

Secrets Management

Graham Williamson

April 24, 2023



**LEADERSHIP
COMPASS
2023**

Secrets Management is a broad subject that covers any protected data or information that must not be divulged to others. In this document the term 'secret' refers to a software token, a key pair or a certificate that must be managed and, if divulged, only released to an authorized party.

The focus of the document is on 'management' because, with the proliferation of secrets, particularly in the cloud native environment, it is impossible to effectively manage these without the appropriate tools to create, administer and remove tokens, keys and certificates as required to manage access to protected resources.

Contents

Contents.....	3
Figures	4
Introduction / Executive Summary	5
Highlights.....	6
Market Segment	6
Definitions.....	9
Delivery Models	10
Required Capabilities.....	11
Leadership	12
Overall Leadership.....	13
Product Leadership.....	14
Innovation Leadership.....	15
Market Leadership	18
Correlated View.....	20
The Market/Product Matrix.....	21
The Product/Innovation Matrix	22
The Innovation/Market Matrix.....	23
Products and Vendors at a Glance	25
Product/Vendor evaluation	28
AppViewX – CERT+	29
CyberArk - Conjur	32
Entrust – Key Control.....	35
HashiCorp - Vault	38
Intercede – MyID	41
Keeper Security	44
Keyfactor - Command.....	47
Nexus – Smart ID	50
Oracle – Key Vault.....	52
Smallstep.....	55
Versasec – vSEC:CMS.....	58
Vendors to Watch.....	61

Methodology..... 63

 Types of Leadership 63

 Product rating 65

 Vendor rating 66

 Rating scale for products and vendors..... 67

 Inclusion and exclusion of vendors 68

Figures

Figure 1 - Secrets Management Solutions..... 9

Figure 2: Overall Leaders in Secrets Management 13

Figure 3: Product Leaders in Secrets Management 14

Figure 4: Innovation Leadership in Secrets Management 16

Figure 5: Market Leaders in Secrets Management 19

Figure 6: The Market/Product Matrix for Secrets Management 21

Figure 7: Product/Innovation Matrix for Secrets Management 23

Figure 8: Secrets Management Market/Innovation 24

Introduction / Executive Summary

The term 'secrets' has recently been seconded into the IT lexicon. It is being used as a collective noun for passwords, keys, certificates, and tokens that must not be disclosed i.e., they must be 'kept secret'.

Account take-overs remain the most common mechanism for unauthorized intrusion to protected systems, resulting in cybersecurity compromise. This vulnerability is increased by issues such as poor password management, service account credentials hardcoded in config files, and database passwords kept in shared folders. The problem is exacerbated for cloud development environments where account credentials are held in S3 buckets, Azure DevOps, CI/CD tools and various source-code repositories. In multi-cloud environments the beleaguered CIO has no option but to employ 'secrets management' technology to help mitigate the risk of account compromise.

Secrets Management is a wide field. In this Leadership Compass the term refers to credentials that are used by people, systems or devices seeking access to a protected resource such as an application, database, software module or device; the authentication credential may be a password, a token, or a key.

Passwords are a perennial problem and are slowly being replaced by other authentication mechanisms, but while they are still widely used, a mechanism is needed to securely manage them. While passwords are secrets that must be managed their usage is diminishing so this document focuses on token and key management solutions.

Software tokens can be a passphrase stored on a system that is substituted for a password when a complex password, one that a human cannot remember, is required. One-time-passwords are also tokens. These are machine-generated and used in conjunction with an authentication server to validate a possession factor such as an OTP device or smartphone. API tokens are increasingly used to transmit user data to an application. Examples are authentication tokens such as an HTTP file containing a header, payload with identity attributes and trailer, or JSON Web Tokens that can also pass identity data in a JSON array to a relying application for authorization purposes.

Keys include basic API keys used to identify code components, TLS keys for session protection, signing keys used to validate source identities and encryption keys used to protect documents and files. PKI private keys that are used for signing and/or encryption, must be protected. While PKI certificates are not 'secrets' a mechanism is required to ensure validity and currency of a certificate.

Secrets management requires a secure storage facility with the capability for approved persons to manage access rights to the stored secrets. The solution will release secrets as required, and as appropriate, for access to applications and supported platforms. It should also provide secrets management functions such as identifying expiring secrets and removal of secrets no longer required.

While legacy operations will continue to use passwords for some time, new deployments should embrace access control solutions that leverage the benefits of secrets management. Vendors featured in this document cover secret storage vaults, credential lifecycle managers and key management tools, as well as DevOps tools for cloud deployment.

Highlights

Organizations seeking to protect their sensitive resources such as a computer application or corporate documentation should analyze their current requirements and understand the industry direction before committing to a specific solution.

- Passwords provide a simple authentication mechanism that is well understood by users and represent a low-friction option for access control.
- Increasingly stronger authentication mechanisms such as multi-factor authentication are being adopted to improve cybersecurity.
- A software ‘token’, typically stored on an end-point system or a removable device, can provide more complex or longer passwords or passphrases for increased protection. If used in conjunction with a PIN or biometric it can enable multi-factor authentication. Recent developments in this sector include private access tokens for secure access to web services.
- Certificates, typically used in asynchronous key models, provide security for a wide range of applications from account access to sensitive document protection.
- Secrets management supports popular access control mechanisms including the OpenID Connect (OIDC) federation and the Fast Identity Online (FIDO) Alliance.
- The release of the FIDO2 specifications significantly improve the ease with which password-less authentication can be realized.

Market Segment

There are multiple facets to the Secrets Management market sector. From a technological viewpoint it encompasses passwords, software tokens and key management. But in order to determine potential solutions we also consider four use cases: Person IDs, Machine IDs, software supply chains and IoT device management.

Technical Analysis

The ‘secrets’ covered in this document are used for access control to protected resources. This access can be requested by individuals or machine processes. Secrets management covers three broad areas:

Password Management

Password management combines an encrypted vault, to safely store passwords, and a password lifecycle management capability; typically provided in Privileged Access Management (PAM) solutions.

While there are many vault solutions in use today, from password protected Excel files to sophisticated, token-protected password repositories; only solutions that provide password lifecycle management are included in this Leadership Compass. Lifecycle management means that there must be a mechanism to securely generate a password/passphrase and keep it secure. There must be a mechanism to implement the organization's password policy. This might stipulate minimum and maximum password length, password complexity, or password rotation requirements to thwart account takeover attacks. There must be a mechanism to suspend an account, making the password/passphrase inaccessible, and a process to remove a password when an account is no longer required. Some organizations augment their password management with a Privileged Account Management (PAM) system. These systems protect sensitive accounts such as administration accounts by hiding the passphrases to protected accounts and managing logins for privileged users. PAM systems will also automate password rotation and in some cases, provide session monitoring and event logging features. Pure PAM solutions are covered in document 81111 PAM Leadership Compass 2022. Only vendors offering additional functionality such as token and/or key management are included in this document.

Token management

Token management is a diverse subsector including secrets such as authentication tokens passing identity attributes to an authentication service in an HTTP header, JSON Web Tokens to pass data between systems, OAuth Access Token to grant access to a requested resource. In this document 'token' refers to software. In some cases, the term is used to refer to a hardware device e.g. the term 'FIDO token' for multi-factor authentication is sometimes used to refer to a USB storage device that holds a FIDO2 key pair.

A variety of delivery models are used to suit specific use cases. An authentication service will generate an access token to a resource when a user has successfully completed an authentication process. Tokens are often used in DevOps environments where different levels of access control are used depending on the developer's access rights to the Dev, Test and Prod environments. If users are accessing SaaS applications, they will typically be issued a personal token that may include additional data for authorization purposes. If the user is an administrator of their company's tenancy in a SaaS environment, their access token will give them access to the appropriate administrative functions.

Storage of tokens varies depending upon the use case. Authentication tokens are typically resident on a user's end-point client system or on a hardware storage device that plugs into a user's computer, typically a USB port, and interacts with an authentication service to log the person in using a stored token. The user might also need to operate a button on the storage device for a 'proof-of-presence' step, or a fingerprint/facial recognition check for a positive identity validation might be required. One of the drawbacks of a hardware storage delivery model is the necessity to manage the issuance of the devices themselves. Increasingly organizations are choosing to use smartphones for token storage, with the token passed via Wi-Fi or Bluetooth to the authentication service. While this simplifies the device registration process it raises BYOD issues that might deem a personal smartphone inappropriate for corporate purposes.

Another type of token is the Private Access Tokens (PAT), used to simplify user access to websites. They are increasingly being used to supplant CAPTCHA processes that are often considered too 'high friction'.

Key/Certificate management

The use of key-pairs is typically considered the most secure secrets management mechanism. There are several deployment models:

- Synchronous key mechanisms that are typically used for communication encryption with both ends using a 'shared' key,
- Asynchronous key systems use a public-private key pair that is generated securely with the private key protected i.e., not shared.
- Public-private keys with a certificate to verify the key generation provenance, this can be self-signed or signed by a trusted third-party certificate authority,

Key-pair generation can be performed locally, on devices such as a USB device or on highly secure Public Key Infrastructure (PKI), typically managed via a certificate authority, that generates a certificate that validates the provenance of the key pairs and establishes a validity period. PKI combines encryption and digital signing to support multiple use cases from basic application authentication to secure email and document storage.

Secure Shell (SSH) uses a public key (validated via a certificate) to encrypt messages and verify the sender. It is widely used in the UNIX environment to secure communications and support SSH commands. It is typically used to provide SSO across multiple systems.

FIDO2 uses PKI for authentication purposes, with the user's private key maintained on their end point device such as a PC, USB authenticator or smartphone. Authentication can either use the WebAuthn method for web application access or the CTAP2 protocol.

The most widespread protocol for PKI is the X.509 certificate-based protocol used for encrypting and digitally signing communications. Mainstream operating system suppliers provide PKI support through their CA processes. Deployments of X.509 PKI can be tailored to the assurance level required, from self-signed certificates to highly secure certificate authorities (CAs) and secure key management. Public key infrastructure uses a key pair; communication encryption uses the recipient's public key to encrypt, and the user's private key is used to decrypt. Digital signing uses the sender's private key to attach a hash to the file and the recipient uses the sender's public key to verify the signature.

Secure Production Identity Framework for Everyone (SPIFFE) uses a PKI model to generate keys, SVIDS (X.509), and assigns them uniquely and specifically as identifiers for a software workload for distributed systems. The environment consists of a SPIRE server for registering workload Ids and an API to a relying Node on which there is SPIRE agent supporting the software deployment via a workload API.

In selecting a Secrets Management solution, the required level of security is generally considered the most important element. While an OTP solution provides MFA, dramatically improving authentication security, FIDO2 will further improve both the assurance level and reduce user friction, but an enterprise PKI environment, with trusted root certificates, will

provide high-level authentication assurance depending upon the authenticator device selection and the user-registration process.

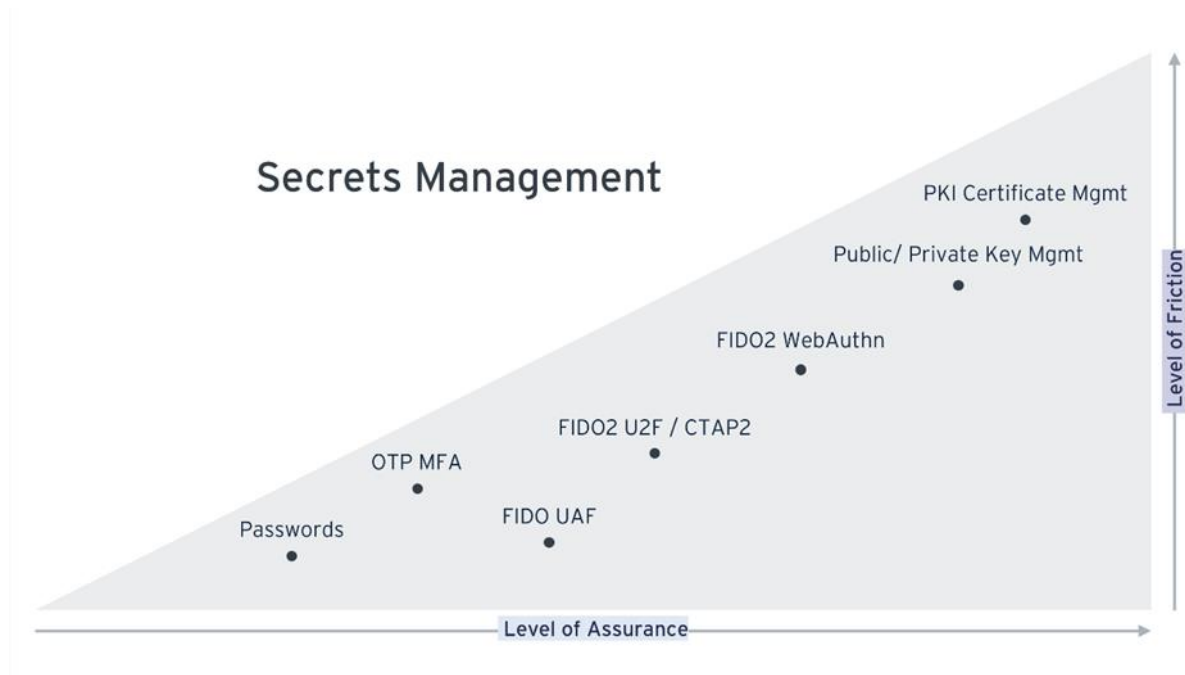


Figure 1 - Secrets Management Solutions

One-time-passwords provide multi-factor authentication because users need a device to read or enter a PIN to login. OTP is typically used to provide a second factor for a username/password authentication. FIDO Universal Authentication Framework (UAF) was devised to login without passwords via a mobile phone. FIDO Universal 2nd Factor (U2F) provides a framework for wide acceptance of two-factor usage, FIDO2 adds protocols for authentication and web-application secure login using PKI. Key management systems significantly enhance the ability of PKI environments to suit enterprise use cases. Managing certificates, and ensuring key pairs are generated in secure infrastructure, provides the highest level of security, and enables a high level of authentication assurance.

Definitions

The Secrets Management sector has sown confusion by giving words different meanings. A token now refers to not just the token but the device on which it is stored. Attestation, well understood in the IAM industry, is now being used by FIDO to reference device provenance. Passkey is being used to refer to FIDO2 key pairs as well as the technology to store them across multiple devices.

For clarity, the following definitions are used in this Leadership Compass:

- Authenticator – device used to store key pairs used to authenticate users to a protected resource. It could be a PC, USB device, smartphone, smartcard etc.
- Certificate – a human-readable document issued by a CA that attests to the provenance of a user’s keys; it is usually signed by the CA for document integrity.

- Credential – attributes granted to a user or device for the purpose of accessing a protected resource e.g., passwords, tokens or keys; it can also refer to a certificate.
- Key – a machine-readable character string typically used by a relying application or protected resource to determine the access rights of the requesting user or device.
- Key pair – related keys used for access control, encryption, or digital signing; they may be synchronous (a single key) or asynchronous (public/private key-pair).
- Passkey – a FIDO protocol that allows key-pairs to be shared across devices e.g., USB, smartphone, PC etc. Enables login from an alternate device if required.
- Secret – a credential that identifies an individual, a user group, or a device; it must be protected to avoid unauthorized use.
- Storage device – a hardware device used to store user credentials e.g., smartcard, USB device, smartphone etc.
- Token – a software file containing user information typically passed to an application via an API. It does not refer to a storage device or an OTP hardware device.

Delivery Models

Deployment models run the gamut from on-premises software appliances to microservices deployments managed via a CI/CD pipeline automation tool. Increasingly a Software-as-a-Service model is finding favor as customers become more comfortable with the security capabilities of cloud infrastructure.

The selected deployment model will vary depending upon the use case to be supported. The following are typical secrets management use cases:

Person IDs

There is a myriad of instances where protection of person identifiers, and associated secrets, is required. This is typically associated with authentication to protected resources which may also include authorization to specific functionality. Both software tokens e.g., HTTP authorization token and key-pair technology e.g., FIDO2 or CA-generated key-pairs have a part to play in protecting Person IDs.

The increasing support for FIDO2 and the decreasing costs of USB storage devices means there is potential to move to an environment with a lower overall cost with the adoption of WebAuthn for web apps and CTAP for domain login.

Machine IDs

Increasingly automation of software access, be it via APIs or purpose-built connectors, requires cybersecurity protection. Encryption of communication to protect data in transit and digital signing of messages to validate the source of the communication are common methods of raising cybersecurity levels.

Machine IDs are used to secure software workloads that are typically deployed in cloud infrastructure. Docker images and Kubernetes containers require protection for confidentiality and integrity of code deployments. Integrated Deployment Environments (IDEs) must provide

secrets management for keys, tokens and passwords used by DevOps staff, and protect against exposed secrets.

Next Gen DevOps

DevOps staff have both Person ID and Machine ID requirements. Often the Integrated Development Environment (IDE) is not managed via a company's IAM system because it can be quite complex and fluid. Managing who has access to Dev, Test, Pre-prod and Prod environments requires diligent staff and a solution that can accommodate time-limited escalation of privileges and associated governance. The problem is exacerbated in multi-cloud environments requiring tight access controls on multiple Admin accounts.

A bigger issue is the management of software module deployments. In a cloud native environment, it is no longer realistic to expect DevOps staff to know where modules are deployed, so developers cannot be expected to know the machine ID and associated keys for a software workload, particularly in a micro-services scenario. DevOps staff need appropriate tools that provide libraries of routines and CI/CD pipeline automation. These tools need to be configured to use the appropriate signing, and in some cases encryption, keys so that code deployments meet the integrity and security levels required by each application.

IoT Authentication

Most IoT environments facilitate cybersecurity protection using a variety of methods. Edge computing typically provides network-level protection by restricting access to devices or controllers.

But IoT devices are often deployed in unrestricted, sometimes remote, locations and must transmit data back to a supervisory system, and supervisory systems communicate to devices, either in a real-time control capacity or in a periodic firmware update. These communications must be signed and, in some cases, encrypted. The keys necessary to achieve this must be protected and managed.

Required Capabilities

There is not a single list of required capabilities. Companies must understand their current secrets usage and the shortcomings of their current processes, they must evaluate their corporate capacity to manage a secrets management environment and ensure a strategy is in place to guide the development of their security technology. Items to consider include:

<p>Mature PKI environments.</p>	<p>In many cases a company's PKI environment grows as demands increase; in the absence of a holistic analysis of corporate requirements. While vendor systems provide good point-solutions they are often inadequately managed, with expiring user certificates and unmanaged root certificates. Encryption algorithms may be out-of-date, and personnel may be unaware of how the CAs and HSMs should be managed.</p>
---------------------------------	--

	Deploying contemporary tools can rectify these shortcoming and future-proof the corporate cybersecurity environment.
Multi-cloud environments.	With the increasing adoption of cloud deployments many corporations are finding that their secrets management task transcends on-premises applications and likely covers multiple cloud service providers, in this situation the use of a software appliance, or a 'PKI-as-a-service' that can accommodate AWS Secrets Management, Azure Key Vault and Managed HSM, Google Cloud KMS, and other private cloud services, is a requirement.
Microservices support.	For companies deploying in a microservices environment the use of a secrets management solution is essential. The sheer volume of key management events, often with short-lived validity timeframes, and the need to facilitate distributed encryption/decryption tasks, mandates the use of tools that minimize manual intervention.
DevOps support.	Companies undertaking significant software development have an acute secrets management requirement. Containerized software workloads are deployed to multiple cloud services availability zones that typically require digital signing, and in some cases encryption. It is not realistic to expect DevOps staff to manage the requisite keys so a tool to automate the CI/CD pipeline is required.
IoT requirements.	The days of un-encrypted communications from device to controller are mostly gone. IoT devices now assume secure communications, often with keys built into their firmware. To the degree possible these keys should be incorporated into the corporate key or certificate management systems and the IoT environment should be included in the corporate secrets management guidelines.

Vendors featured in this Leadership Compass can accommodate one or more of these requirements. Prospective suppliers should be selected based on their coverage of the client's specific use case requirements.

Leadership

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

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

- Product Leadership

- Innovation Leadership
- Market Leadership

Overall Leadership

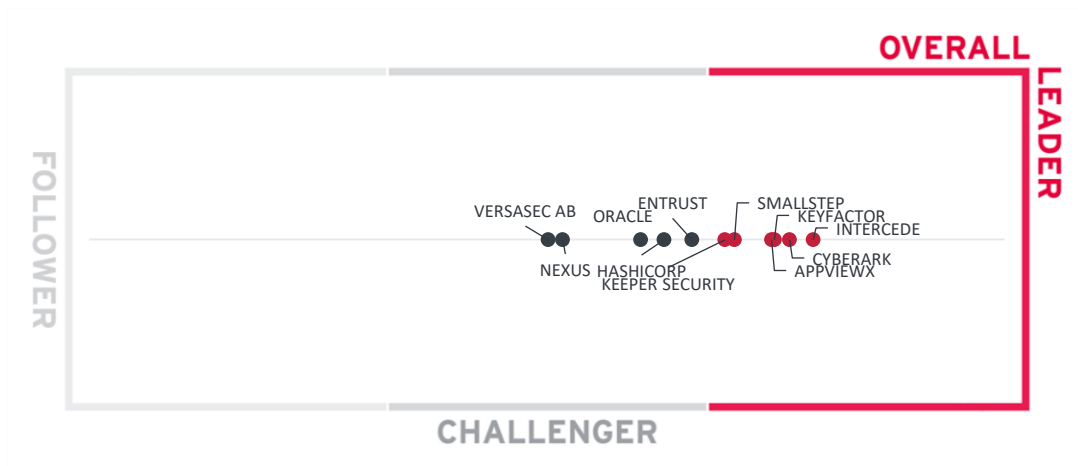


Figure 2: Overall Leaders in Secrets Management

It is difficult to determine Overall Leadership in a market segment that is so diverse. AppViewX offer an innovative machine ID solution, CyberArk is a leader in terms of their market size and their innovative Conjur solution. Intercede offers a leading credential management solution. Keeper Security offer a unified cybersecurity platform, Keyfactor and Smallstep provide particularly innovative offerings in key management and machineID tools.

Overall Leaders are (in alphabetical order):

- AppViewX
- CyberArk
- Intercede
- Keeper Security
- Keyfactor
- Smallstep

In the Challenger group we have HashiCorp’s widely used vault solution, Entrust’s vault management product and Oracle’s Key Vault solution. Nexus and Versasec provide leadership in credential management.

Product Leadership

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

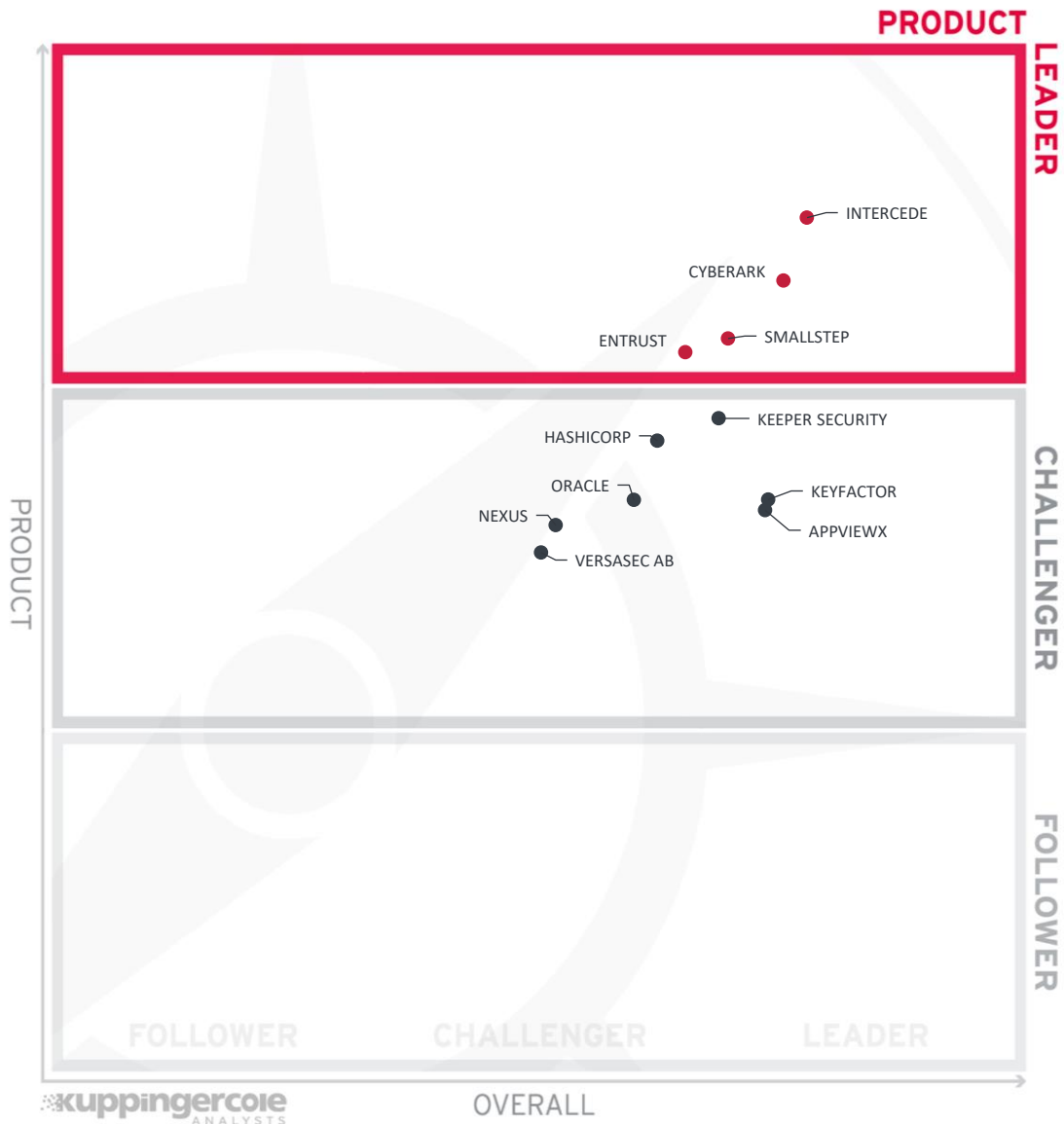


Figure 3: Product Leaders in Secrets Management

Product Leadership is where we examine the functional strength and completeness of vendor solutions. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are shown in the center rectangle. No vendors are in the Followers section due to the emerging nature of the secrets management sector.

In the Product Leadership rating, we look for functional strength in the vendors' solutions, regardless of their market size.

Four vendors are singled out for Product Leadership in their specific product sector. (In alphabetical order) they are:

- CyberArk
- Entrust
- Intercede
- Smallstep

CyberArk's Conjur offering provides an important extension to the company's leading PAM product, enabling a comprehensive solution to protect 'secrets. Entrust's solution provides visibility and management across multiple vaults. Intercede's leadership is in the completeness of their credential management solution. Smallstep's solution leverages the capability of their product partners to suit multiple use cases.

In the Challenger section Keeper Security and AppviewX focus on DevOps staff support, HashiCorp offer strong vault management, Keyfactor offers strong key management capabilities, and both Nexus and Versasec provide strong credential lifecycle management.

Innovation Leadership

Next, we examine **Innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments.

In the case of secrets management innovation is incredibly important because the sector is young and developing. The industry sector is moving quickly to provide effective solutions for emerging needs that, in many cases, are not well-understood. Innovation is not about delivering a constant flow of new releases, rather, innovative companies take a customer-focused approach, delivering features that assist companies to maintain an improving security posture despite rapid technological advances.

In the following chart the vertical axis shows the degree to which each vendor had developed an innovative solution, plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership chart is divided into three rectangles: Innovation Leaders occupy the top section, Challengers are shown in the center rectangle and Followers would be in the lower section, although no vendors are shown in this section due to the level of innovation required in the secrets management sector,

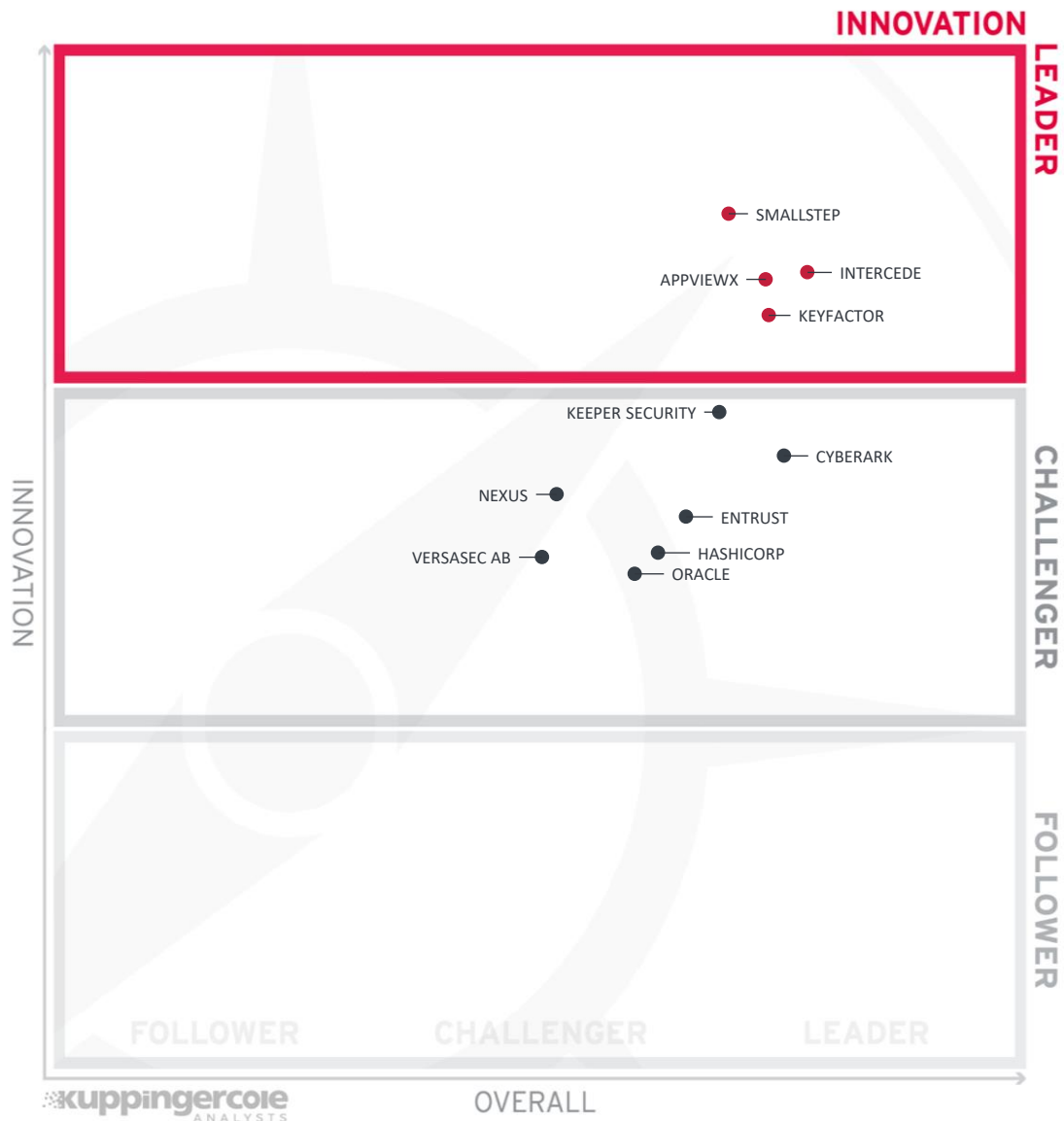


Figure 4: Innovation Leadership in Secrets Management

Innovation Leaders (in alphabetical order):

- AppviewX
- Intercede
- Keyfactor
- Smallstep

AppviewX is recognized for its support for service partners and DevOps platforms. Intercede provides wide integration with corporate identity services. Keyfactor brings an innovative digital-trust approach to identity credentialling. Similarly, Smallstep adopts a zero-trust platform management solution approach.

The balance of vendors assessed are in the Challenger area because, due to the emerging nature of the sector, vendors must be innovative and constantly developing features to assist their clients by providing solutions to emerging problems. Keeper Security offers innovation across both person and machine identity areas, CyberArk's Conjur solution provides strong integration and governance capabilities for machine IDs. Entrust's innovation provides cross vault support with overarching management capabilities, Hashicorp's innovation is in the wide application of their vault solution to customer needs, Oracle have innovated in the tools provided to extend their Key Vault product beyond traditional database and systems support. Both Nexus and Versasec have innovated in providing lifecycle credential management for specific use cases.

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.

The vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

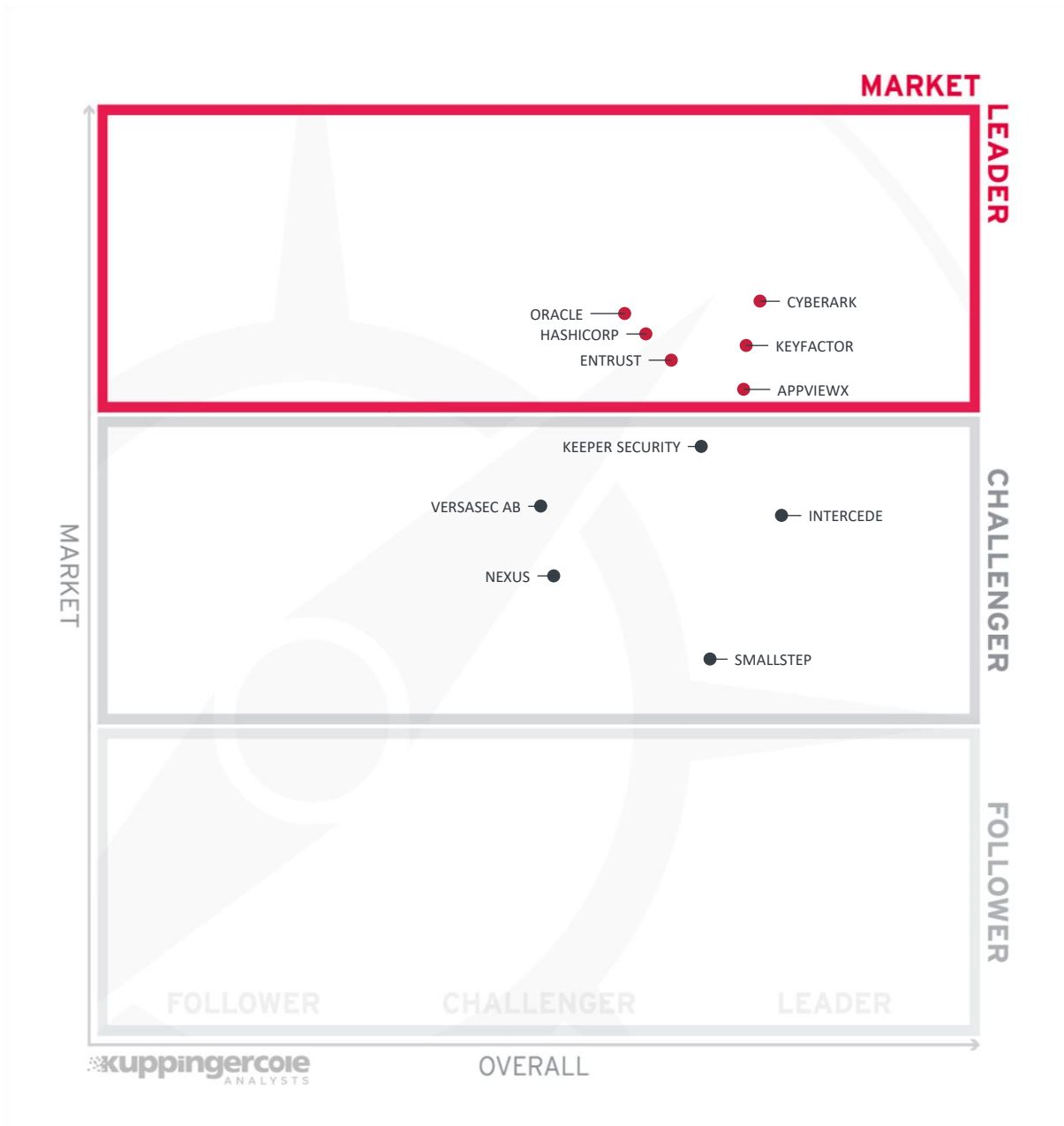


Figure 5: Market Leaders in Secrets Management

Market Leaders (in alphabetical order):

- AppviewX
- CyberArk
- Entrust
- HashiCorp
- Keyfactor
- Oracle

The Market Leadership area is somewhat skewed due to the infancy of the Secrets Management market sector. The companies located in the Leader rectangle are large

companies with significant marketing capabilities, a significant customer base and well-developed partner networks.

In the Challenger group all have good marketing approaches but are considerably smaller than the Leaders. Keeper Security have a comprehensive go-to-market program combining partner and in-house support staff, Keyfactor has a particularly broad solution catering for a breadth of customer requirements. The three credential management solution suppliers, Intercede, Versasec and Nexus, have all developed marketing approaches to suit their target markets. Smallstep is a recent entrant into the secrets management sector and will move up the market axis as their market reach develops.

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.

The Market/Product Matrix

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

The vertical axis represents the market position plotted against product strength rating on the horizontal axis.



Figure 6: The Market/Product Matrix for Secrets Management

Vendors below the line have a weaker market position than might be expected according to their product maturity. Vendors above the line are somewhat 'overperformers' when comparing Market Leadership and Product Leadership.

This chart illustrates the developing nature of the Secrets Management sector. It comes as no surprise that the larger companies are at the top of the chart and Smallstep is at the bottom. Similarly, based on the functionality provided by the solutions in their respective segments, CyberArk Conjur, Entrust, Intercede and Smallstep and are in the righthand squares of the chart, due to their relative corporate strengths.

The Product/Innovation Matrix

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



Figure 7: Product/Innovation Matrix for Secrets Management

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

Intercede, Smallstep, Keyfactor and AppviewX are recognized for the innovative nature of their solutions with Intercede and Smallstep further recognized for the completeness of their respective solutions in their placement in the top right hand square. Most vendors are in the center square demonstrating a satisfactory level of innovation and functionality in their product areas. CyberArk Conjur and Entrust are recognized for their product leadership.

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. Vendors which are highly innovative must focus on improving their market position. Mature organizations with a good market presence need to focus on innovation, especially in an emerging sector such as Secrets Management.



Figure 8: Secrets Management Market/Innovation

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 while having a lower market share, and therefore the biggest potential for improving their market position.

AppviewX, Keyfactor, Intercede and Smallstep are all recognized for their innovation within their respective approaches to secrets management. CyberArk, Entrust, Hashicorp and Oracle occupy the top middle square due to their marketing presence but slightly lower innovation rating. The top left square is vacant because it's not possible to be in secrets management without a significant level of innovation.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Secrets Management. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
APPVIEWX	positive	positive	strong positive	neutral	positive
CYBERARK	strong positive	positive	strong positive	positive	strong positive
ENTRUST	positive	strong positive	positive	positive	positive
HASHICORP	strong positive	positive	positive	neutral	strong positive
INTERCEDE	strong positive	strong positive	neutral	strong positive	strong positive
KEEPER SECURITY	strong positive	strong positive	neutral	positive	positive
KEYFACTOR	positive	positive	positive	neutral	neutral
NEXUS	positive	positive	neutral	neutral	positive
ORACLE	strong positive	neutral	positive	neutral	strong positive
SMALLSTEP	strong positive	strong positive	positive	positive	positive
VERSASEC AB	positive	strong positive	neutral	neutral	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
APPVIEWX	strong positive	positive	positive	positive
CYBERARK	positive	positive	strong positive	strong positive
ENTRUST	neutral	strong positive	strong positive	neutral
HASHICORP	neutral	strong positive	positive	positive
INTERCEDE	strong positive	positive	neutral	neutral
KEEPER SECURITY.	positive	strong positive	neutral	positive
KEYFACTOR	strong positive	strong positive	strong positive	positive
NEXUS	positive	positive	neutral	neutral
ORACLE	neutral	neutral	strong positive	strong positive
SMALLSTE	strong positive	neutral	neutral	neutral
VERSASEC AB	neutral	positive	neutral	positive

Table 2: Comparative overview of the ratings for vendors

It is recognized that in placing the vendors in a single table, as above, comparison between vendors is encouraged. However, the featured vendors differ greatly in the focus of their solutions. To assist in better understanding the functionality of each vendor’s offering the following matrix is provided.

	Person IDs	Key mgmt	Vault storage	Credential mgmt	DevOps tools	Machine IDs
APPVIEWX	○	◐	◑	◑	●	●
CYBERARK	◑	●	◑	◑	●	●
ENTRUST	◑	◐	●	◑	◑	◑
HASHICORP	◑	◐	●	◑	◑	◑
INTERCEDE	●	●	○	●	○	○
KEEPER SECURITY.	●	◐	◐	◐	●	◐
KEYFACTOR	○	●	◐	◐	◑	●
NEXUS	●	●	○	●	○	◑
ORACLE	◑	◑	●	◑	◑	◑
SMALLSTEP	◑	●	◑	◐	●	◐
VERSASEC AB	●	●	○	●	○	○

Table 3 Functionality comparison

● Fully supported, ◐ Mostly supported, ◑ Some features supported, ◑ Few features supported, ○ Not supported

Product/Vendor evaluation

This section contains a quick rating for every product/service we have 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 secrets management market sector. We look at the following eight categories:

- Person IDs – the degree to which the vendor’s solution fulfills the requirements for managing credentials for human authentication.
- Tokens – the ability of the vendor to accommodate the management of software tokens for authentication, encryption, API signing etc.
- Keys/Certificates – the solution’s ability to facilitate the lifecycle management of key-pairs and associated certificates.
- Credential Management – the ability of the vendor’s solution to enroll users/devices, issue keys/tokens and remove them on expiry/loss.
- Authenticators – the solution’s support for creation of secure key-pairs and issuance of an authenticator such as a smartcard, USB storage device or smartphone.
- Integration tools – the ability of the solution to integrate with corporate tools such as identity stores and databases.
- Management & Governance – the support provided by the solution for corporate tools such as SOC, SIEM and reporting tools.
- Machine IDs – the ability of the solution to manage digital signing/encryption of software workloads and DevOps supply chain requirements, it may also secure IoT device communication.

AppViewX – CERT+

Headquartered in New York, USA, with additional offices in the U.S., U.K., Australia, and India. AppViewX commenced operations in 2014 and now have more than six hundred staff worldwide and over 300 active customers, with in excess of 500M keys and certificates under management. The company provides certificate and key lifecycle management, and automation. AppViewX focuses on moving organizations from legacy operations, mostly on point solutions and manual operations, to a modern environment providing a comprehensive solution with central management, policy enforcement and fine-grained access control.

AppViewX's core product is CERT+, providing full certificate lifecycle management for X.509 certificate-based environments, from any private or public CA, SSH access control, Kubernetes certificate management and cloud CLM (AWS, GCP, Azure). CERT+ supports digital signing of software workloads and digital encryption; the product also supports IoT device identity management. AppViewX also offers a private trust PKI-as-a-Service, PKI+, that seamlessly integrates with CERT+ to replace expensive and inefficient on-premise internal PKIs.

AppViewX provides a discovery service for certificates and keys which performs a network scan that catalogs them, identifies their characteristics (algorithms, key sizes), and determines their validity period. This provides visibility into the enterprise certificate infrastructure which is the first step in managing it. Certificates can then be monitored, and automatically renewed before expiration, avoiding unnecessary costs, application outages and security weaknesses.

Self-service is provided via automated enrollment, issuance, and renewal of certificates. Approval workflows are supported with role based access control (RBAC). A central control plane, with an intuitive UI provides visibility across all certificate processes. APIs, supporting the enrollment protocol, facilitate DevOps and device integration. A graphical depiction of the certificate creation process facilitates analysis and provides click-to-view visibility into APIs used in the process. A graphical depiction of the hardware description language for the crypto-mesh is provided showing the relationships between the various pods and key issuance services. Cert-Orchestrator supports Kubernetes, development tools such as Ansible, Terraform, Jenkins and OpenShift, and platforms such as Envoy. It can integrate with public or private CAs and supports the ACME framework, as well as SCEP, EST, Windows auto-enrollment, and others.

AppViewX also provides governance over certificate infrastructure with the ability to define fine-grained role-based access control and the ability to group certificates on business use-cases for auditing and compliance purposes. Audit trails for user key/certificate usage can be created to document activity and prevent unauthorized actions. The processes enforced by AppViewX provide the ability to properly govern key/certificate issuance and eliminate non-compliant use of certificates. The UI provides useful services: it can show a certificate's chain of trust back to the root CA, or it can display a graphic of the enrolment process to assist in key management. Policy creation and enforcement capabilities enable PKI and security teams to establish enterprise-wide PKI governance for internal policy compliance as well as security standards and industry regulatory mandates.

The product is available as a SaaS service or it can be deployed on corporate infrastructure.


Security	positive	
Functionality	positive	
Deployment	strong positive	
Interoperability	neutral	
Usability	positive	

Table 4: AppViewX's rating

Strengths

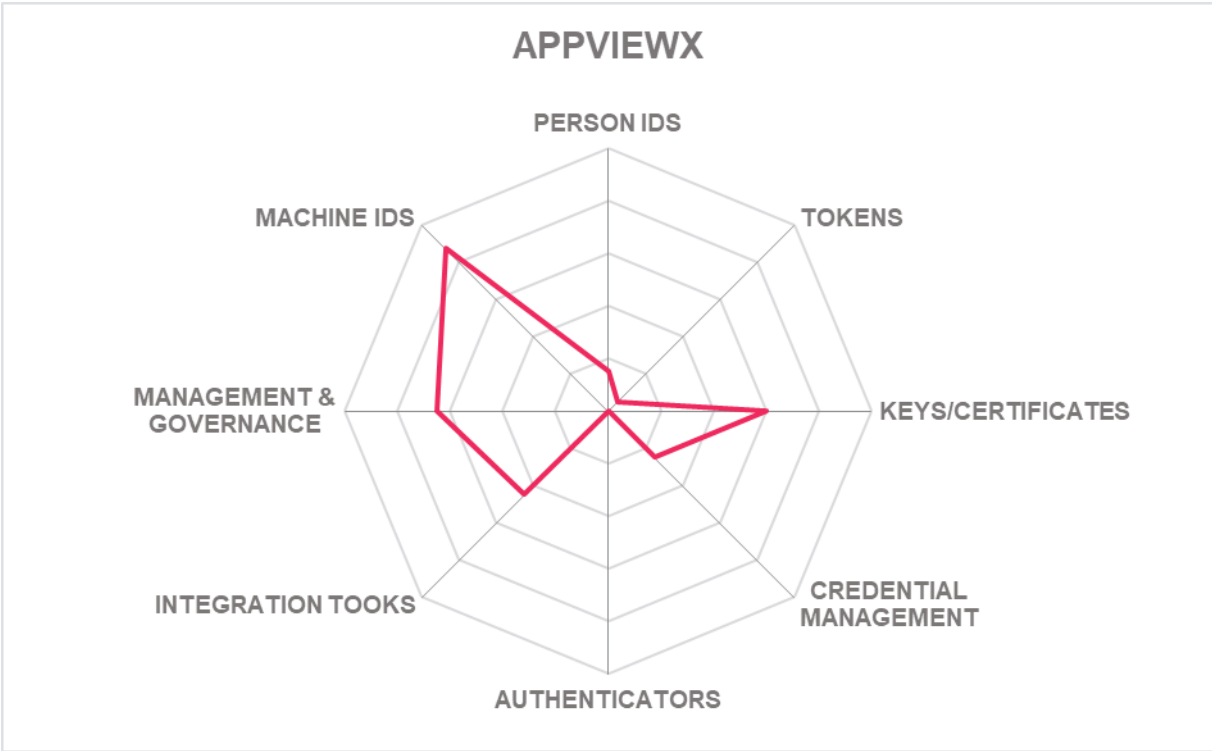
- Comprehensive key management
- Discovery service for in-use certificates
- Support for DevOps tools and processes
- Innovative depiction for the certificate management process
- Governance audit and reporting

Challenges

- Credential manager support for life-cycle management of key-pairs
- Support for 3rd party CAs
- Support for IoT devices

Leader in





CyberArk - Conjur

CyberArk is best known for its leadership in the Password Administration Manager (PAM) sector, but over the last few years it has made some significant product enhancements to extend its capabilities and influence in the password-less environment. One of the markets being targeted is machine identities and CyberArk's solution is aptly named Conjur, it is targeted at DevOps staff.

The CyberArk Secrets Manager supports developers, security staff and operations personnel managing application secrets across the enterprise. This includes cloud native apps and developers CI/CD pipelines supporting Kubernetes across AWS and Google Cloud, and supporting DevOps tools such as Jenkins, Terraform, Ansible and GitHub. For security staff Tenable, Rapid7, Fourscout, Aqua and Qualys are supported. For IT operations staff integration with ServiceNow, AppDynamics, BMC, WebLogic, WebSphere and Apache Tomcat are provided. Fetching a secret from Conjur is an API call for these applications and services. Conjur also supports device identities via gateways to various OT environments such as Siemens, Honeywell, GE and others.

CyberArk is pursuing a 'best practice' blueprint for securing application secrets. Kubernetes is a major direction for CyberArk and Conjur, as support for multi-cloud development environments is increasing.

Two new offerings are focused on support for cloud native applications and CI/CD pipeline automation.

- Conjur Cloud – is a SaaS service, integrated with DevOps tools. It's available as Conjur Enterprise, a self-hosted software appliance deployed on corporate infrastructure.
- Secrets Hub – is a SaaS managed service integrating project teams in AWS secrets Manager.

Futures include self-hosted support with Secrets Hub, public APIs for automation, support for Azure and the release of a 'discovery' service to provide visibility across the secrets management plane. Conjur product futures include 'Conjur Edge', a local instance that maintains services in the event of a network interruption, a new Management UI simplifying the user experience, and a 'dynamic secrets' service providing just-in-time elevation of privileges. Conjur also supports IoT devices via key management to gateway systems.

Licensing varies depending on the product. CyberArk Conjur Open Source is provided license free, Conjur Enterprise is charged by region based on the number of containerized environments. Conjur Cloud is charged by the number of workload IDs.

Security	strong positive	
Functionality	positive	
Deployment	strong positive	
Interoperability	positive	
Usability	strong positive	

Table 5: CyberArk's rating

Strengths

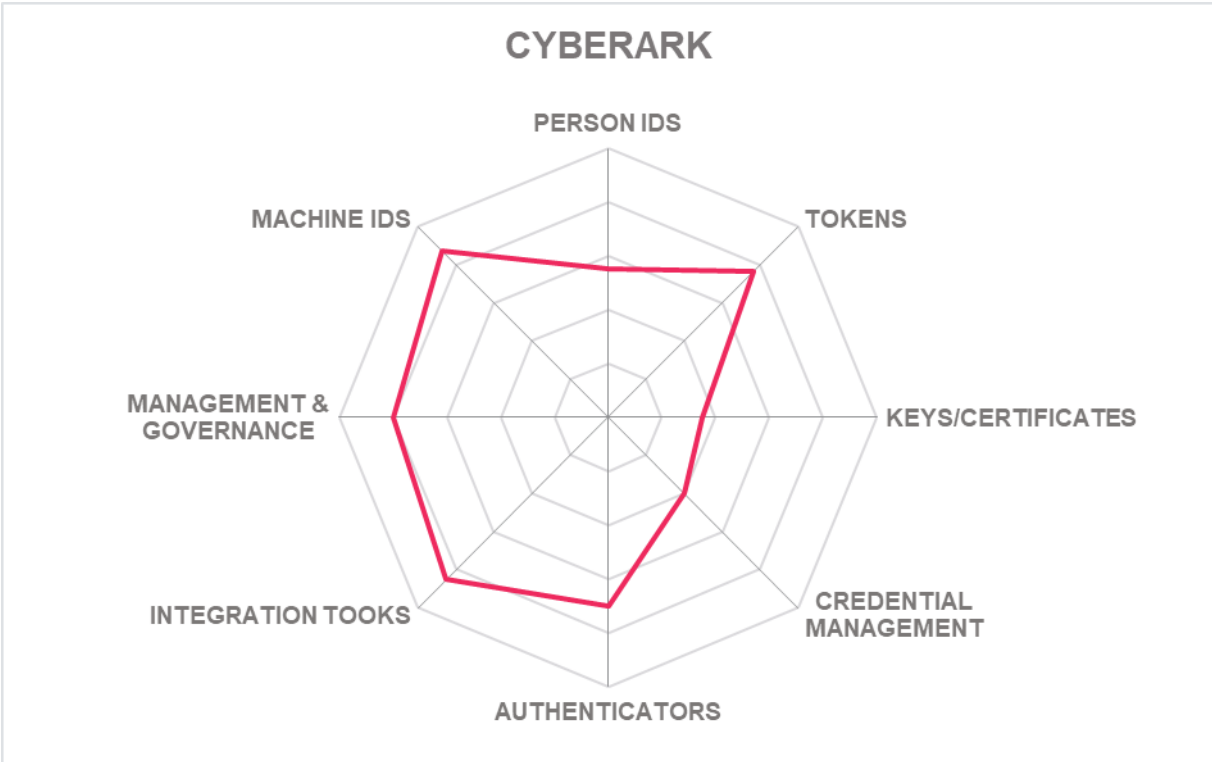
- Platform Integration automates secrets management for the developer environment
- Secrets are always held in Conjur, not the local dev environment.
- APIs to enterprise identity services for approval management and governance
- Good multi-cloud and microservices support
- Flexible licensing offering

Challenges

- Transitioning into a 'full service' secrets management solution provider
- Providing support for the increasing number of cloud-native platforms
- Integrating Conjur into a unified CyberArk credential management solution

Leader in





Entrust – Key Control

Entrust is an enabler for trusted identities, payments and digital infrastructure. Its wide breadth of solutions is critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption and more. Entrust is based in Minneapolis, USA, and operates in over 150 countries worldwide.

Supported technologies include Identity/Auth, PKI, IoT/Machine Identity, Certificate Lifecycle Management, Key Management and Encryption, and Hardware Security Modules. It also offers public trust certificates like SSL/TLS and Verified Mark Certificates.

A recent addition to Entrust’s product suite is Key Control providing managed and unified vault environments, with the ability to unify vaults in different business units, different geographies, different technologies, and to provide centralized management via the Key Control facility.

Entrust was an early adopter of SaaS solutions and offers Identity-as-a-Service, PKI-as-a-Service, Digital Signing-as-a-Service, Instant ID-as-a-Service, and Identity Verification-as-a-Service.

Key Control 10 provides the ability to centralize the management of diverse security vaults including tokenization vaults and database encryption key vaults. Popular vault environments include the AWS KMS, Google Cloud KMS, Azure BYOK, SSH (via proxy management for key protection), and the OASIS KMIP protocol,

Policies for each vault can be monitored centrally with a notification generated if a specific security requirement, e.g. encryption standards policy has not been met.

The solution is deployed as an appliance using an OVA file, providing quick deployment; equivalent formats for AWS, Azure and GCP are supported. The management UI allows the administrator of each vault (which will typically have at least two nodes for redundancy purposes) to manage their local environment while KeyControl provides enterprise governance oversight.

Key Control Compliance Manager provides visibility across all vaults and cloud key stores providing a detailed view of stored keys and software tokens. It supports management reporting on compliance and trending data and can report back to vault owners and app owners on key usage and history. KeyControl Compliance Manager enables policy management via monitoring of algorithm usage, key length and validity periods and related compliance reporting.

The Compliance Manager is deployed as a virtual appliance, typically on customer infrastructure.

Security	positive
Functionality	strong positive
Deployment	positive
Interoperability	positive
Usability	positive



Table 6: Entrust's rating

Strengths

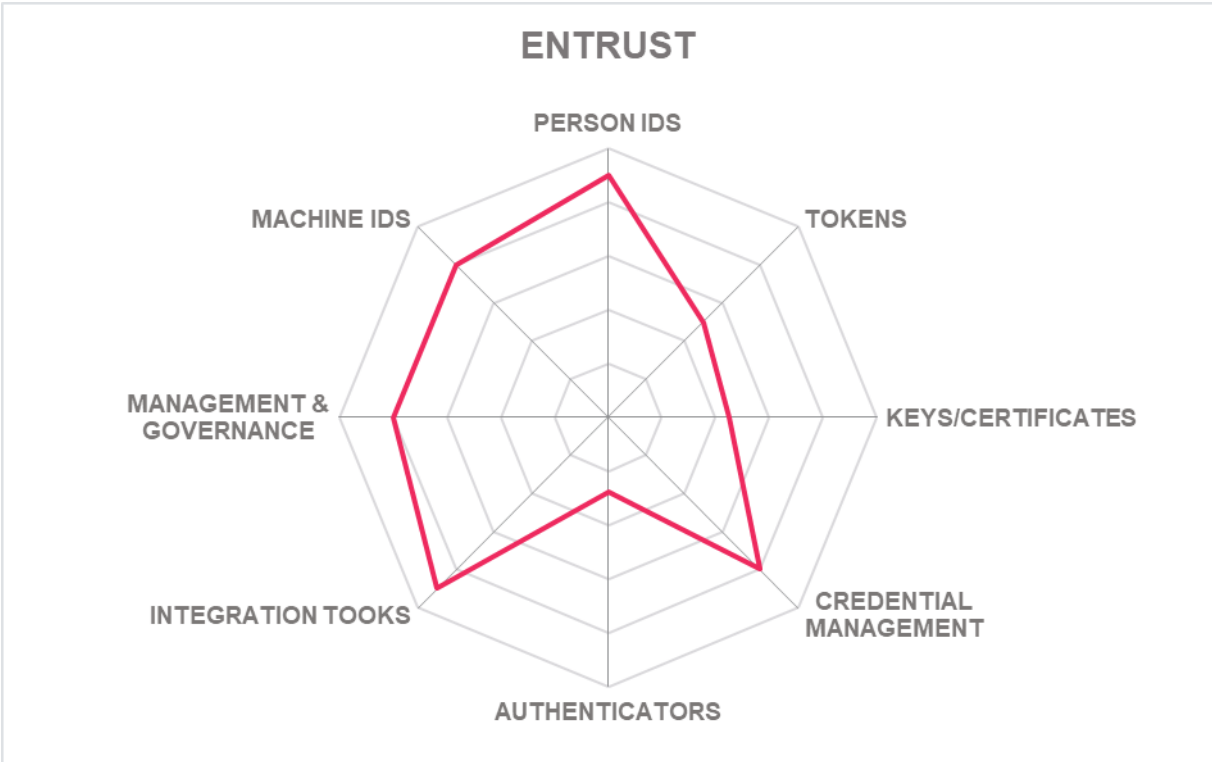
- Centralized management of diverse vault environments
- Ability of local vaults to manage their own policies
- Visibility of key characteristic across corporate vaults
- Strong SaaS delivery model
- Good governance oversight

Challenges

- Integration with Entrust's Person ID solutions
- Lifecycle credential management
- Integration with corporate resources such as IdPs

Leader in





HashiCorp - Vault

HashiCorp is headquartered in San Francisco, USA. Their vision is to enable companies to secure their entire infrastructure by identifying everything and everyone, issuing certificates for key management, encrypting data and communications so that strong corporate security policies can be maintained. Central to achieving this vision is certificate management as a secure, more flexible, and scalable way to identify software workload, devices and individuals and secure network connections.

HashiCorp's focus, as a provider of cybersecurity tools, is on protecting enterprises as they migrate from a high-trust IP-based network environments to a dynamic environment characterized by low-trust services. It is designed to be secure by default, supporting a fully managed environment, enabling automation of simple and repeatable deployments.

The core component is Vault, an open-source secure storage service that can be deployed as an on-premises solution, typically self-managed with enterprise support. Or it can be accessed as a managed cloud-based service from an AWS availability zone.

Vault is, in effect, a credential broker that unifies multiple IdPs (AD, LDAP, Radius, Duo, OKTA etc.) and provides a management plane to control authentication to protected services. Vault becomes an abstraction layer to supported services.

The secrets engine can be programmed to provide just-in-time credentials that can be established for a controlled lease duration. For instance, if a contractor is substituting for a sick staff member, they can be given access for an 8 hour period after which the access token is automatically revoked. Database credentials are supported and automated key rotation is provided. Kubernetes secrets are also supported.

The certificate manager provides visibility and auditability across assets and the ability to implement approval workloads. Lifecycle management of certificates is provided from issuance to expiry. Certificates about to expire are identified with alerts issued to responsible persons. Revocation (CRL & OCSP) is supported. It is delivered as a hosted SaaS offering or it can be deployed on-premises.

HashiCorp's Vault is very versatile; the 'Swiss army knife' of credential management. It enables access control policy to be implemented, managing access to all sensitive resources.

Boundary is HashiCorp's Cloud Platform tool that provides access to applications and critical systems with fine-grained authorizations. It enables remote access workflows to be automated for human-to-machine access with granular authorization for trusted identities.

HashiCorp's Consul supports multi-cloud service networking. with service discovery and service mesh capabilities. It enables platform operators to deploy a secure, fully managed, service mesh, enabling developers to discover and securely connect any application on any runtime service such as Kubernetes, Nomad or Amazon ECS.

ACME Device Attestation is supported for TPM-enabled devices and smartcards.

Licensing is versatile with ‘Enterprise Service’ pricing based on the number of supported clients,

Futures include a focus on ‘day-two ops’ streamlining the maintenance and optimization of certificate management. This will make it easier to identify components that need certificates, providing greater visibility on violations of certificate management best practice, and enabling companies to migrate from legacy PKI deployments to secure cloud-native environments.

Security	strong positive
Functionality	positive
Deployment	positive
Interoperability	neutral
Usability	strong positive



Table 7: HashiCorp's rating

Strengths

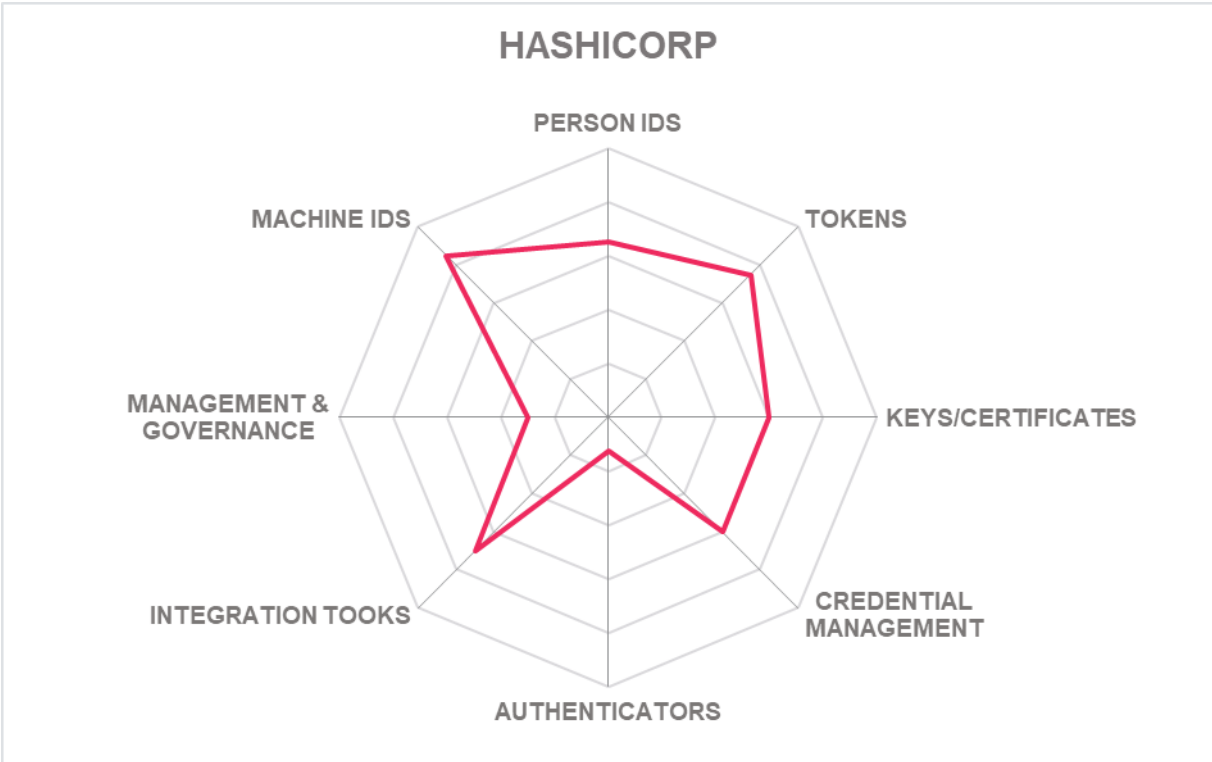
- Mature supplier of Vault technology
- Simple certificate management interface
- Support for ACME Device Attestation
- Strong support for multi-cloud solutions
- Comprehensive DevOps tool support

Challenges

- Support across emerging DevOps tools for cloud-native platforms
- Integration of identity management solutions to manage person IDs
- Support for device identifiers in OT environments

Leader in





Intercede – MyID

Intercede, with over 20 years' experience in providing cybersecurity solutions, is based in Leicester, UK and maintains a significant presence in the US.

The core product is MyID® which is a software platform providing the ability to securely manage the issuance, suspension and revocation of PKI and FIDO credentials that are deployed to user devices for authentication to protected enterprise resources. The solution provides lifecycle management from the generation of key pairs and related certificates for public key infrastructure, to the expiry or revocation of credentials. Intercede supports a robust registration process, including the ability to validate documents for identity verification. The solution can provide certificate authority functionality or integration to 3rd party CAs. Key pairs can be issued to smartcards, USB devices, or end-point devices via virtual smartcard functionality. Encryption protocols include SHA256, AES 2048 and 4096, and can support ECC and 3DES. Both X.509 and FIDO2 key management is provided.

MyID® credential management associates a credential with a person. Lifecycle management can be managed by administrative personnel or via self-service facilities from client devices such as PCs or smartphones, or shared devices such as kiosks. A competitive advantage is the policy management provided by the solution, ensuring corporate guidelines such as authenticator regulation requirements or minimum key-lengths are followed. Central administration of credentials is also managed via policies that are established to guide the issuance process for specific credential types e.g.: does it require a face-to-face meeting, is there an approval workflow, are there device constraints regarding hardware or software capabilities, is a PIN or TouchId required, or is a specific FIPS firmware standard required. MyID® supports multiple keys on a device, allowing users to use one device for access to multiple systems. User transparency as to which key is being used is dependent upon the system requirements allowing the same PIN or TouchId to be used across systems.

Support for robust cybersecurity processes including an audit regimen that provides audit log management for all Admin and system events signed by the HSM device and user keys, ensuring non-repudiation of user events. Clients typically define 'allowed lists' of whitelisted applications, with a signing ceremony initiating admission to the PKI environment.

Integration with corporate repositories allows roles to be imported, or they can be established within MyID®, for approval workflow and policy management purposes. MyID® supports frameworks such as ADFS, OIDC etc. Rest APIs are provided for integration with other services.

MyID® integrates with Windows Hello and can add credentials to the Windows Hello for Business container.

Intercede has recently acquired Authlogics for password and OTP type authentication solutions. Authlogics have sophisticated password threat analysis capabilities, with large repositories of compromised passwords garnered from the dark web.

Security	strong positive
Functionality	strong positive
Deployment	neutral
Interoperability	strong positive
Usability	strong positive



Table 8: Intercede's rating

Strengths

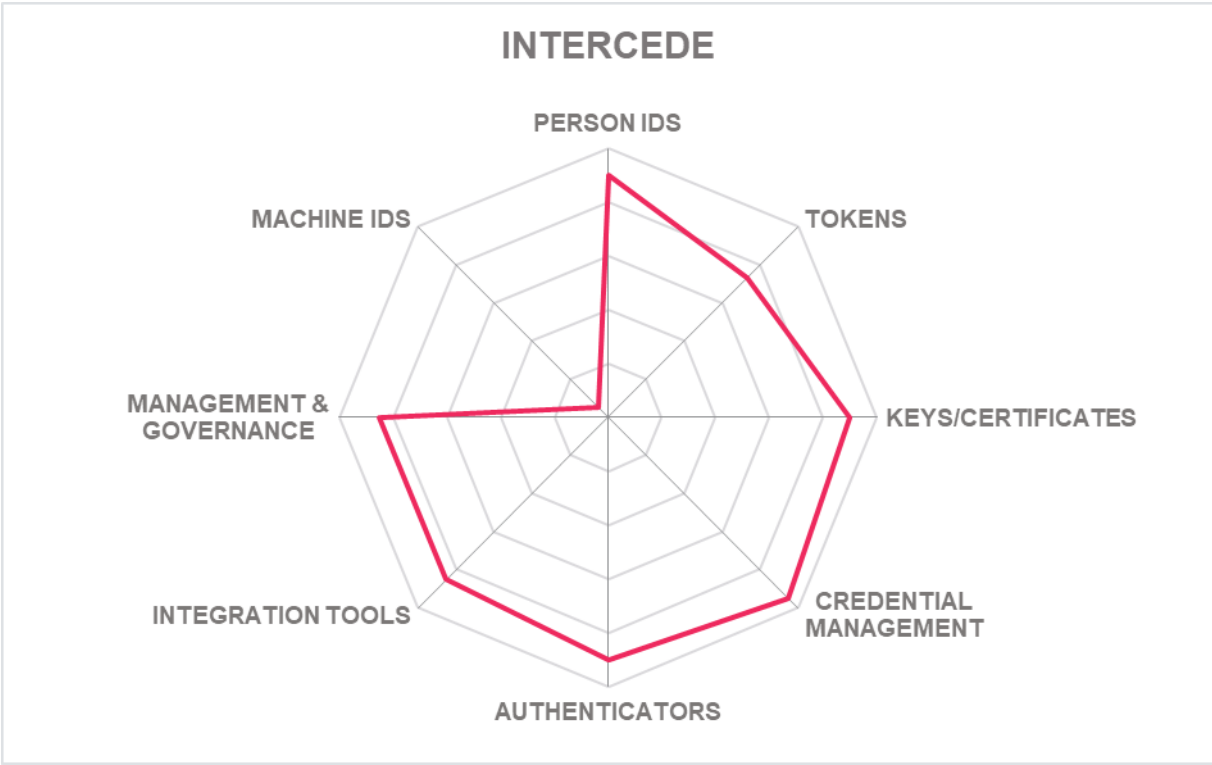
- Sophisticated credential lifecycle management capabilities
- Integration with corporate identity management services
- Policy management control over authenticator issuance
- Provision of high assurance IDP and authentication services
- Support for FIDO2 key pair management and attestation

Challenges

- Support for machine IDs
- Support for cloud-native DevOps environments

Leader in





Keeper Security

Keeper Security, headquartered in Chicago, USA, was founded in 2011 to provide expertise in enterprise identity security and access management encompassing password management, secrets management and privileged access management.

Keeper Security has observed the rapid dissolution of previously well-defined perimeters to an organization's security leading to a situation in which there is now no border to corporate networks, making management of access to protected resources more difficult. With enterprise infrastructure spread across multiple networks, multi-cloud deployments, a myriad of cloud apps and credentials spread over an increasingly complex and largely unmanaged environment, a method to protect secrets is now essential.

Furthermore, the proliferation of IoT devices, coupled with exponential growth in the adoption of cloud computing, including cloud native approaches, is now the root cause of rapidly expanding cybersecurity vulnerability.

Keeper Security maintains that a ubiquitous unified cybersecurity platform is required to avoid an increasing number of data breaches as cloud adoption accelerates and the network perimeter vaporizes. Device proliferation means that zero trust & zero knowledge security are now a requirement. Keeper Security's Breach Watch provides dark web monitoring that constantly scans employees' Keeper Vaults for passwords that have been exposed.

Keeper MSP provides password management as a Service. It is a multi-tenant password manager with privileged account management solution, enforcing policies and governance controls. Reporting and auditing capabilities are also provided. Functionality includes password management and sharing, password-less authentication, single sign-on security, privileged session management, remote infrastructure access, zero trust security, credential governance and controls, SSH key management, secure remote database access, secrets management for DevOps and industry compliance and reporting,

Keeper Security promotes a Zero Trust – Zero Knowledge framework. Data is encrypted and decrypted at the device level so that the server never receives data in plain text and no keeper employee can view unencrypted data. Decryption and Encryption of vault secrets takes place locally on the user's device using Elliptic Curve (EC) keys when deploying with SSO, or key derivation when logging in with a Master Password. Multilayer encryption provides access control at the user, group, and admin level. Sharing data uses PKI-based secure communication.

Keeper Security has a comprehensive go-to-market strategy. At the bottom is the B2C offering, for small business and the SOHO offering for home offices, The SMB solution satisfies the small-to-mid sized business which are also served by the Managed Service offering for mid-market sector companies. These sectors are serviced by a sophisticated network of partner organizations as is the enterprise market segment. At the top of the go-to-market stack is the Public Sector State/Local & higher education sector, and the Federal Gov (civilian & cabinet-level) sector, serviced by Keeper resources directly.

Keeper Security maintains AWS availability zones in the US, Canada, Europe, Japan and Australia.

Security	strong positive
Functionality	strong positive
Deployment	neutral
Interoperability	positive
Usability	positive



Table 9: Keeper Security's rating

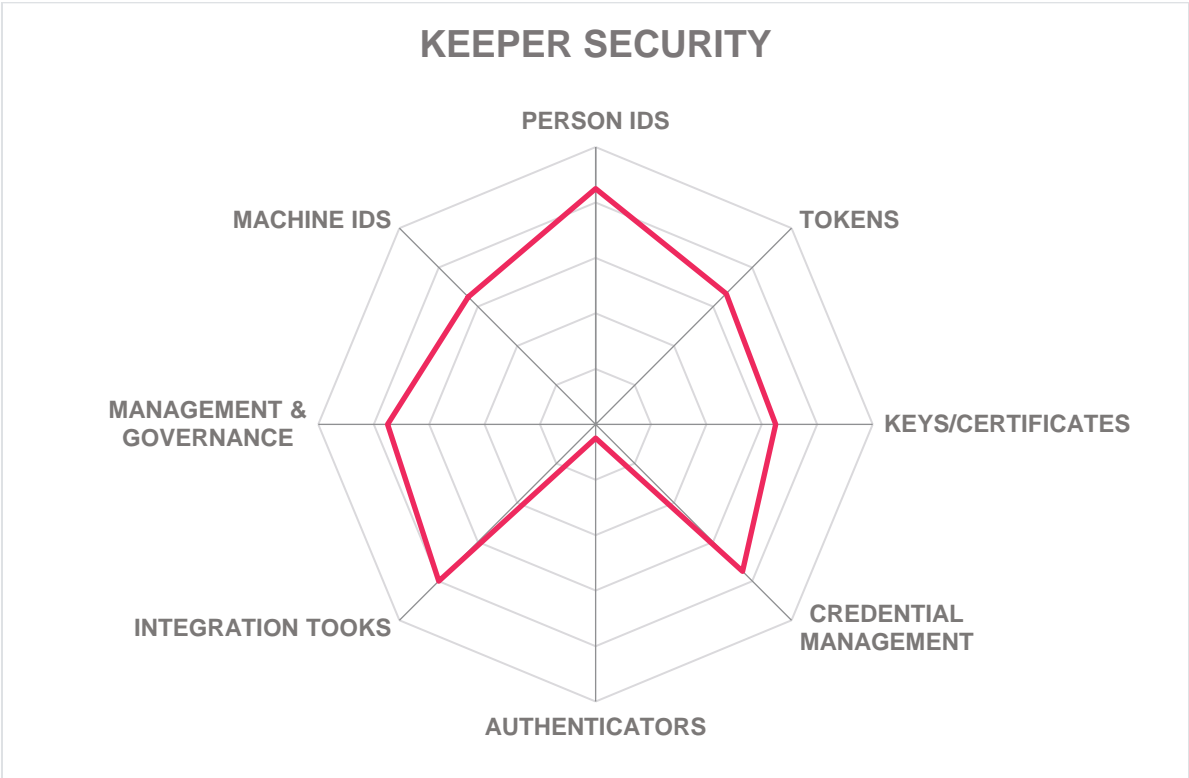
Strengths

- Fusion of password management and privileged access management
- High assurance solution with full encryption of communication
- IdP integration with major providers
- Strong DevOps support
- Comprehensive go-to-market strategy and partner network

Challenges

- Integration with legacy corporate resources e.g., on-prem services
- Market direction in managing person authentication
- Support for token/key storage devices





Keyfactor - Command

Keyfactor provides an identity-first security solution for modern enterprises. Headquartered in Ohio, Keyfactor has been in business for more than 20 years. The company has more than 400 employees and a global reach of more than 1,500 customers. Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and person. By simplifying PKI, automating certificate lifecycle management, and securing every software workload, and device, Keyfactor helps organizations to establish and maintain digital trust at scale.

Keyfactor manages a wide variety of keys: X509, CITS, SSH, Code-signing, encryption libraries etc. With the increasing emphasis on machine identities, Keyfactor helps avoid the problem of Machine ID sprawl.

Keyfactor is built on the open-source EJBCA tool, and it provides the ability to manage certificates, their issuance, knowing where they are deployed and identifying expiring certificates so they can be re-issued if required. It allows selection of the required CA for each certificate. It manages the RA process and enables governance over the security environment. The user interface enables administrators to select from a wide range of certificate types and to select the required algorithm for key-pair generation. It supports all major HSMs and provides extensibility via support for major REST and Web-services API protocols. Interfaces are also supported for EST, CMO, SCEP and ACME platforms. Keyfactor enables customers to manage policies associated with key usage, assuring only approved access to protected resources is granted.

Keyfactor's focus is on enabling emerging use-cases: DevOps, IoT and hybrid cloud requirements, as well as replacing outdated, complex PKI environments with a mainstream management solution. Keyfactor EJBCA simplifies PKI and enables it to scale. Multiple deployment options are supported:

- Software appliance
- Hardware appliance
- Cloud (AWS & Azure)
- SaaS – turnkey PKI hosted and managed by Keyfactor.

Keyfactor Command provides orchestration and automation of PKI environments, updating and simplifying outdated and complex PKI processes, by managing certificates, providing visibility over expiring certificates and providing control over certificate infrastructure.

Keyfactor Command for IoT manages device identities at scale. Keyfactor Command for IoT manages the issuance of keys for IoT devices, it automates discovery and governance of IoT security environments and can digitally sign software workloads, firmware updates and device data.

Keyfactor Signum provides digital signing, securing the integrity of software workloads such as code deployments firmware distribution or document signing.

Keyfactor’s competitive advantage is its ability to provide a single platform that unifies PKI management across the IT environment, IoT infrastructure and DevOps automation needs.

The product can be deployed on-premises, in cloud services or it can be consumed as a SaaS solution.

Licensing is subscription based. EJBCA is based on the number of instances being run and active certificates, on the certificate lifecycle management platform is based on the amount of infrastructure being supported.

Keyfactor’s product development is focused on quantum computing protection for code-signing and PKI. Keyfactor maintains leadership positions with standards organization working groups such as NIST, IETF (the Internet Engineering Task Force), and the CA/B (Certificate Authority / Browser) forum. Keyfactor expects to release full-stack post-quantum code-signing, certificate issuance, and certificate management in 2023.

Security	positive	
Functionality	positive	
Deployment	positive	
Interoperability	neutral	
Usability	neutral	

Table 10: Keyfactor’s rating

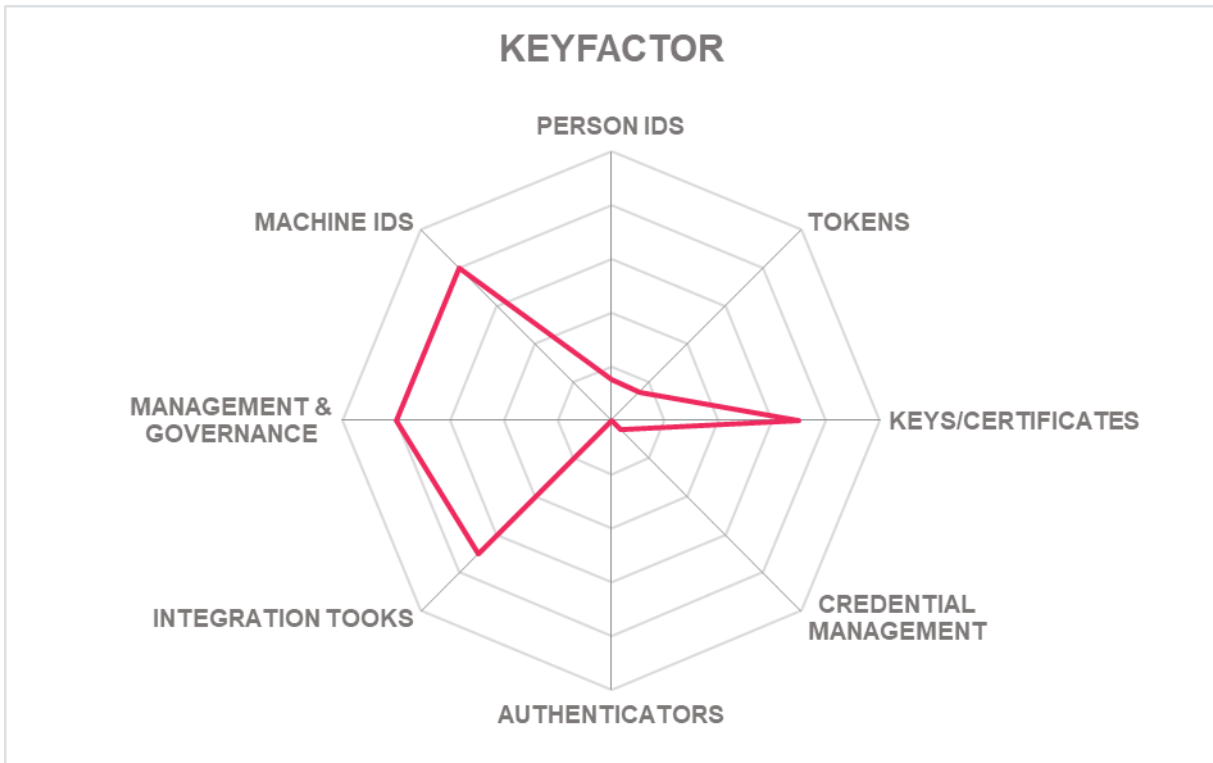
Strengths

- Comprehensive management of diverse key types
- Support for digital signing
- Comprehensive solution across IT, IoT and DevOps environments
- Strong Open-source support
- Multiple deployment options

Challenges

- Integration with corporate tools e.g., IdPs
- Support for corporate governance solutions

Leader in



Nexus – Smart ID

Nexus is part of the In Groupe; they commenced operations in 2004 and have over 300 employees across 5 offices in Europe. The vision of the company is to ‘create a safer society for everyone.’

Nexus has two main offerings:

- Go PKI – a solution to issue and manage PKI certificates.
- Go Cards – a comprehensive solution for generating personalized and encoded identification cards.

These are combined in the Go Workforce product that manages trusted identities on smartcards, PCs, smartphones etc. Integration to IdPs is provided via an OIDC connector, SCIM support and APIs for database connection.

Nexus also provides a credential management solution called Smart ID, typically deployed on corporate infrastructure. The Smart ID solution provides lifetime management of credentials from issuance to retirement on smartcards, USB devices and virtual smartcards on mobile devices. Smart ID supports both the registration and issuance of keys to storage devices as well as the management functions needed to support authentication and encryption requirements. The solution provides PKI certificate/key management for the modern workforce as well as PKI-based identities for IoT devices. Smart ID for the enterprise is deployed on corporate infrastructure.

Registration of keys/certificates to a user’s record in the corporate IdP facilitates the use of user credentials for authenticating corporate applications. Smart ID enables clients to implement policies controlling access to protected resources and authenticator device usage for key-pair generation.

The solution is available as an on-premises deployment with a support and maintenance agreement or as a SaaS solution. Licensing is by subscription based on the number of users.

Nexus also offers Machine ID automated enrollment and management using PKI standard protocols (ACME, SCEP, EST etc.) and REST APIs.

Future development is focused on improving the user experience, an expansion of the PKI-as-a-Service solution and eIDAS support for France, Germany & Nordics. Nexus is also working on a graphical BPMN tool to define registration and issuance process to improve visibility over the steps in the processes that manage key/certificate lifecycle management deployment via the Nexus solution. Nexus maintains a strong professional services team to assist clients to migrate from legacy solutions to a Nexus environment.

The development roadmap includes a ramp-up in physical access control services with innovation in the use of mobile devices and wearables.

Security	positive
Functionality	positive
Deployment	neutral
Interoperability	neutral
Usability	positive



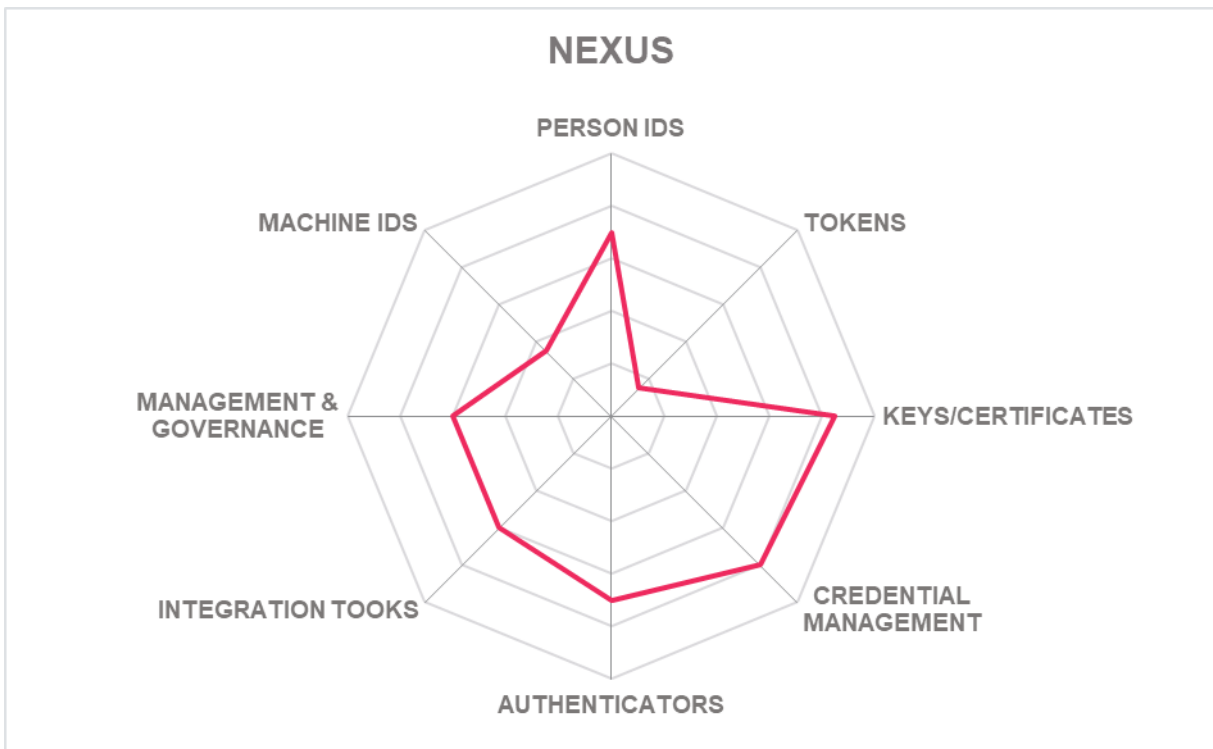
Table 11: Nexus's rating

Strengths

- Full-lifecycle credential management solution
- Wide support for diverse authenticator devices
- Managed service for PKI key management
- Integration options for identity provider services
- Integration of IoT devices

Challenges

- Expansion of enterprise support globally
- Support for emerging authentication solutions e.g., Windows Hello for Business, FIDO2
- Crypto support for smartphones



Oracle – Key Vault

Oracle is a major supplier of database solutions and has for many years offered the Key Vault product that is primarily used to store encryption keys for encrypted Oracle Databases, MySQL databases, and Oracle infrastructure components such as ZFS Storage Appliance, Advanced Cluster File System (ACFS), and GoldenGate encrypted trail files. KeyVault is increasingly being used to store secrets for other purposes, and recent releases have enhanced the product's capabilities in this area.

Key Vault provides highly available and fault-tolerant encryption key management. While it's focused on database architectures it is fully capable of managing secrets for other purposes, providing Oracle Key Vault customers with the ability to store other secrets, at no additional license cost.

Installation is highly automated; it simply requires the IP address of the host server and an administration password, and the system will install the operating system, database and application and be ready to use within 30 minutes. Key Vault is delivered as a software appliance that can be installed in company data centers, on dedicated servers or as a VM guest. It can also be deployed on Oracle Cloud Infrastructure from the Oracle Cloud Marketplace. Multiple instances of Key Vault can be paired to form a highly available cluster across an enterprise's entire infrastructure, including their cloud tenancy in Oracle OCI. A competitive advantage for Oracle is the high availability this affords, with 'seven nines' being claimed for Key Vault critical infrastructure.

Key Vault administrators and endpoint owners can strictly control if and with which person or process a secret can be shared, optionally granting read-only access to the keys and/or secrets.

Key Vault provides certificate storage and distribution. Any certificate uploaded to Key Vault will be managed for expiration date and will be included in certificate management reporting that provides visibility over keys used across the corporate environment, including the algorithms they employ and their usage. A Java SDK provides the ability to automatically rotate keys where allowed.

Key Vault can also centrally manage and distribute Java KeyStores. A typical workflow might be an administrator (person or process) updating a Java KeyStore (JKS) in Oracle Key Vault, allowing read-only endpoints to automatically download the updated JKS. The password that is applied to a JKS that contains private keys is also managed by the Key Vault administrator and is automatically applied when the JKS is downloaded and stored on a local disk.

Key Vault can be deployed as a software appliance, typically on a VM, or on the Oracle Cloud Infrastructure. It supports the KMIP protocol and PKCS11.

Licensing is per-installation, and is not dependent on the number of encryption keys stored or endpoints deployed. There is no extra charge to store other secrets.

Recent developments include the release of on-line SSH keys whereby the keys never have to leave the Key Vault. Current development is focused on support for the Azure Cloud and branching out to the storage of other 'secrets'.

Security	strong positive	
Functionality	neutral	
Deployment	positive	
Interoperability	neutral	
Usability	strong positive	

Table 12: Oracle's rating

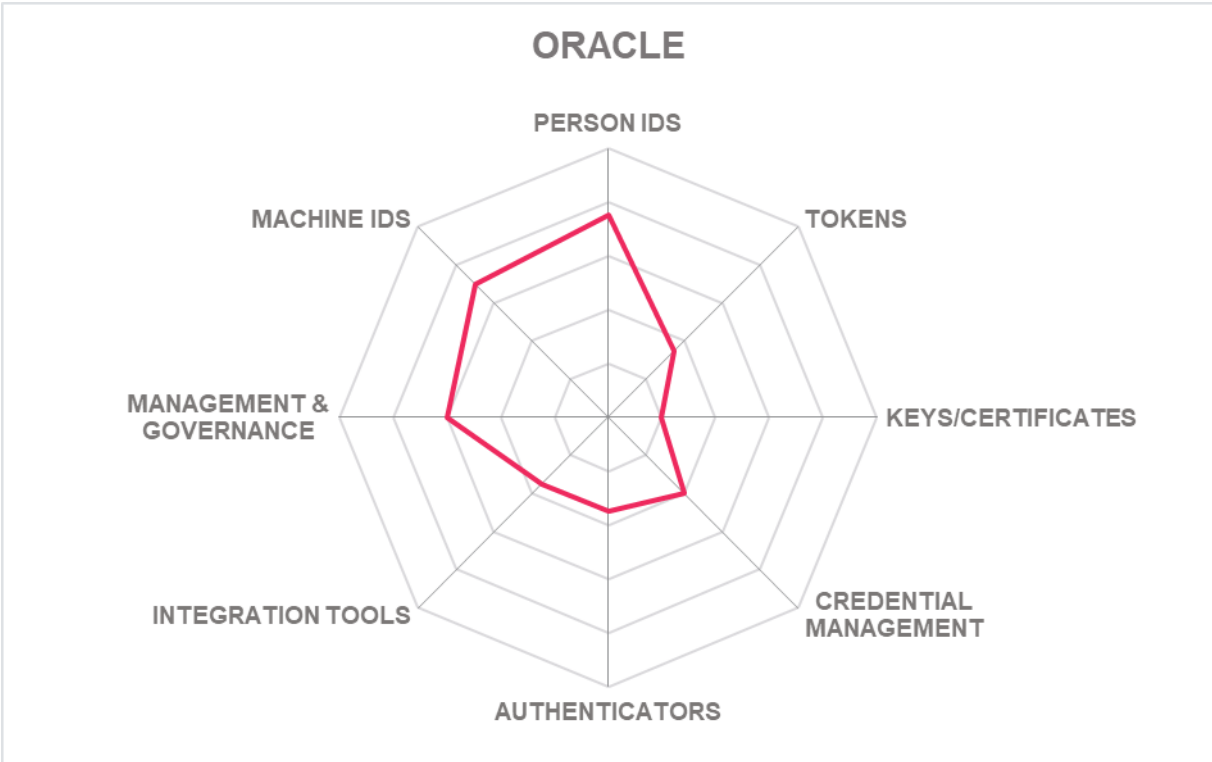
Strengths

- Mature key management, primarily for Oracle infrastructure keys
- Integrated 'wallet' approach for users to manage their keys
- On-line SSH key service
- HA key management across on-prem and cloud infrastructure
- Ability to leverage existing infrastructure for secret management requirements

Challenges

- Credential management for non-Oracle keys
- Support on major public cloud services
- Only viable for Oracle customers





Smallstep

Smallstep is a startup based in California providing a PKI solution to secure cloud deployments. The solution is focused on machine IDs and is packaged as an 'orchestration platform' for DevOps. The solution secures access to organization infrastructure by identifying everything and everyone, and issuing credentials to identities for authentication and encrypting data. Smallstep consider their main offering as an 'identity orchestration' company.

Smallstep considers encrypted communications as a base requirement for enterprises today, and PKI management of their 'secrets' i.e. identity credentials, is expected. The core offering is an open-source certificate manager providing advanced access control, approval workflows and audit/reporting tools.

Smallstep Certificate Manager is built on the ACME framework and provides a comprehensive PKI service for secure network connections (TLS, HTTPS, SSH). The product provides a flexible and scalable solution for secrets management that is secured via a comprehensive certificate management process. Support for ACME Device Attestation, securing keys to the source devices, is in the development pipeline.

The following platforms are supported:

Kubernetes Istio, MongoDB, OpenSSH, gRPC, Cassandra, Vault, Kafka, RabbitMQ, Elastic, Ansible PostgreSQL Docker, Linkerd, Caddy

The Certificate Manager provides a managed service that automates certificate management. It builds on an open-source offering, adding advanced access control, audit and transparency across the certificate management environment.

The provision of certificate inventories aids in the management of certificates and related access control.

Smallstep ACME Registration Authority can automate the initial enrolment, and subsequent renewal of certificates for compliant clients such as Certbot, Terraform Caddy and Kubernetes cert-manager.

Smallstep SSH provides a low-friction solution for SSH key management. It supports OAuth for integration with the corporate IdP and automates issuance of certificates. It manages expiry and revocation of system access if a user is removed from the IdP.

Smallstep is delivered as a secure and highly available SaaS offering. It can be hosted on-premises or deployed on cloud services.

The development pipeline is focused on delivering a Zero-Trust Platform solution that provides management of, and transparency over, access control within an organization.

Security	strong positive
Functionality	strong positive
Deployment	positive
Interoperability	positive
Usability	positive



Table 13: Smallstep's rating

Strengths

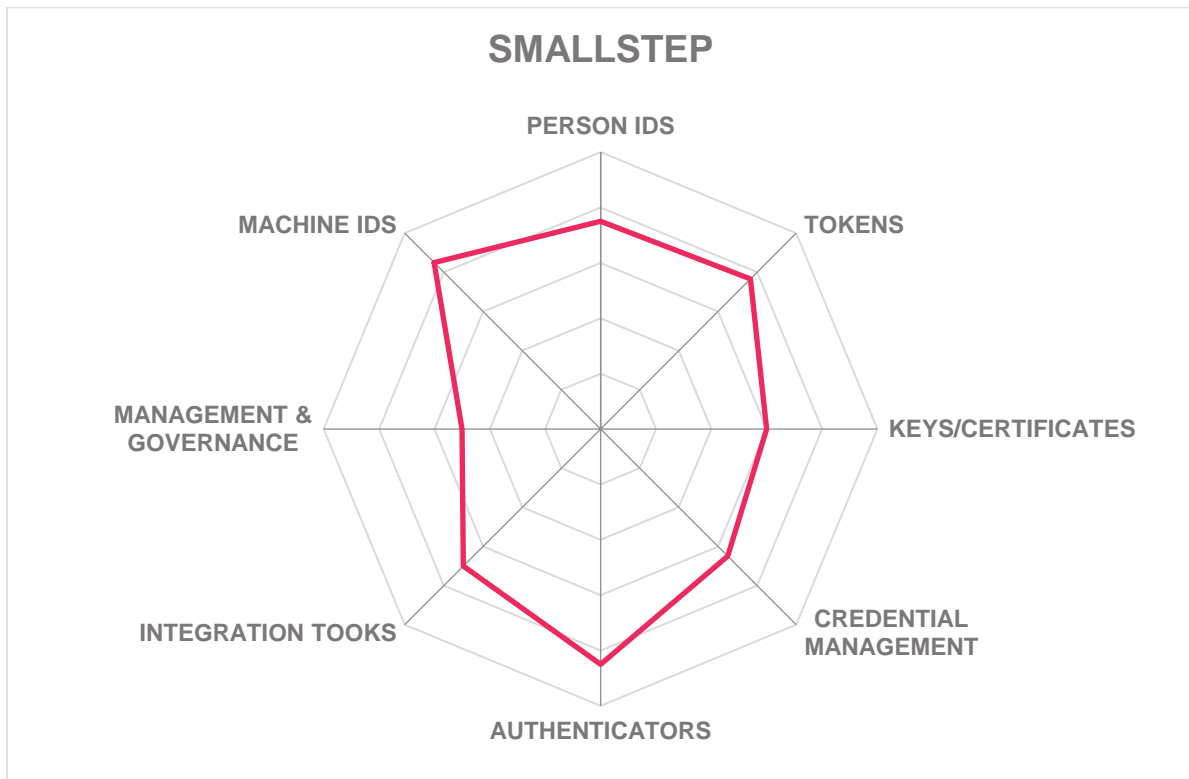
- Automated certificate management
- Strong DevOps platform support
- Registration authority integration
- Support for major multi-cloud and microservices tools
- Open-source support

Challenges

- Wider support for people key/certificate management
- Integration with corporate governance tools
- Marketing program extension

Leader in





Versasec – vSEC:CMS

Versasec commenced operations in 2007 and is headquartered in Stockholm, Sweden. The company maintains offices in Austin, USA, Cairo, Egypt, Kuala Lumpur, Malaysia, Merseburg, Germany and Waterloo, UK.

Versasec provides an enterprise-level Credential Management System solution that issues and manages digital identity credentials, providing secure authentication, digital signing and encryption, for people and things. vSEC:CMS supports PKI and FIDO credentials for the corporate market using key storage devices such as smartcards or USB authenticators.

The vSEC:CMS product suite is a complete credential management system that can be deployed either as an on-prem software solution or in a VPC available on Azure and AWS Marketplaces. A 'lite' app, called vSEC:CMS Agent or vSEC:CMS User, enables service desk reps, or users via a self-service app, to manage credential lifecycle events. A cloud-based deployment is available via the vSEC:CLOUD managed service.

vSEC:CMS enables administration and management of authentication credentials in a secure way. The product suite provides functions for managing physical and virtual smart cards, Windows Hello for Business, Thales IDPV, RFID devices, corporate badges or USB storage devices with PIV or FIDO capabilities. Full lifecycle management of credentials is supported from the initial issuance, to maintenance requirements, to revocation. Maintenance includes modification of user details, PIN changes, blocking/unblocking keys, and certificate management.

Registration of a new user can occur in a number of ways. The on-boarding process can call vSEC:CMS via an API, requesting the issuance of a smartcard or USB device. Customizable workflows then allow the device to be associated with a user and to personalize the device which is typically delivered in a PIN-locked state. When the user receives the device they authenticate using a secondary authentication method to complete the process which securely sets their PIN and applies the appropriate policies to activate the device. The process can also be accomplished via a self-service application. Alternately, an enterprise can elect to use a batch issuance process with PINs communicated via an out-of-band process.

Enrollment typically includes generation of asymmetric keys, requests for certificates, optional escrowing of keys used for encryption, printing company and user information on the physical device, setting PIN policies, distributing PINs using PIN mailers, setting PUCs, writing RFID files and more.

vSEC:CMS integrates with corporate IdPs, letting relying-party applications take advantage of FIDO2 and PKI with the use of standard federation/SSO protocols

Corporate governance is supported by writing events to Windows logs and via an events database (SQL) that can be fed into a SIEM tool; providing transparency over the credentialing process

Machine identities can be managed via the built-in ACME server which allows for certificates of any_type to be issued/re-issued and revoked from all connected endpoints, including microservices.

Security	positive	
Functionality	strong positive	
Deployment	neutral	
Interoperability	neutral	
Usability	positive	

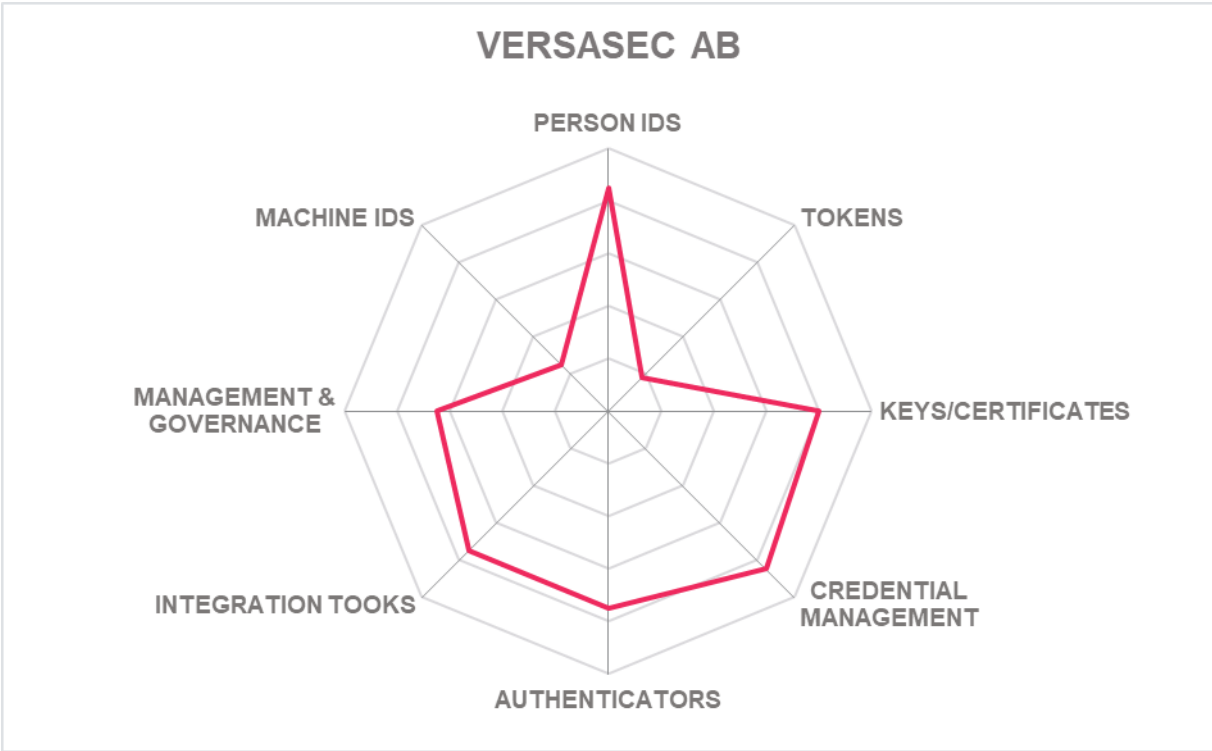
Table 14: Versasec's rating

Strengths

- Mature credential management solution
- Integration into corporate management tools
- FIDO2 support
- Self-service for authenticator issuance and deployment
- Mobile device support for authenticators

Challenges

- Credential manager support for life-cycle management of FIDO2 key-pairs
- Support for Machine ID automation
- Integration with DevOps tools



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

Akeyless

Akeyless Security is an Israeli company dedicated to protecting and managing credentials, certificates, and keys used by machines, applications, and DevOps teams.

The Akeyless Vault Platform is a SaaS vault service to create and securely store credentials such as certificates and keys for use across hybrid and multi-cloud environments.

Akeyless Secure Remote Access for humans and machines provides support for DevOps staff needing access to remote infrastructure and staff 'working from home'.

Why worth watching: Akeyless provide a comprehensive solution focused on securing software workloads for DevOps staff.

Axiad

Axiad is based in California, USA and is focused on delivering secure authentication solutions for their clients.

The Universal CMS solution manages end-user credentials via an on-premises application. It is designed to suit a wide range of use cases in a future-proof solution that unifies the management of credentials across the enterprise. It UCMS solution streamlines the authentication workload, it can be deployed on Windows, Linux and MacOS infrastructure.

Why worth watching: Axiad has built a reputation as a reliable supplier of tools for secrets management.

HYPR

Based in New York, USA, HYPR is a cybersecurity company focused on password-less authentication of users.

The focus is on providing an MFA environment that supports SSO for staff and partners as well as a solution that can scale to accommodate a company's customer base to secure remote access from account-take-over vulnerability.

The Hypr solution supports PCs, smartphones and USB devices, it integrates with corporate IdPs and major identity authentication service providers.

Why worth watching: HYPR fully supports FIDO 2 and maintains an impressive customer base and partner network.

Thales

Thales Group is a French multinational company that provides mature secrets management via number of products:

The Thales HSM provides tamper-proof key generation and storage. It is available as a hardware appliance or via a cloud solution. SafeNet KeySecure is a virtual solution for scaling key management in a to manage keys and data encryption in an environment that can scale and enforce access control across cloud infrastructure

The Vormetric Data Security Manager provides a key management solution with policy enforcement via a centralized security management console.

Why worth watching: With the acquisition of Gemalto, Thales secured their reputation as a world leader in digital security.

Venafi

As a leading supplier of security solutions to industry Venafi's solutions are built around securing typical operations within an enterprise.

- Jetstack Secure is a certificate manager that automates validation of cloud native workloads for Kubernetes and OpenShift platforms. It ensures PKI controls and provides an auditable chaining of trust for workloads deployed as Kubernetes containers.
- SSH Protect provides visibility, intelligence and automation for your SSH machine identity management
- TLS Protect is a TLS solution that can discover all your SSL/TLS certificates and corresponding private keys in order to protect machine identities from outages and to quickly respond to certificate vulnerabilities or CA compromise
- CodeSign Protect is a private key management facility that ensures private keys never leave their secure location (typically the infrastructure on which they were generated)

Why worth watching: Venafi is a mature supplier of secret management tools.

Methodology

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.

Related Research

[81111 Leadership Compass PAM 2023](#)

[81215 Leadership Compass Passwordless Authentication](#)

[80767 Leadership Compass CIEM & Dynamic Resource Entitlement & Access Management \(DREAM\) platforms](#)

Copyright

©2023 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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

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

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