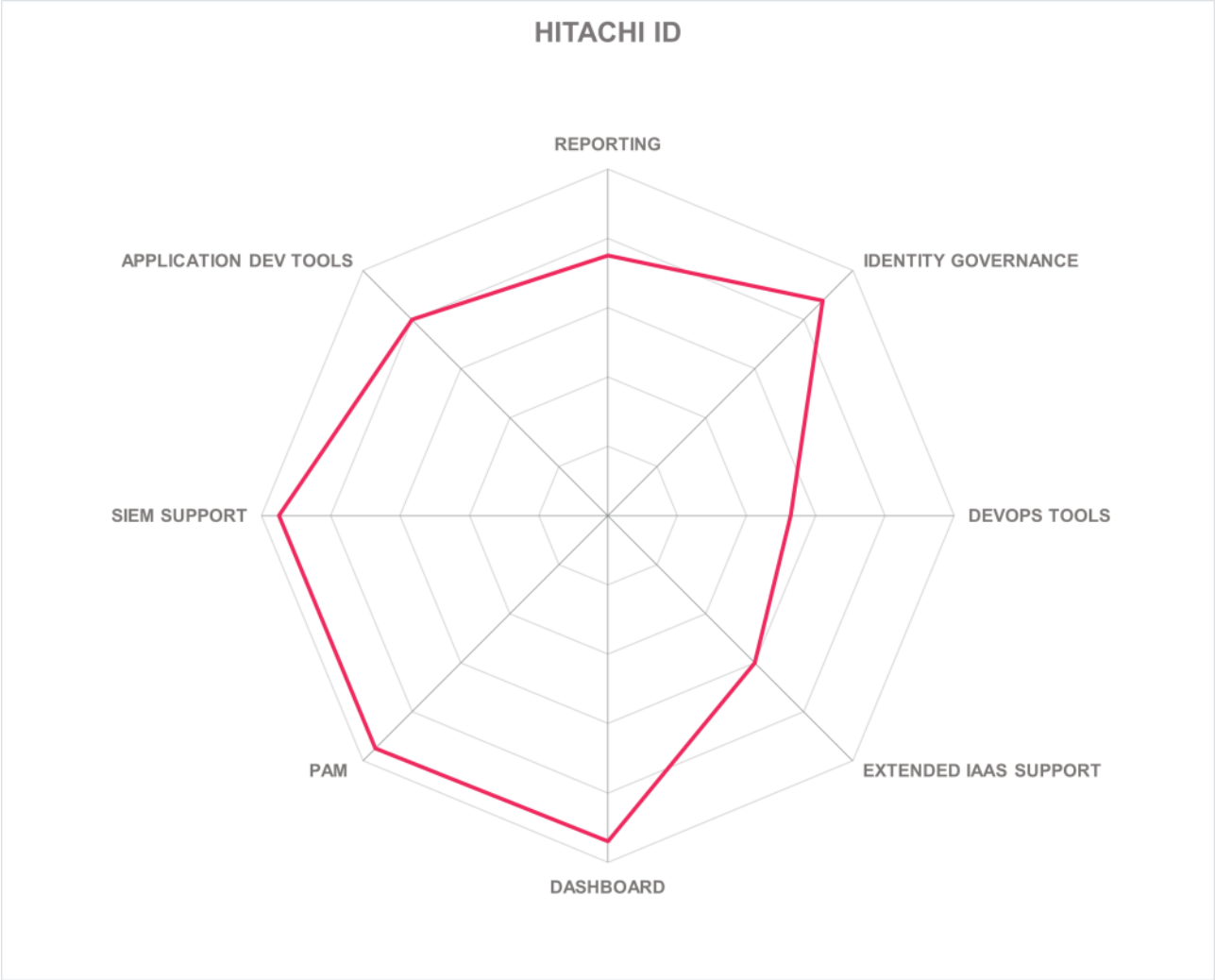
- HitachiID platform is built on proven and tested technology
- Dashboarding is a single pane, robust and easy to use
- Technology partnership with Elastic is interesting and may result in faster rollout of cloud native capability
- Good support of JIT access for machine and non-machine identities
- Cross-account access visualization, automatic discovery and remediation of over-privileged accounts, risk scoring, etc.

Challenges

- Feels in transition between traditional password-based PAM into something more flexible and cloud native
- There is a kit of parts and knowledge available here that may eventually lead to an effective DREAM solution - but not quite yet
- Lacks API compatibility for authentication to cloud resources

Leader in




HITACHI ID
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.9 NextLabs

NextLabs provides data-centric security software to protect business-critical data and applications. It is based in San Mateo, California. Taking a zero trust approach to access and entitlement management across cloud, NextLabs focuses on managing access to data and data lakes across AWS, Google Cloud and Azure and other cloud infrastructures. NextLabs cloud-native products are built on the Kubernetes containerized architecture and support hybrid and multi-cloud deployment model. The company says that 40% of its customers deploy AWS currently.

NextLabs Control Centre is a cloud authorization service for dynamic entitlement and access management. It is a centralized platform that enforces access and entitlement policies consistently across the enterprise and beyond.

The platform is powered by NextLabs' dynamic authorization policy engine (XACML compatible) in which entitlement and access rights to an organization's IT infrastructure, applications, data, and other sensitive assets in the cloud and on-premises are granted dynamically in real-time via attribute-based policies.

Accessed from a single pane of glass dashboard, NextLabs Control Centre provides an unusual combination of CIEM along with data governance and data classification features on which to build policies to control access to cloud resources. NextLabs maintain several policy administration, analysis, and audit tools to support the increasing importance of policy governance.

There is out of the box Support for Docker, Terraform, OVA / OVF, AMI, Kubernetes on EC2, Azure VM, Google Cloud VM, EKS, AKS, GKE, and OpenShift. The platform is engineered to fit policy to entitlements and access to cloud infrastructure and data held there. NextLabs also offer a Policy Engine sidecar for microservices access enforcement to control authorization in a service mesh architecture using centrally managed policy.

NextLabs can support both structured data and unstructured data payload. Unstructured data support is especially useful for engineering and big data analytics.

The platform can deploy on-premises or as SaaS and can access resources running on AWS, Azure, Google Cloud, IBM Cloud Salesforce, and SAP OpenShift and VM Ware cloud infrastructures. There is strong support for container orchestration services including different interpretations of Kubernetes, but modern cloud support also extends to Infrastructure as a Code (IaC) and proprietary cloud monitoring services from AWS, GCP, Azure, and other CSPs. There is also support for SIEM platforms Prometheus and Splunk.

NextLabs Control Centre integrates with third-party Identity Providers (SAML & OIDC based) such as Azure AD, Google, and Okta for authentication. The Policy Engine within the platform can capture data and logs and send to a SIEM platform or a lighter logging app. The platform can also discover service accounts and API entitlements.

Entitlement configuration, permission management, least privilege enforcement, auditing, and alerting can

be automated. Alerts are generated for ghost permissions, excess permissions, and excess privileges. This is a solid package with some unique data governance options.

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

NEXTLABS®

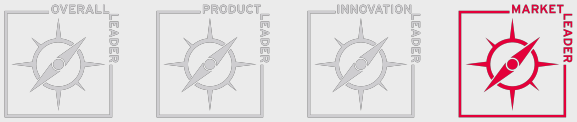
Strengths

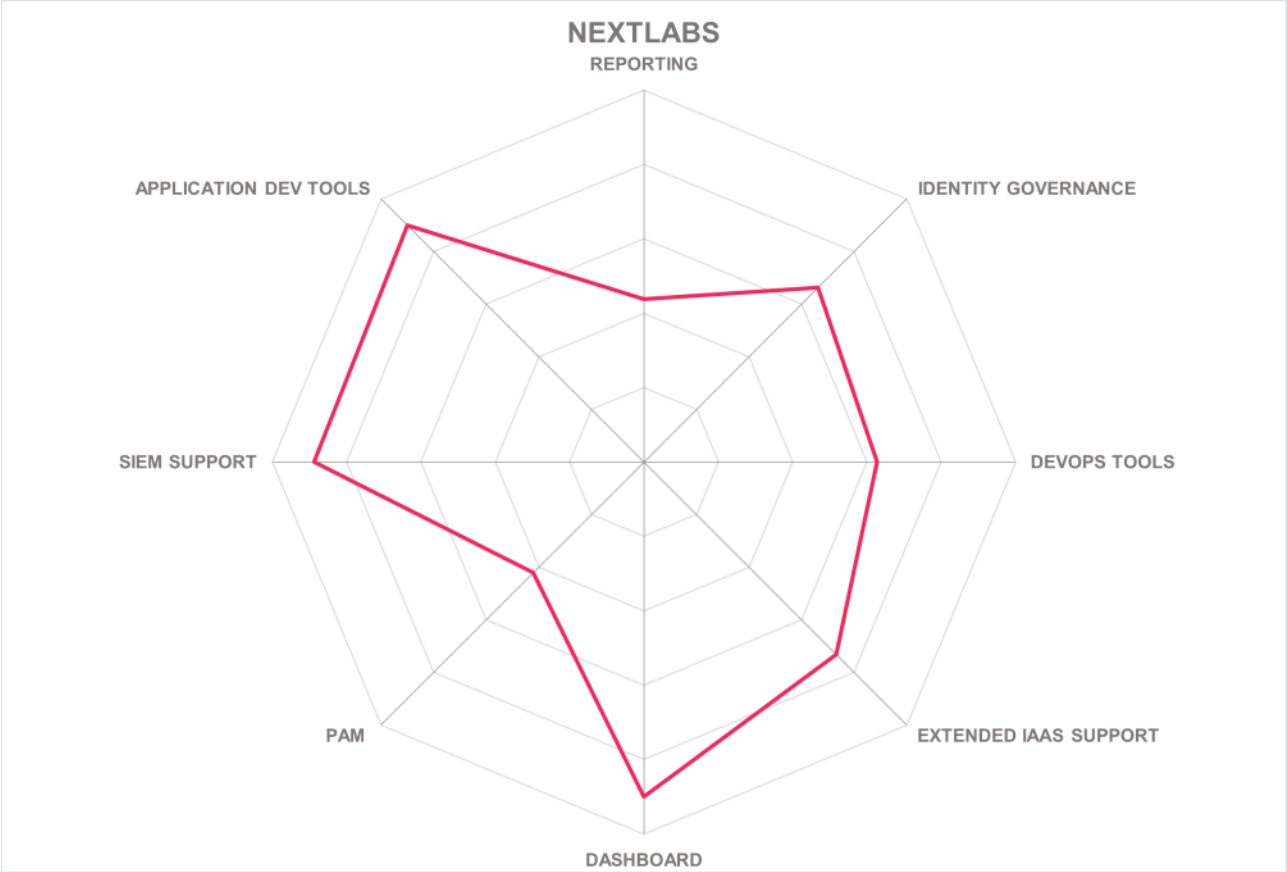
- Comprehensive cloud management tool based on policies which also includes useful data governance tools
- Can automate Least Privilege enforcement across a cloud infrastructure
- Zero Trust Architecture with strong support for third-party Identity Providers
- Out of the box Support for Terraform, Kubernetes on EC2 and Azure VM
- Unique use of containers to segregate and manage access to data
- Supports proprietary cloud monitoring services from AWS, GCP, Azure and other CSPs

Challenges

- Many CIEM analytics and admin capabilities missing
- Not suitable for those organizations with large numbers of standing privilege accounts

Leader in




NEXTLABS
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.10 ObserveID

ObserveID is a start-up software company launched in 2021 and based in Los Angeles with a strong focus on CIEM. Its solution is aimed at hybrid and multi-cloud architectures enabling real-time identity management, automation, and governance. Being this new, the code behind the platform is fully cloud native and the platform is available as SaaS and as a managed service directly from ObserveID itself.

ObserveID Platform is offered in two formats: for enterprises with existing IGA/IAM/PAM solutions, by piggy backing on those and increasing functionality through automation of access to the cloud - thereby improving their ROI and operational efficiency; and for greenfield organizations looking for a CIEM solution that includes lightweight PAM and IGA functionality.

ObserveID is agentless solution and offers integration with Azure, AWS, and GCP, with Oracle support coming later in 2022. There is currently limited support for containerization with Kubernetes, Docker, and Azure AKS on offer. There is some third-party SIEM support but only those through the AWS and Azure marketplaces or via syslog.

The well-designed dashboard provides good insight across IaaS including Cross-Account Access visualization, remediation of over-permissioned identities (user, role, group, and resource) to create least privileged roles, delivery of on-demand and Just-in-Time permissions which are time and resource bound, plus risk scoring and over-privilege discovery for machine and non-machine identities. Like other dashboards it hides the proprietary connectors of the three main CSPs and allows insight into usage of cloud by identities and by presenting information in a single window.

The full range of entitlements can be discovered for all identity types and there is wide automation of functions including entitlement configuration, provisioning and permission management, scale of enforcement policies, least privilege enforcement, and alerts for suspicious behaviour. Privileged accounts cannot be automatically discovered, however.

This is fundamental tool that does the basics of CIEM for popular IaaS demands but needs wider IaaS coverage and more reporting capabilities to go further towards managing more complex cloud infrastructures. But a lot is already delivered in a short space of time, especially in the automation of identity management chores and log management. If ObserveID can maintain its current technical growth trajectory with rapid customer acquisition it could be a major player in CIEM sooner rather than later.

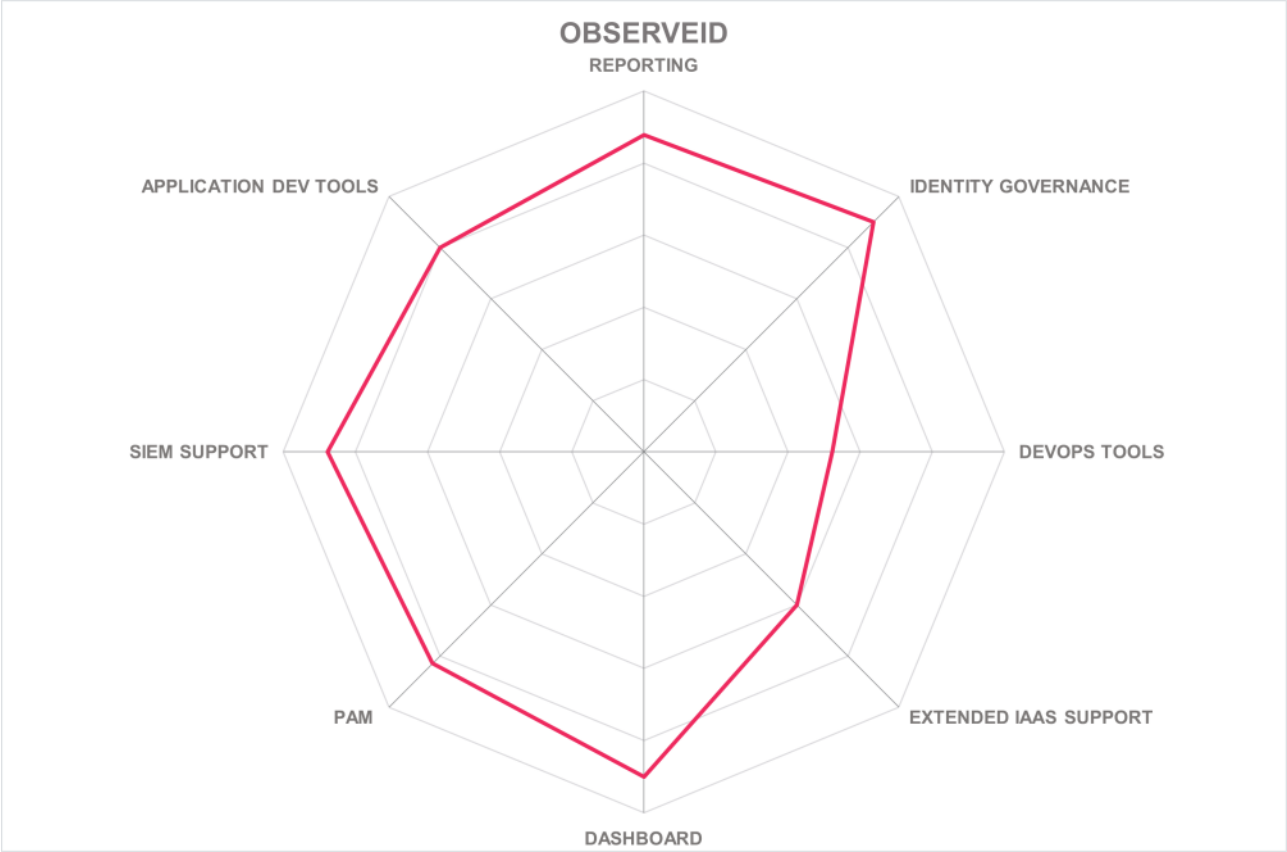
Security	●●●●●
Functionality	●●●●○
Deployment	●●●○○
Interoperability	●●●●○
Usability	●●●○○

Strengths

- Useful automation and integration of existing PAM/IGA/IAM tools
- ObserveID support Hybrid infrastructure - major CSPs along with traditional on-premises infrastructure
- Has some basic PAM tools of its own useful to smaller cloud native organizations
- Access changes can be configured on behavior patterns and risk scores
- Wide range of entitlement discovery for machine and non-machine identities
- Given how short as time the vendor has been established a lot has been achieved in terms of functionality

Challenges

- Vendor is very new and still in early-stage growth, no established customer base
- We look forward to greater DevOps and developer CIEM features to take advantage of cloud native architecture
- Standing privileged accounts not discoverable


OBSERVEID
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.11 Palo Alto Networks

Palo Alto Networks is a cybersecurity software vendor based in California. Palo Alto Networks Prisma Cloud is designed to protect resources stored in multi-cloud environments. The platform can monitor and regulate access and activity within the major IaaS providers including AWS, Azure, GCP, and IBM as well as AliBaba and Oracle. This is supported by strong support for microservices and Infrastructure as Code (IaC) targets across cloud infrastructures.

Palo Alto Networks Prisma Cloud offers deployment options based on customer need; either as a SaaS option or a self-hosted solution that users deploy and manage. The self-hosted version is suitable for use in air-gapped and isolated environments. The wider platform is built around APIs, which lets users configure custom integrations as they wish. The platform uses agents and agentless processes for deployment. Agents are required for the workload prevention?capabilities, for other capabilities, including CIEM and CSPM it is API based with no agents needed.

While support for cloud infrastructure is broad and deep, what sets this package apart is its logging and monitoring activities that go granularly across several proprietary cloud monitoring tools such as Amazon Cloudwatch, Azure DevOps Services and proven SIEM tools such as Splunk and Prometheus (for monitoring container activity).

The focus is also on highlighting GRC issues that arise from poorly configured cloud access and entitlement. For example, it can highlight unused permissions and the parameters can be set across organizational or department admins. The dashboard gives a quick view measurement of compliance risk and , typical of an excellent UX and single pane of glass . Some compliance standards come out of the box, but customers can create and apply custom policies.

The platform compiles data from flow logs, configuration logs, and audit logs over an encrypted connection to provide granular telemetry and maintain historical context for incident investigation and forensics. Teams can then use the console or APIs to interact with this data to configure policies, investigate and resolve alerts, set up external integrations, and forward alert notifications.

An absolute highlight of this platform is its unique (in this Leadership Compass) software governance capability (Software Supply Chain Security) – with a feature that allows bugs or flaws in code to be highlighted (e.g., in Visual Studio) and fixed within the Prisma Cloud platform. That is genuine innovation. At the same time other development environments are supported; for example, a fix request can be submitted into the Palo Alto Networks Prisma Cloud dashboard, and it will be fixed in GitHub.

For the roadmap Palo Alto Networks is planning advance capabilities to improve permission creation lifecycle, further focus on DevOps capabilities, and implementation of zero trust and zero standing privileges?approachThis platform is an extremely powerful logging and monitoring tool for managing activities across multi-cloud environments including deep support for workload needs, and it adds to Cloud GRC capabilities well.

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

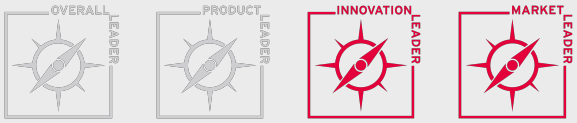
Strengths

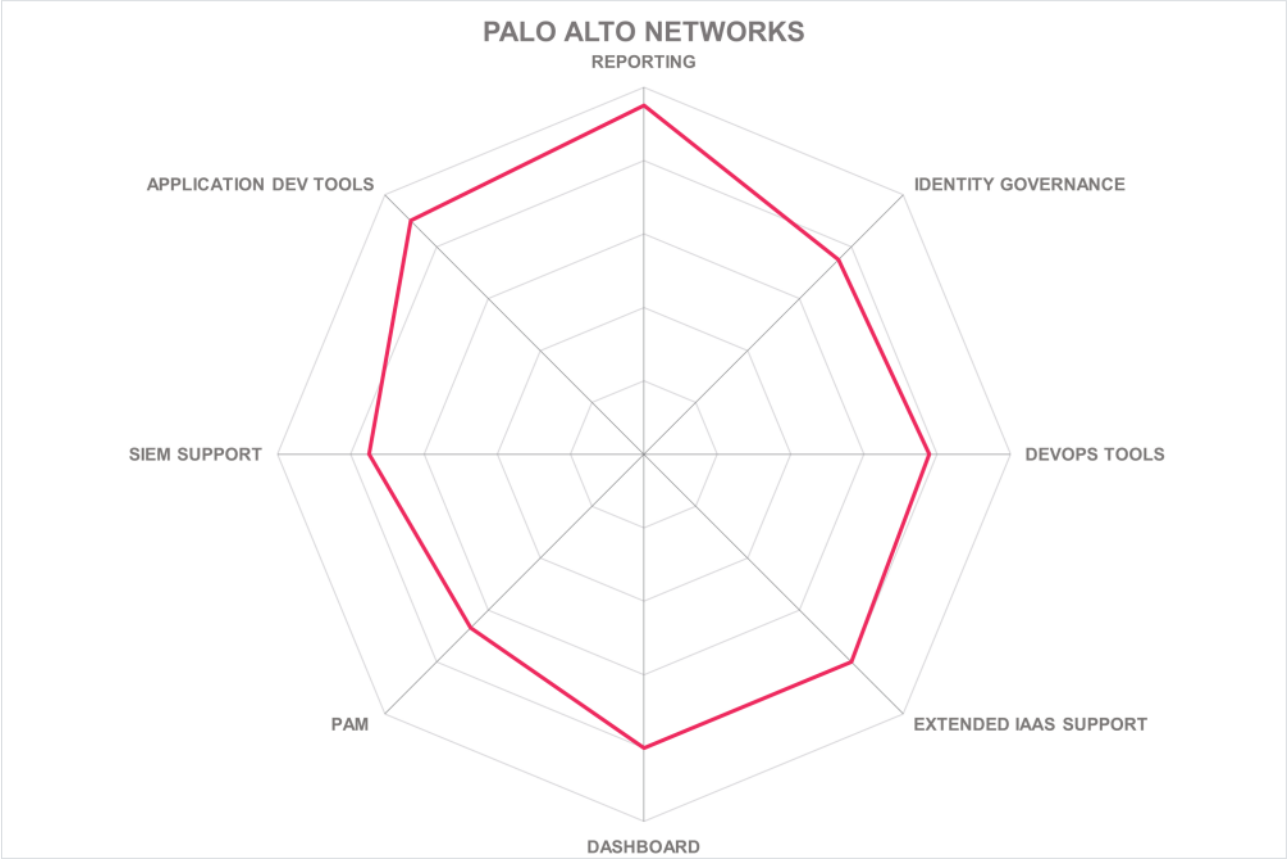
- Unique software governance capability (Software Supply Chain Security) –allows bugs or flaws in code to be highlighted and fixed within the Prisma Cloud platform.
- Logging and monitoring activities that go granular across several proprietary cloud monitoring tools such as Amazon Cloudwatch
- Highlights GRC issues that arise from badly configured cloud access and entitlement
- Neat dashboards with some consumer like touches to check compliance
- Compliance standards come out of the box, but customers can create and apply custom policies

Challenges

- We look forward to the deeper DevOps support in the roadmap
- No PAM based capabilities, but this may not matter if it can integrate with third parties in future

Leader in




PALO ALTO NETWORKS
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.12 Remediant

Based in San Francisco, Remediant was founded in 2013. Its SecureONE product has agent-less and vault-less technology at the core of its PAM platform that provides JIT access for all privileged accounts, abolishes shared accounts altogether, and stores no credentials at all. In the context of DREAM, this JIT approach to access and workflow rights may be an advantage.

Key to SecureONE functionality are three named Insight dashboards that give granular levels of Privileged Access Discovery: Privileged Users, Access Segregation, and Cumulative Access. The Privileged Users dashboard shows admins and IT security leaders point-in-time data on the total number of users given privileged access either directly or as part of a group and to which domains or servers. Those groups or users shown to have excess privilege can be paired back over a set timeline (days to months).

More granular data is available in the Segregation Access dashboard which graphically displays standing privileged access across tiers – such as domain, servers and workstations and from that work out those users who may be most at risk from compromise. Those users can then be replaced with time-limited JIT access , which is the heart of SecureONE.

Finally, the Cumulative Access dashboard showcases total number of privileged users based on a combination of workstations and servers across the IT infrastructure. Again, too much standing privilege access to network entities can be replaced by JIT access. Taken together, these dashboards can reveal excess privilege and assist on a journey to reduce standing privilege to zero.

The focus is currently very much on Privileged Access, but CIEM functionality is coming with indication of IaaS and Salesforce resources being included in the dashboards and discovery process. All dashboards are continuously updated to detect changes in access rights. The package works well in a world where privileged access is not necessarily being granted by admins but by users setting up their own resources and workflows, hidden from the executives.

SecureONE has further refined its integrations with EDR/XDR platforms from SentinelONE, VMWare Carbon Black, and CrowdStrike to interrogate suspicious access. A new Investigate Session button takes admins to any of the supported EDR tools between start time and end time of a JIT session and details what happened, what files were touched, what DNS lookups happened, etc. Bad users can be blocked by EDR in future. Remediant Policy Management and Enforcement Automation support heavy DevOps workflows.

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

It also supports role-based access control as well as attribute access control – however it lacks dedicated support for some more traditional advanced PAM capabilities such as AAPM. This is where pure JIT may fail for larger organizations that still need to vary privilege access safely.

Remediant now offers a SaaS deployment option for an API first multi-tenant architecture, with full microservices support. This SaaS version is offered to MSSP and MSP markets too.

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

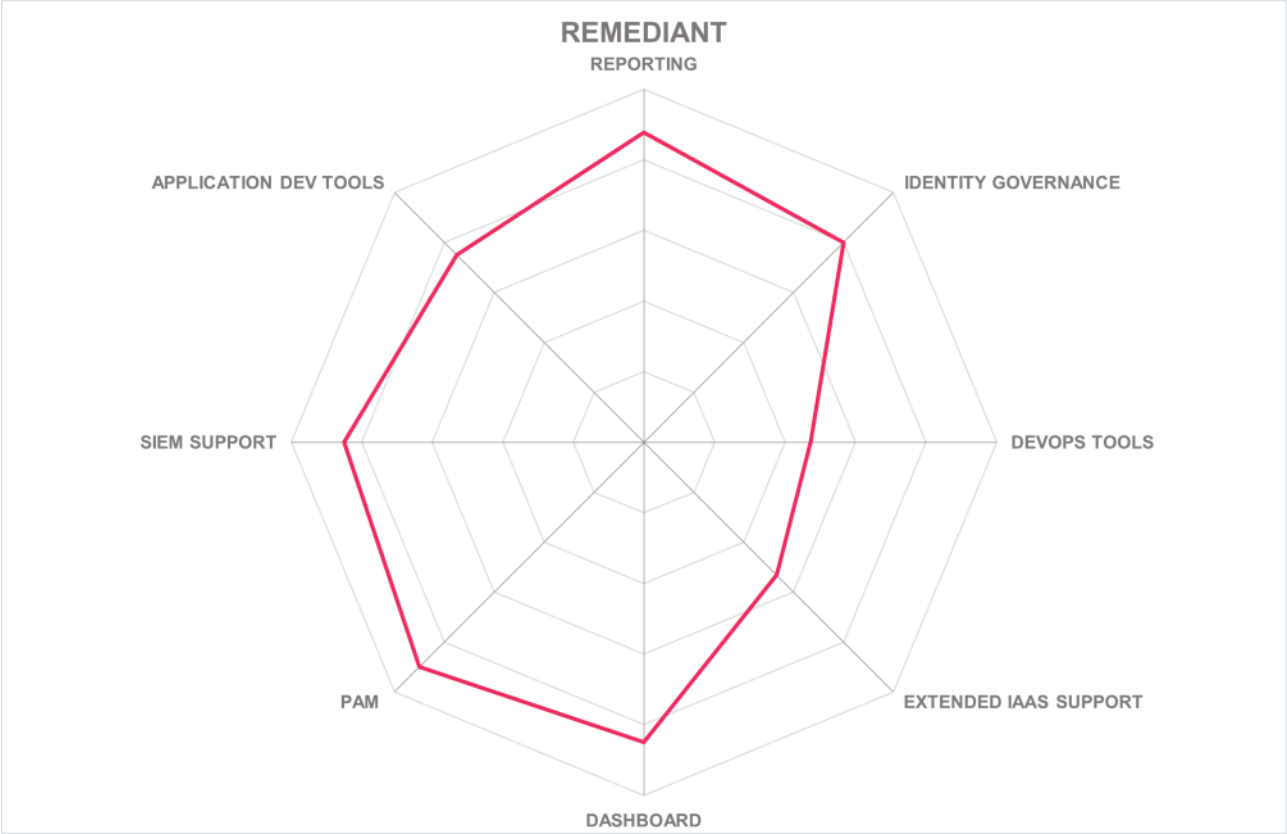
Remediant

Strengths

- Remediant has strengthened its core product with improvements to dashboarding and capabilities
- Tools provide a robust and intuitive method to manage privileged access to domains, servers, and workstations and to eradicate excess standing privileges
- For those organizations looking for an effective tool to convert most of the privileged access to JIT this platform should be on a short list
- Strong integration with leading EDR/XDR platforms neatly ties PAM to those platforms' strengths and new forensics capability finger points bad actors
- CIEM focused functionality fits neatly into the dashboard approach with integration possible for IaaS and SaaS applications

Challenges

- Those looking for a more traditional PAM solutions within DREAM may want vaulting, in depth analytics, SAPM and other capabilities, etc.
- We hope that Remediant adds to the IaaS and SaaS access management capabilities quickly as the pure JIT approach suits the needs of agile well
- More granular analytics capabilities would be welcome if SecureONE is to manage entitlements and access to wider parts of cloud-based infrastructure


REMEDIANT
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.13 SailPoint

SailPoint is based in Austin, Texas. SailPoint Cloud Access Management is designed to regulate access in multi-cloud environments. The company is known for its Identity Governance platforms. SailPoint Cloud Access Manager taps into that accumulated knowledge to offer a core set of capabilities for CIEM.

Due to the extensive support for IaaS and deeper cloud architectures that SailPoint IGA solutions already provide, SailPoint Cloud Access Manager is compatible Tier 1 and Tier 2 CSPs. Support for container-based deployments is less comprehensive (Kubernetes, Docker, Goggle GKE, HashiCorp Nomad, Amazon EKS, and Azure EKS), making this more suitable to managing identity entitlement for end users and less so for machines, particularly in DevOps environments. Proprietary entitlement and identity protocols of the three main CSPs are supported natively.

On the other hand, the level of support for entitlement discovery is good, and includes machine identities, service accounts, APIs, and RPA workflows. Support for SIEM is a major strength with 10 mainstream third-party applications supported – which would be expected form SailPoint but does add an extra layer of useful functionality to the platform. All SailPoint solutions provide support for AzureAD and Okta federation tools and wide support for well-known PAM platforms – making this potentially integrate well with legacy IAM applications among customers.

Cloud Access Management visibility includes insight into over-permissioned identities (user, role, group, and resource) to create least privileged roles/policies, privileged account discovery, over-privileged discovery, usage behaviour analytics, and cross account access visualization plus reporting available out of the box.

The capabilities found in SaaS Management put it quite close to the leaders in CIEM. This can shine a light on shadow IT usage in SaaS, access risk, open up SaaS visibility, and improve control efficiency.

The dashboard simplifies access visibility with an interactive graphical map of access, from identities to entitlements to resources. It can identify excess privileges and right-size access by finding unused and sensitive entitlements scattered across the multi-cloud environment. SailPoint continues to integrate with PAM providers and SailPoint will invest more into adding PAM type capability into areas such as SCIM, an area in which it has expertise.

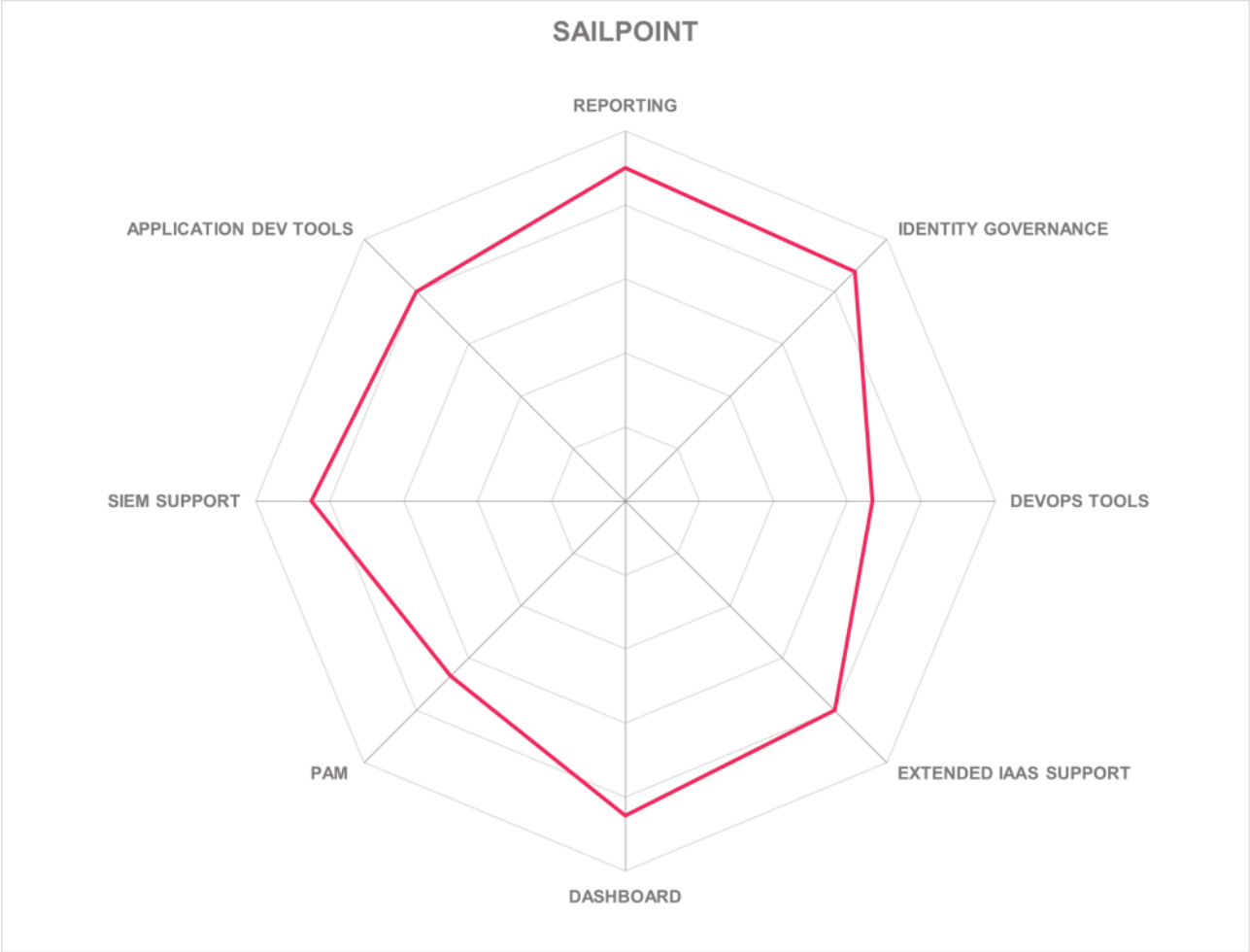
SailPoint

Strengths

- Strong support for entitlement discovery and privileged accounts
- IGA heritage plays well here as would be expected
- Fine dashboard with graphical displays of risk and access data
- Solid support for Tier 1 and Tier 2 CSPs and mainstream orchestration platforms
- SaaS monitoring capabilities close to the best of CIEM specific platforms
- Useful for identifying unused cloud entitlements

Challenges

- Strong on identifying human identity activity, less so for machines
- SailPoint has an opportunity to meld its IGA and PAM experience into a leading DREAM compliant platform


SAILPOINT
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.14 Saviynt

Saviynt is an IAM vendor based in El Segundo, California, founded in 2015. Saviynt delivers IAM solutions through a converged, SaaS-based platform called Enterprise Identity Cloud (EIC). The platform comprises five products - Identity Governance and Administration (IGA), Cloud Privileged Access Management (CPAM), Application Access Governance (AAG), Third-party Access Governance (TPAG) and Data Access Governance (DAG) and powered by an intelligent identity warehouse.?

Saviynt EIC is a SaaS platform delivered on public cloud platforms: GCP, AWS, and Azure. Saviynt designed the solution to be fully cloud-native and to utilize APIs to integrate with as many leading enterprise applications as possible. The platform has built-in Cloud Entitlements Manager (CIEM) features - which is hugely beneficial for keeping a record of complex cloud usage (scaled up and down), and for agile and fast-moving DevOps environments. In addition, as part of its converged Enterprise Identity Cloud (EIC) platform, Saviynt's cloud PAM has access to fully compatible IGA features.

While Saviynt Cloud PAM resides in the cloud, customers can control usage and management from consoles that sit on-premises, in the cloud, or in hybrid stacks. Account discovery, session recording and session management as well as more advanced features such as Risk Analytics, credential-less access, and a risk and controls library are all accessible from the dashboard. The web-based interface is designed to be user-centric, and in this, the company has succeeded in creating a very clean and simple interface, in line with current practice.

Other notable features include continuous discovery of cloud workloads and entitlements plus always-on monitoring of services and workloads for security errors or misconfigurations. A new Risk Exchange tool allows bi-directional data integration with leading 3rd-party solutions from SIEM and Vulnerability Management vendors.

The platform has the extensibility to aggregate the full entitlement information from all identities and the processing power to analyse entitlements and data in into a single hub. Saviynt is addressing the increased importance of DevOps, CI/CD, and Infrastructure as Code (IaC) teams within organizations. Its pipeline includes plans to change the way DevOps code deployment entitlements are managed by switching the focus from managing access in the OS (via SSH/RDP) to managing commands in orchestration software such as Terraform (or similar), with changes deployed in updated containers.

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

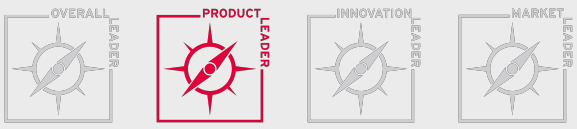
Strengths

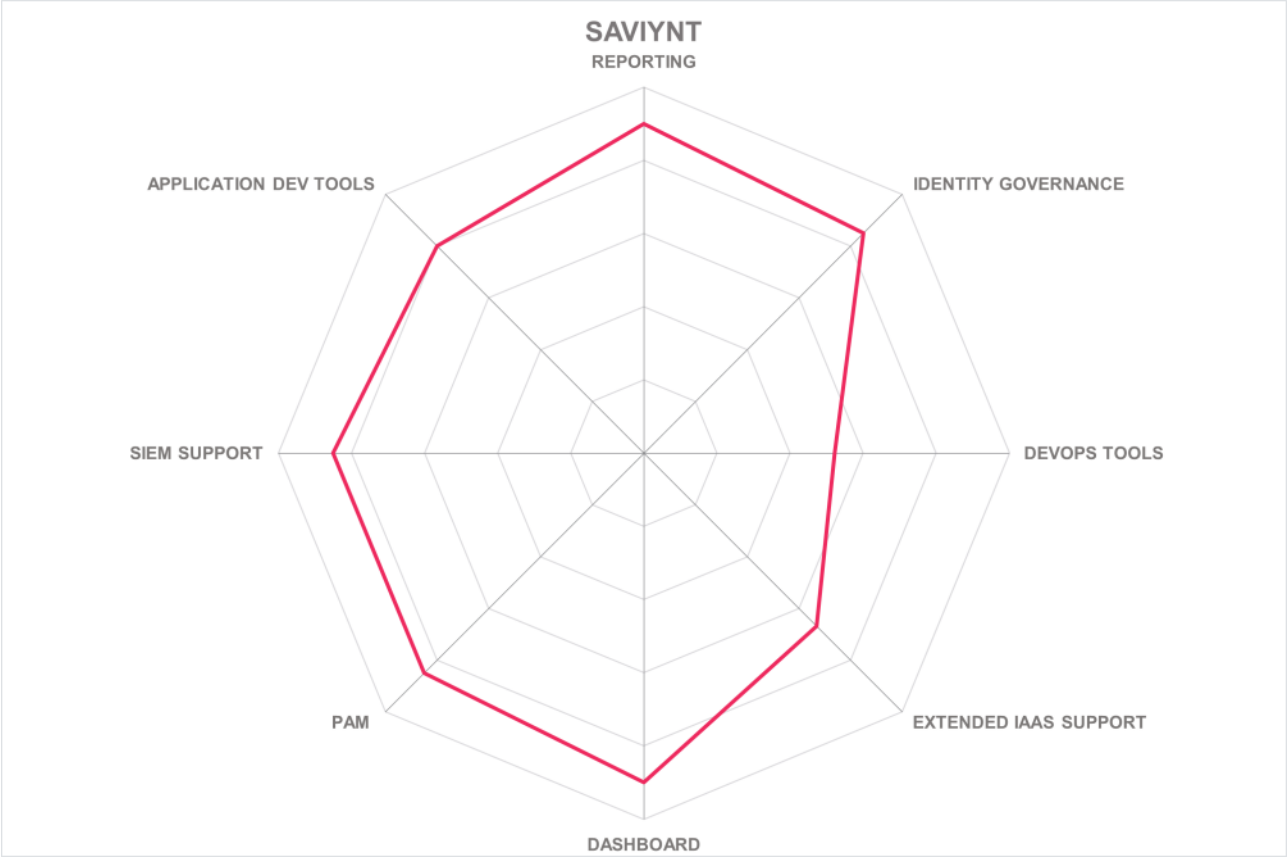
- Integration of designed-in CIEM functions takes PAMaaS to a new level
- Strong reporting from well-designed dashboards
- The company has exciting plans to embed access management within code and infrastructure layers dispensing with permissions at the application/OS layer
- A good step towards reducing reliance on passwords
- Good control of redundant IDs and unused passwords
- Solid DevOps tools and improved Machine Identity capabilities

Challenges

- Saviynt may wish to explore a completely password free platform in the future
- This is a solid and innovative platform that now needs effective marketing to increase its customer base
- This is a fresh approach to PAM which as markets transition to hybrid PAM/DREAM applications may well pay dividends

Leader in




SAVIYNT
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.15 Sectona

"Sectona is a PAM vendor based in Mumbai, India with a regional office in Dubai, United Arab Emirates. Sectona also has regional offices in Europe, Southeast Asia and Africa Sectona Security Platform is focused on PAM for cloud environments and offers continuous discovery of privileged accounts with JIT access. The company has moved to a decentralized platform approach to PAM and cloud access by decoupling components such as Secrets Management, Single Sign On, and Privilege Escalation.

The new platform delivers a dashboard providing user authentication for remote & privileged users, access to cloud consoles (admin and non-admin), hybrid resource discovery across multi-cloud environment (but not yet entitlement discovery), proxy-based access to multi-cloud resources using least-privileged-based and JIT techniques, and dynamic secrets management for AWS & SQL Databases. There are also strong PAM capabilities such as PUBA, automated discovery of privileged accounts and privileged escalation. Multi-cloud support for key cloud platforms for AWS, Azure, and GCP, a compliance engine to fix violations against security best practices, and dashboard risk alerting for anomalous activities are present.

Sectona has improved its JIT capability with Zero Standing Privilege (ZSP) support. Privileged Task Management (PTM) now allows scripting of SSH and PowerShell commands to automate routine tasks while Privileged Account Lifecycle management is now fully accessible from the Management Console. A highlight of the platform is session risk scoring for threat analysis which gives an at-a-glance view of performance against pre-existing security and data theft categories

It is up to speed with features such as adaptive authentication, which will become more common on PAM in the future, as well as Application to Application Password Management (AAPM) by using APIs and SDKs for many platforms. Sectona platform components also include a web access layer, and the Vault supports high availability with multi-site and cloud-native architecture support for deployment. Proxies can be spread across multi-cloud environments to support the desired functionality.

Sectona is planning to release a lightweight CIEM in the next 12 months. This should be promising given the cloud-native nature of the existing PAM components and capabilities. The full CIEM piece is 8-9 months away according to Sectona. We look forward to that rounding out this platform.

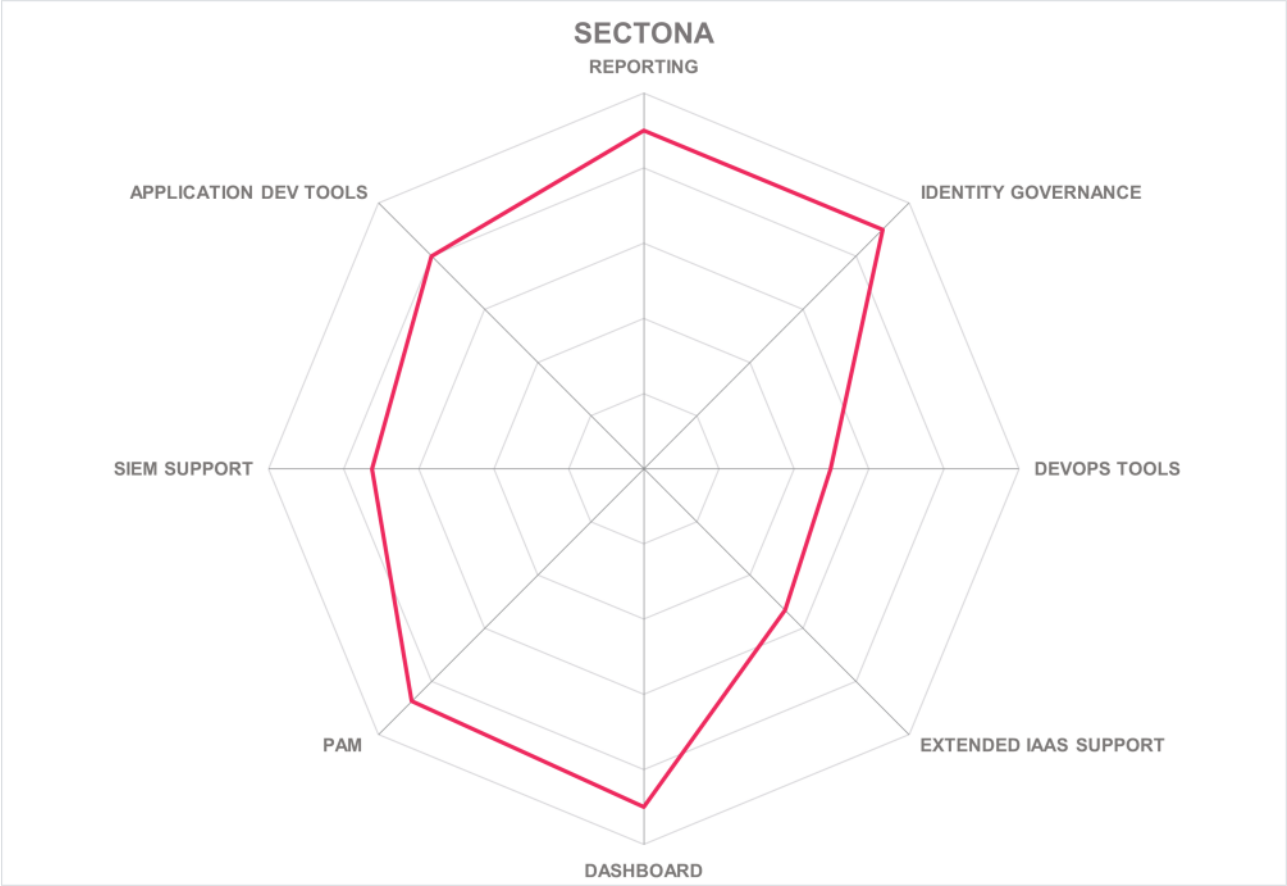
Security	●●●●●
Functionality	●●●●○
Deployment	●●●○○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- Strong support for authentication standards and protocols for both machine and non-machine identities, and hardware tokens too
- Useful dashboard with wide functionality and reporting capabilities
- Strong automation tools as standard
- Strong focus on machine identity management
- Well featured for managing privileged access in the cloud

Challenges

- Remains PAM platform that improves privileged access to IaaS, but some way from a fully featured tool for DREAM or CIEM
- Limited cloud support in its current iteration, we look forward to wide compatibility when the CIEM module arrives
- Limited but growing DevOps supportCannot discover human identity cloud entitlements


SECTONA
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.16 Senhasegura

Based in São Paulo, Brazil, MT4 Tecnologia produces Senhasegura as its flagship access management portfolio. Comprised of multiple modules, Senhasegura already offers comprehensive PAM capabilities and now has extended its scope with some specific CIEM capabilities for privileged identities with Senhasegura Cloud IAM. The platform can run SaaS or on-premises and is engineered on cloud-native code.

The Cloud IAM (essentially its CIEM offering) module is designed to manage, monitor, and log all access across multi-IaaS clouds use by the customer. The module is designed to manage compliance as well access risks. Senhasegura Cloud IAM can expose unused privileges assigned to machine and non-machine identities. The tool is compatible with proprietary IAM tools and credentials generated by CSPs and creates a proxy connection for identities to clouds, thus hiding those IAM tools from end users.

Credentials and service accounts for end users and applications are delivered in JIT for the multiple CSPs that Senhasegura supports (including smaller cloud technologies such as Rackspace and OVH). Senhasegura applies the same protocols and workflows for access to cloud resources within Cloud IAM that it has established for its more traditional PAM capabilities – including the design and capabilities of the common dashboard that can be used to administer Cloud IAM.

Within the dashboard, admins can set IAM security requirements according to CSP best practices guide and create an Identity Entitlement Map – a graphical representation of the relationship between identity, its permissions and service. Its offers Dynamic Privilege Resizing which right-sizes privilege for machine and non-machine identities according to the services they really use. Permissions not used in a set time period will be automatically removed.

The dashboard allows discovery and onboarding of cloud accounts and for entitlements to be set – such as read only access. There are several automation capabilities built into Senhasegura Cloud IAM, but it still lags some competitors in terms of features such as entitlement and permission management and auto-scaling of entitlement policy.

Senhasegura has shown in the past that it is capable of innovating and adding capabilities rapidly according to market changes and customer demands. Its promise to deliver secret-less authentications, better integration with CI/CD tools, and discovery of Kubernetes PODs (crucial for DevOps access and workflows), and container-based secrets should be taken seriously. These will extend its Dev and ephemeral access capability significantly for cloud infrastructures. There will also be JIT access for admins direct to CSP consoles.

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

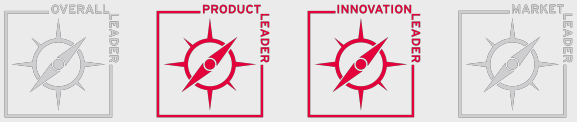
Strengths

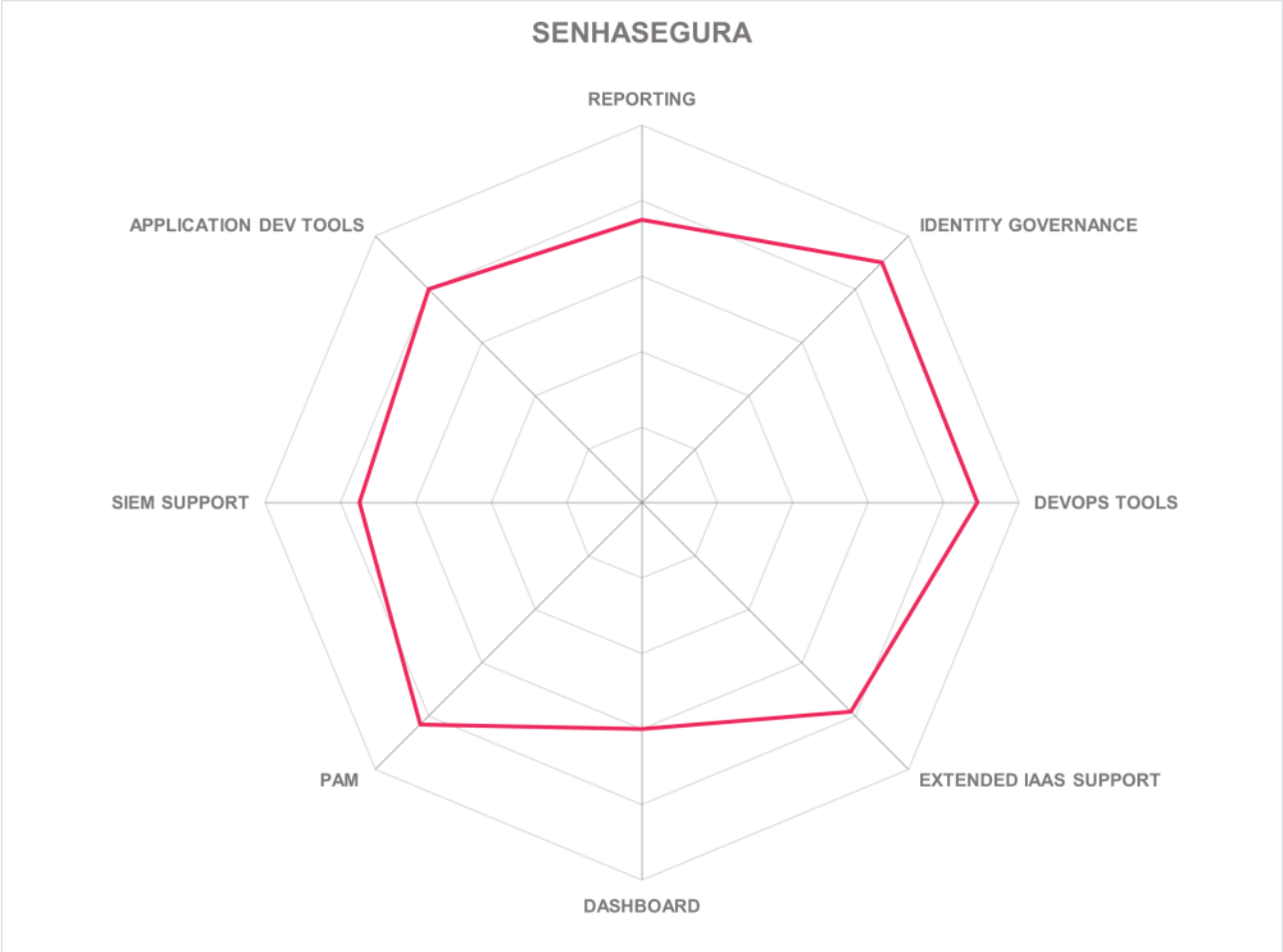
- Strong support for container technologies and all major cloud services with Tier 2 supported
- Good integration with well-known SIEM platforms
- Strong PAM capabilities already built in including PADLM
- Human and machine entitlement discovery with useful automation tools for remediation
- Vendor has taken on board the importance of compliance issues in the cloud

Challenges

- Needs better integration with CI/CD tools
- We would like to see discovery of Kubernetes PODs to improve DevOps capabilities
- Senhasegura is proving itself an innovative and agile vendor, but lack of brand awareness in US and Europe continues to hold it back

Leader in




SENHASEGURA
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.17 SSH Communications Security

Based in Helsinki, Finland, SSH Communications Security (SSH) offers PrivX as its primary product for the PAM market. SSH PrivX provides ephemeral certificate-based Just-In-Time (JIT) access for SSH and RDP protocol authentication, which will find applications for accessing dynamic resources in the cloud.

SSH 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 devices, admin portals to a company's SaaS services, like Salesforce or Twitter, or internal web tools.

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 systems and HSM. There is support for session recording and compliance, and recordings are encrypted. All SSH/RDP/HTTPS/VNC sessions are audited and logged and be used for 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. Other important areas of functionality covered include SAPM, AAPM, PADLM, PUBA, and CPEDM, but traditional endpoint privilege management is missing here. Instead SSH promotes HTML5 thin client approach which reduces the need for endpoint security.

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 can be deployed in container environments orchestrated by Kubernetes, and 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.).

This is a highly scalable, highly compatible credential management system which already serves well for PAM and DevOps cloud users coming in from remote locations. Extending this architecture across all clouds, machine and non-machine entitlements will be a natural and welcome step rounding out the missing CIEM part here. PrivX is cloud-native and supports a wide array of IaaS and microservice architectures. It is more than ready to take the next step to widening full CIEM capability for access management.

SSH.COM

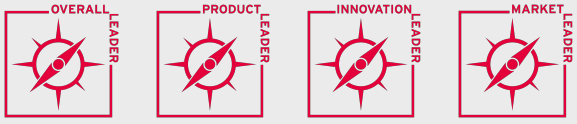
Strengths

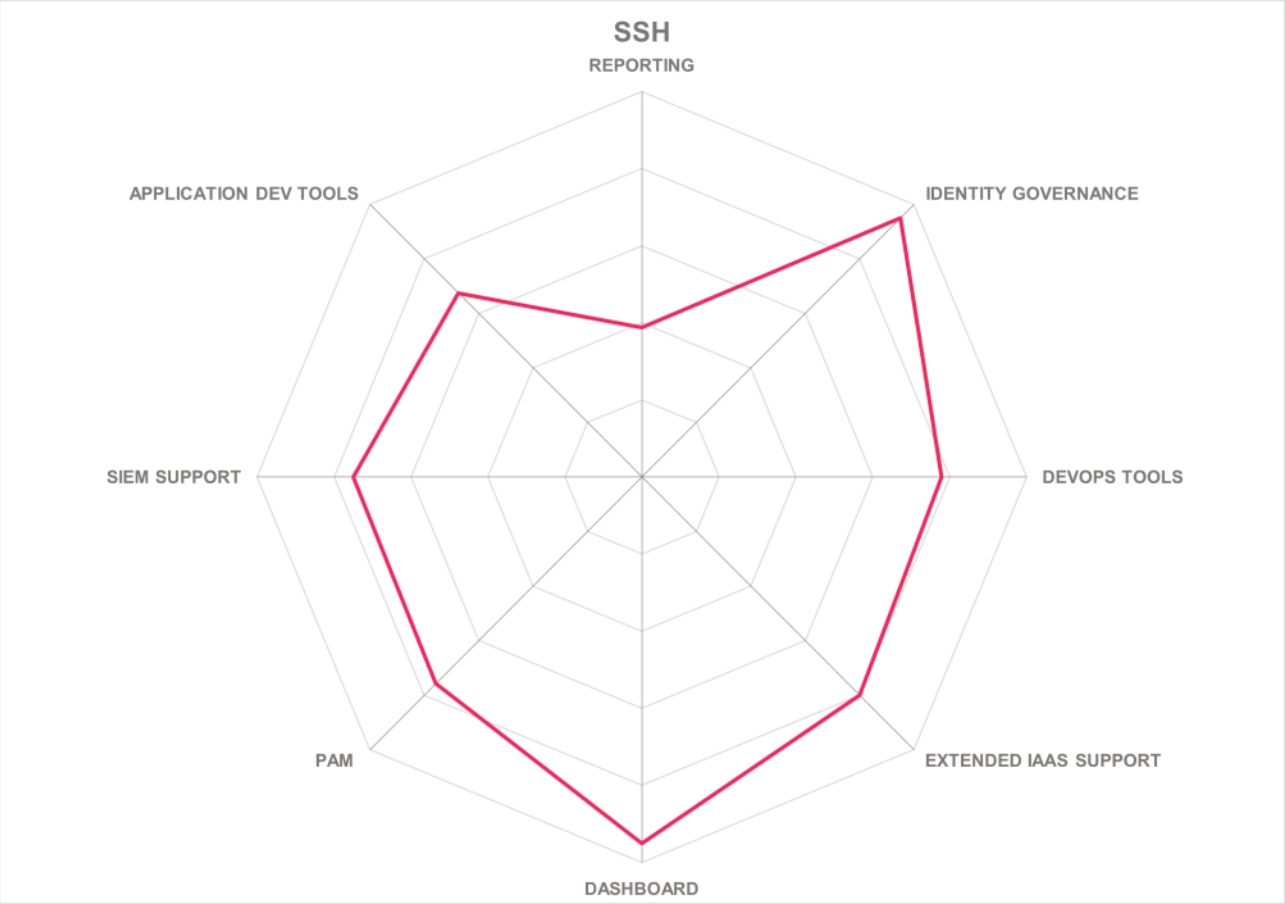
- Full range of IaaS providers supported
- Well featured dashboard that is easy to navigate
- Lean footprint and rapid access make it ideal for DevOps and other agile environments
- Reduces one level of vulnerability by eliminating static passwords and vaults
- Eliminates the risk of redundant credentials being stolen or misused

Challenges

- Needs wider containerization platform beyond Kubernetes compatibility and Docker support as the core code of PrivX is ideal for lean cloud environments
- The promised support for more DevOps tools such as Jenkins should come ASAP
- Absence of traditional endpoint privilege management keeps the solution lean but may be missed by some

Leader in




SSH
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

5.18 strongDM

Founded in 2015, strongDM is an IAM software vendor. Its Infrastructure Access Platform is designed to authenticate and manage access to cloud resources from endpoints and is highly focused on compatibility with the needs of developers.

The platform has two major components: a cloud-based authentication layer and a Credential Gateway that allows access to cloud resources by leasing credentials from supported vault technologies. HashiCorp Vault and proprietary secrets managers from AWS and Google Cloud Platform are currently supported.

strongDM Infrastructure Access Platform supports almost all known CSPs, container tools, Linux clouds, DevOps pipeline tools, and microservices, demonstrating their focus on DevOps and secure remote. All targets are available via the strongDM gateway on a permanent JIT, agentless basis. Authentication is taken care of with SSO support from industry standard IdPs such as Azure Active Directory, Okta, and One Identity One Login. There is no support for or integration with PAM tools. Rather, the company sees this platform as a competitor to traditional PAM platforms.

On the other hand, the developers have provided significant API and SDK support to enable integration with many modern developer-focused apps including Slack, Chef, Ansible, JumpCloud, Terraform, and others. Customers with the necessary resources to connect apps, , can potentially extend strongDM Infrastructure Access Platform quite extensively and create fast, cloud native CIEM applications.

What is missing is significant access and entitlement management tools to support the undoubtedly lean and efficient access protocols within the platform itself. There is no dashboard either - users are expected to offload logging and analytics to third-party solutions including Splunk or the cloud monitoring tools found in AWS, Google, and Azure. The saving grace is the very wide API support that would allow some of the missing parts of DREAM capability to be assembled (Jira, PagerDuty, and DataDog spring to mind here). But not all buyers will want that task and will look for a more integrated OOB solution for DREAM and CIEM requirements.

The strongDM platform does not provide entitlement management or reporting tools because the company does not see itself as competing against CIEM or traditional IGA solutions. Instead, the platform has very extensive API support and a library of integration tools and scripts, enabling DREAM capabilities (Jira, PagerDuty, and DataDog spring to mind here).

The strength of this product lies in its applicability to a wide swath of users (developers, data scientists, marketing, HR, operations, etc.) all of whom need access to resources that contain sensitive data. strongDM fits well into the modern paradigm of security products being purchased by department heads rather than centrally by IT or CISO management. Roadmap items include enhanced support for IdP platforms, native access request workflows directly from the desktop client, improved support for SIEM and UEBA platforms, and a revamped desktop app.

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

strongdm

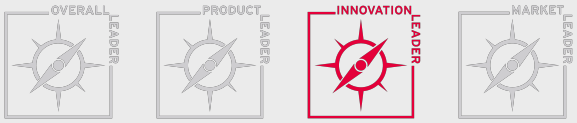
Strengths

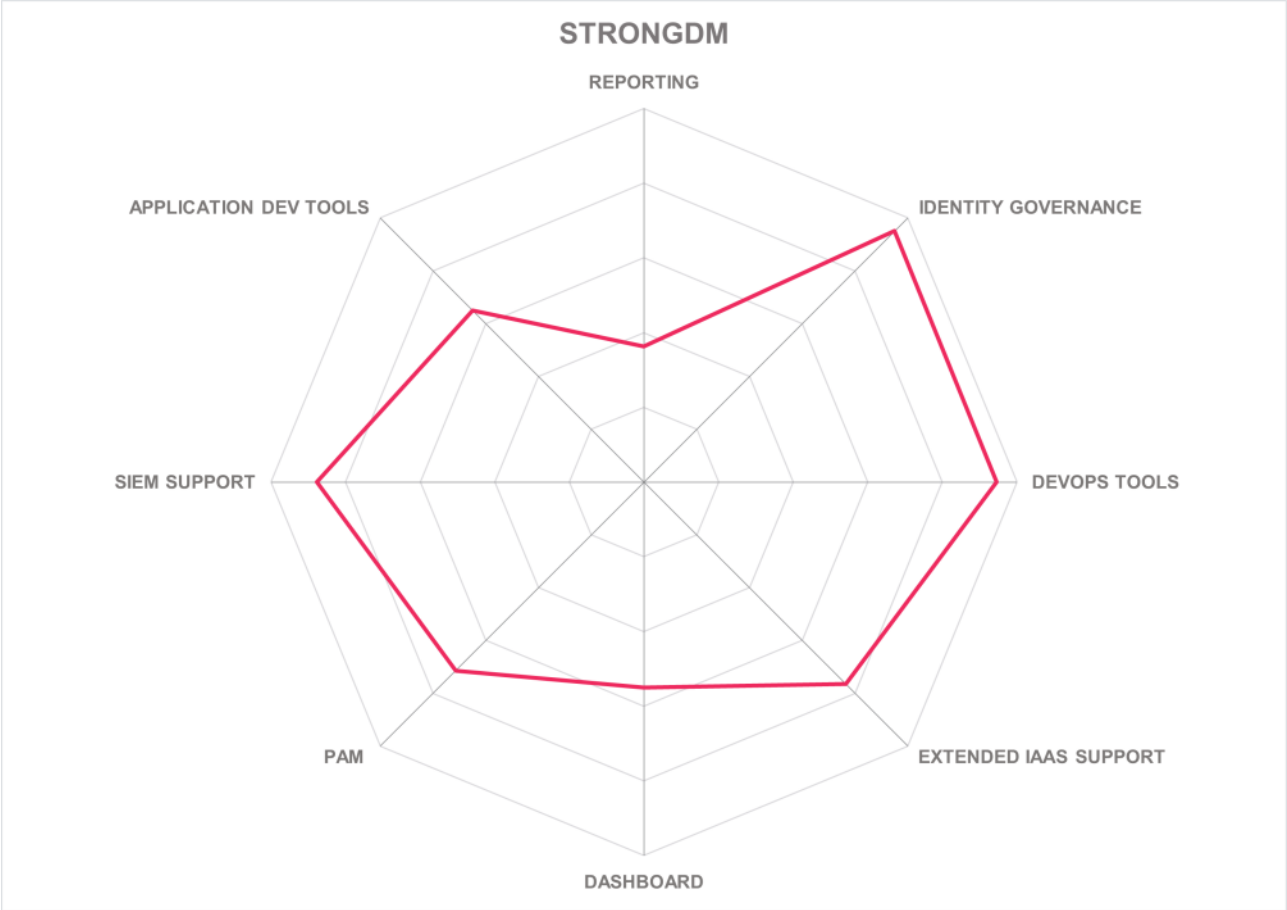
- Extensive support for cloud and IaaS technologies and DevOps tools
- Simple and lean platform makes remote access to cloud tools possible while sandboxing internet-facing endpoints
- Excellent API and SDK support makes integration easy for those with resources to extend capability for CIEM
- Supports third-party IdPs to great effect

Challenges

- No fully featured dashboard so far but this may well come in future releases
- No on-premises version of strongDM but some customers may prefer that
- Look out for deeper integration with IdP players such as Ping in the future

Leader in




STRONGDM
REPORTING
IDENTITY GOVERNANCE
DEVOPS TOOLS
EXTENDED IAAS SUPPORT
DASHBOARD
PAM
SIEM SUPPORT
APPLICATION DEV TOOLS

6 Vendors to Watch

6.1 Aserto

Based in Seattle, Aserto is a start-up that enables SaaS application developers to use native permissions, based on dynamic role modelling and targeted RBAC through its authorization platform, which allows admins to manage users, groups, permissions, and dimensions.

Why worth watching?

As part of the composable trend, Aserto offers a dynamic and highly specific CIEM authorization platform that focuses on a key part of digital management for an increasing number of organizations.

6.2 JetStack

JetStack is an established technology services company that helps enterprises build platform infrastructure using Kubernetes. JetStack Secure focuses on managing machine identities (CA based) to allow components to communicate in multi-cluster container environments, primarily Kubernetes. It is limited in many other functions but is included here because of the excellent way it does manage machine identities and misconfigured certificates across containers. This is an important part of dynamic resource management.

Why worth watching?

Cloud and container environment support is wider than many others in this report The platform is at the forefront of the Shift Left movement and decentralizing identity management to LOBs

6.3 C3M

C3M is a cloud security vendor founded in 2018 and based in San Francisco. C3M Cloud Control contains CIEM, CSPM, and Infrastructure as Code (IaC) security solutions. It supports the three main cloud service providers, AWS, Azure, and GCP. Customers can choose one or more of the modules available from the vendor, depending on requirements.

Why worth watching?

The platform is deployed without agents on SaaS or on-premises – which will appeal to those who feel this is more secure.

6.4 Atos

Atos is one of the largest IT consultancies, and has with the DirX portfolio and the Evidian products as own product offerings. DirX, under the Atos brand, provides a comprehensive set of IAM capabilities targeted at complex, large-scale environments.

Why worth watching?

Atos DirX solutions are proven in their support for complex, large-scale environments and cover both IGA and Access Management capabilities.

6.5 Symantec Secure Access Cloud

Symantec Secure Access Cloud is marketed by Broadcom. It is deployed in IaaS clouds or in on-premises data centres. This zero-trust access service sandboxes applications and security services. When an authenticated user requests remote access to a cloud resource, the Secure Access Cloud creates a secure temporary connection between the user and the requested resource.

Why worth watching?

It uses Zero Trust principles to issue JIT access to specific cloud resources, while keeping the infrastructure, services and network paths hidden from the users.

6.6 Microsoft Entra Permissions Management

Microsoft Entra Permissions Management is a CIEM platform that provides comprehensive visibility and control over all permissions for any identity and any resource across all major clouds, and identity providers including Azure Active Directory, Ping Identity, and Okta.

Microsoft Entra Permissions Management uses bots to crawl networks, scan existing permissions, and highlight which identities have used these permissions, and how they have been used.

A key part of the platform is the Permissions Creep Index (PCI) which assesses the risk level associated with unused or excess permissions and the gap between permissions granted and actively used.

Why worth watching?

Customers that already use Microsoft Defender for Cloud will benefit from automatic access to Microsoft Entra Permissions Management from that platform's dashboard - we expect many more integrations with Microsoft applications over time. Microsoft has already made rapid advances to fashion the original CloudKnox CIEM platform into an improved and recognizably Microsoft product. Further development should be of siginificant interest to those organizations focused on the Microsoft ecosystem.

6.7 Flosum Trust Center

Flosum was founded by an ex-Salesforce enterprise architect. Flosum has developed an application lifecycle management tool native to the Salesforce platform, giving Salesforce developers direct access to the platform to improve fast access automation and orchestration. An advantage is that Flosum leverages Salesforce's UI for all actions.

Why worth watching?

Flosum is a great example of placing DevOps cloud access front and centre of SaaS platforms and improving security by keeping production data secure in Salesforce. The future is here.

6.8 JumpCloud

JumpCloud focuses on the SMB market and for the "post Microsoft Directory Infrastructure" for those customers that have not established an Identity Management solution. The platform provides a single pane of glass dashboard that is compatible with multiple platforms.

Why worth watching?

JumpCloud provides a useful level of identity and cloud management for cloud-native organizations not yet wedded to MS Active Directory.

6.9 SecurEnds Credential Entitlement Management

SecurEnds offers cloud-native Identity Governance software and is based in Atlanta, Georgia. SecurEnds Credential Entitlement Management is designed to monitor user access to cloud resources.

Why worth watching?

Well-featured entitlement management platform that uses ML to discover and mange identity entitlement to ITSM and other SaaS platforms.

6.10 Sonrai Cloud Security Platform

New York based Sonrai bases its platform on tracking identity access across multi-cloud environments, designed to catch identities changing roles or gaining excess privilege. It uses analytics to simulate every attack path an identity could take to access data, regardless of how many degrees of separation, or how short-lived the identity's access is.

Why worth watching?

A fully identify focused CIEM solution that uses a heavyweight analytics engine to reduce risk across multi-cloud environments.

6.11 Solvo IAM Magnifier

Solvo, founded in 2020, is a startup based in Palo Alto. The IAM Magnifier platform uses a wizard-based tool to enable developers and engineers discover users, assets, services, and policies across cloud development infrastructures such as AWS. It also offers complimentary policy and compliance modules to develop least privilege policies.

Why worth watching?

Solvo uses a simple graphical interface to map IAM entitlements and privilege without having to open up logs within existing IAM platforms.

7 Related Research

Leadership Compass Identity as a Service (IDaaS) IGA
Leadership Compass Privileged Access Management
Leadership Compass Identity Governance & Administration
Leadership Compass Access Management
Market Compass IGA Solutions for ServiceNow Infrastructures
Leadership Compass: Access Governance & Intelligence - 71145
Leadership Compass: Access Management and Federation - 71147
Leadership Compass: Adaptive Authentication - 71173
Leadership Compass: CIAM Platforms - 79059
Leadership Compass: Cloud-based MFA Solutions - 70967
Leadership Compass: Dynamic Authorization Management - 70966
Leadership Compass: Identity Provisioning - 71139
Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141
Leadership Brief Prepare and Protect against Software Vulnerabilities
Advisory Note Redefining Access Governance

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 within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market 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

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities 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 they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain 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 vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, 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 the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). 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. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, 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 either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. 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 a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

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

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. 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. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate 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.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

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

Content of Figures

Copyright

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

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

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