kuppingercole ANALYSTS

Enterprise Secrets Management

Martin Kuppinger

April 28, 2025

LEADERSHIP COMPASS 2025

This report provides an overview of the Enterprise Secrets Management market, spanning secrets for humans, workloads, and things, and a compass to help you find a solution that best meets your needs. It examines solutions that provide secrets lifecycle management for a wide range of secret types and use cases. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and manage these risks.

Contents

Executive Summary

The management of digital secrets has evolved from a niche concern within specific IT domains to a cornerstone of enterprise security strategies. In the Leadership Compass for Enterprise Secrets Management for Humans, Workloads, and Things, we explore a dynamic market segment dedicated to securing a broad spectrum of sensitive credentials that are needed and used in modern IT ecosystems. This market extends beyond traditional key and certificate management to encompass an extensive range of secrets, including API keys, tokens, SSH keys, encryption keys, passkeys, and more, addressing the needs for managing both human and non-human identities.

The demand for comprehensive secrets management solutions is driven by the increasing complexity of IT environments, the proliferation of machine identities, and the critical need to secure DevOps pipelines, cloud-native applications, and industrial IoT (IIoT) deployments. Organizations face the dual challenge of managing secrets for human users, such as passwords and authentication tokens, and for non-human entities, including workloads, applications, and devices. Poorly managed secrets expose enterprises to significant risks, including data breaches, account takeovers, and operational disruptions. These risks are exacerbated by common issues like secrets sprawl, insufficient visibility, hardcoded credentials, and inadequate lifecycle management.

Key business drivers for adopting enterprise-grade secrets management solutions include regulatory compliance, the shift towards zero-trust architectures, and the need for crypto-agility to respond to evolving security threats, including those posed by quantum computing. Enterprises are increasingly seeking solutions that provide centralized governance, thorough auditing, automated secrets lifecycle management, and integration with a wide range of IT systems and DevOps tools.

Major use cases span many operational domains. For human identities, secrets management supports secrets used in multi-factor authentication, secure credential storage, and traditional certificate-based authentication. In the area of workloads, it ensures the integrity and confidentiality of communications within and across cloud environments, microservices, and CI/CD pipelines. For devices, particularly in IoT and IIoT contexts, secrets management facilitates secure device provisioning, firmware signing, and encrypted communications at scale.

The market structure reflects these varied demands, with solutions categorized based on their support for different types of identities and secrets. Some vendors offer broad, integrated platforms capable of managing secrets across the enterprise, while others focus on specialized areas such as non-human identity (NHI) management or IoT device security. Notably, NHI management is emerging as a significant segment due to the exponential growth of machine identities, far outpacing human ones, and the corresponding need for scalable, secure management practices.

Current trends indicate a convergence of secrets management with adjacent security domains. There is increasing overlap with Privileged Access Management (PAM) solutions, particularly as PAM vendors expand into NHI management. Additionally, the integration of secrets management with Cloud Infrastructure Entitlement Management (CIEM) is gaining traction, reflecting a broader trend towards unified identity and access governance for both human and non-human entities.

Innovations in the field are also being shaped by the rise of DevOps and cloud-native development practices. Solutions are evolving to offer seamless integration with CI/CD pipelines, automation frameworks, and container orchestration platforms, reducing the operational burden on developers while enhancing security postures. Furthermore, support for quantum-safe encryption (QSE) and advanced cryptographic standards is becoming increasingly relevant as organizations prepare for future security challenges.

In evaluating the solutions within this Leadership Compass, we focus on their ability to deliver comprehensive secrets lifecycle management, support for diverse use cases across supporting different types of identities, and strong governance capabilities. We also consider factors such as scalability, ease of integration, and the flexibility to adapt to evolving security requirements. This report aims to provide clear insights into the capabilities of various vendors, helping organizations make informed decisions to strengthen their secrets management strategies in an increasingly complex digital landscape.

For detailed information about the KuppingerCole Leadership Compass Methodology is available in the separate document behind the above link.

Key Findings

- The market for Enterprise Secrets Management spans human, workload, and device identities, focusing on centralized, enterprise-grade management over point solutions.
- Secrets include passwords (with minor relevance for this Leadership Compass), API keys, encryption keys, private keys of certificates, tokens, SSH keys, database credentials, and passkeys, all of which are critical for cybersecurity.
- Poor secrets management leads to risks such as secrets sprawl, hardcoded credentials, and insufficient lifecycle control, leading to security breaches and operational failures.
- The market is evolving beyond traditional EKCM to support modern needs like FIDO2 tokens, passkeys, and extensive non-human identity (NHI) management.
- NHI management is rapidly growing due to the vast number of machine identities, often unmanaged, posing significant security risks.
- Integrated lifecycle management, governance, and automation are increasingly essential, particularly for large enterprises seeking to control "vault sprawl."
- Emerging trends include convergence between NHI Management and CIEM, forming comprehensive identity and access management for non-human identities.
- Solutions are expected to integrate deeply with DevOps tools, offloading security tasks from developers to IT security teams for streamlined operations.
- Overall Leaders are Akeyless, BeyondTrust, CyberArk, Delinea, SSH, and Thales.
- Product Leaders are Akeyless, AppViewX, BeyondTrust, CyberArk, Delinea, SSH, and Thales.
- Innovation Leaders are Akeyless, AppViewX, BeyondTrust, CyberArk, Delinea, SSH, and Thales.

Market Analysis

The market for Enterprise Secrets Management for humans, workloads, and things encompasses solutions designed to securely manage a broad spectrum of digital secrets across diverse environments. It is a market segment where few vendors deliver comprehensive solutions, while we find many specialist vendors covering certain aspects of the market.

Enterprise customers are increasingly requesting comprehensive solutions providing governance and lifecycle management spanning multiple types of secrets and use cases. We expect this to be reflected in the further development of the market, where we also expect to see many acquisitions. In the current state of the market, customers are well-advised to look at both strategic providers of comprehensive solutions spanning multiple identity and secret types, and tactical, specialized solutions for instance for NHI to address gaps in their current security posture. Both are viable strategies in a rapidly emerging and maturing market.

Market Segment Structure

The market for Enterprise Secrets Management is structured around the types of identities and secrets managed, as well as the specific functional capabilities provided. The primary subsegments include:

- **Human Identity Secrets Management:** Focuses on managing credentials such as passwords, passkeys, and cryptographic keys for individual users. Emphasizes secure storage, lifecycle management, and integration with identity governance systems.
- **Workload or Non-Human Identity (NHI) Secrets Management:** Addresses the growing need to manage secrets for workloads, services, and automated processes. Solutions in this segment often integrate with DevOps tools and CI/CD pipelines.
- **Device (Things) Identity Secrets Management:** Covers management of secrets for IoT and IIoT devices, including secure provisioning, authentication, and cryptographic operations at scale.
- **Secrets Discovery and Lifecycle Management:** Provides tools for identifying, monitoring, and managing the lifecycle of secrets across disparate environments, helping organizations reduce "vault sprawl" and enhance governance.
- **Integrated PKI and Cryptographic Key Management:** Encompasses solutions with built-in PKI capabilities or strong integration with external PKI infrastructures, focusing on certificate lifecycle management and crypto-agility.

Delivery Models

Enterprise Secrets Management solutions are delivered through various models to meet diverse organizational requirements:

- **On-Premises Deployments:** Preferred by organizations with strict regulatory requirements or those needing full control over their security infrastructure. These solutions integrate with existing enterprise IT environments and support legacy systems.
- **Cloud-Based Services:** Offer scalability and ease of deployment, particularly suited for organizations with dynamic, distributed environments. These services support

multi-tenant architectures and provide robust API integrations. Almost all NHI management solutions focus on pure cloud deployments.
- **Hybrid Models:** Combine on-premises and cloud capabilities, allowing organizations to maintain sensitive operations locally while leveraging cloud efficiencies for broader management tasks.
- **Embedded Solutions:** Integrated directly into applications, development pipelines, or device firmware, providing seamless secrets management without external dependencies.

Required Capabilities

To effectively manage enterprise secrets, solutions must offer a comprehensive set of capabilities:

Common Capabilities:

- Secure storage for diverse secret types (passwords, API keys, tokens, and certificates).
- Centralized secrets vault with role-based access control (RBAC).
- Automated secrets rotation and lifecycle management.
- Secrets discovery and auditing across distributed environments.
- Integration with identity providers (LDAP, SAML, and OIDC).
- API-first architecture for DevOps and CI/CD integration.
- Encryption at rest and in transit, supporting modern cryptographic standards.
- Detailed auditing, reporting, and compliance tracking.
- Support for multi-factor authentication (MFA) and fine-grained access policies.
- Secrets governance frameworks with policy enforcement.

Human Identity Secrets Management:

- Management of user credentials, including passwords, passkeys, and biometric data.
- Support for strong authentication mechanisms (e.g., FIDO2, smartcards).
- Integration with single sign-on (SSO) and identity governance platforms.
- Self-service portals for credential management and recovery.
- Monitoring and alerting for credential misuse or compromise.

Non-Human Identity (NHI) Secrets Management:

- Automated secrets provisioning for applications and services.
- API key management with granular access controls.
- Integration with DevOps tools (Jenkins, Kubernetes, and Docker).
- Secrets injection for runtime environments without hardcoding.
- Support for SPIFFE/SPIRE for workload identity federation.

Device Identity Secrets Management:

- Secure provisioning and lifecycle management of IoT/IIoT device credentials.
- Support for hardware-based security modules (HSMs and TPMs).
- Scalable management of device certificates and cryptographic keys.

- Remote attestation and device integrity verification.
- Secure firmware updates and over-the-air (OTA) management.

Trends and Evolution

The Enterprise Secrets Management market is undergoing significant transformation driven by shifts in technology, regulatory landscapes, and operational requirements. Historically centered around EKCM for human credentials, the market is now expanding to address the complexities of managing secrets for NHIs and devices.

One of the most notable trends is the rise of Workload Identity Management or Non-Human Identity Management, sometimes also referred to as Machine Identity Management. The proliferation of APIs, microservices, and automated workflows has created an exponential growth in machine identities, far outpacing human users. Organizations face challenges managing these identities securely, as traditional secrets management practices are often inadequate. Hardcoded secrets, poor rotation practices, and fragmented vaults contribute to increased security risks. In response, both emerging vendors and established players, particularly those from the Privileged Access Management (PAM) space, are enhancing their solutions to support NHIs comprehensively.

Another key development is the convergence of secrets management with broader identity and access management (IAM) domains. Solutions are increasingly integrating with Cloud Infrastructure Entitlement Management (CIEM) platforms, creating unified approaches for managing entitlements, access, and secrets across cloud environments. This convergence is particularly relevant for large enterprises seeking holistic visibility and control over their security posture.

The shift towards DevOps-centric environments has also influenced the evolution of secrets management. As organizations adopt agile development practices and continuous deployment pipelines, the need for automated, scalable secrets management becomes critical. Vendors are responding with deeper integrations into DevOps toolchains, enabling better secrets handling without compromising developer productivity or security standards.

Quantum-safe encryption (QSE) is emerging as another focal point. With the advent of quantum computing, traditional cryptographic algorithms face potential obsolescence. Forward-looking secrets management solutions are incorporating QSE capabilities to future-proof their cryptographic frameworks.

Governance and compliance remain central to the evolution of this market. Organizations are under increasing pressure to demonstrate effective security controls and regulatory compliance. As a result, secrets management solutions are enhancing their governance features, offering advanced auditing, policy enforcement, and reporting capabilities to support compliance with frameworks like GDPR, HIPAA, and PCI DSS.

In summary, the Enterprise Secrets Management market is shifting from isolated, point solutions to integrated platforms capable of managing many different secret types across complex, hybrid environments. The focus is on automation, scalability, and governance, with an emphasis on addressing the unique challenges posed by non-human identities, evolving cryptographic requirements, and regulatory demands. Vendors that can deliver

comprehensive, adaptable solutions will be well-positioned to meet the dynamic needs of modern enterprises.

Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

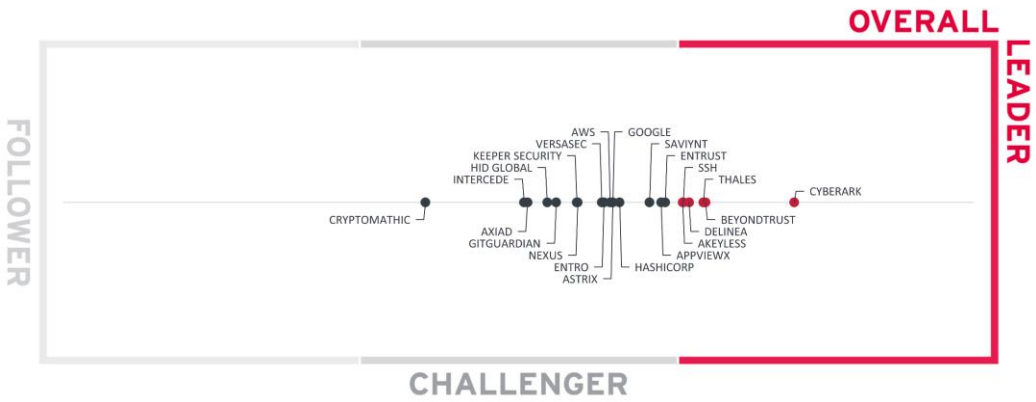


Figure 1: Overall Leadership in the Enterprise Secrets Management market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Among the Overall Leaders, we find CyberArk ahead, with strong capabilities in managing human and non-human identities and a large market presence. Thales, partially building on the technology of Akeyless, also takes a strong position with a broad technology portfolio and global market presence. Following Thales, we find two more vendors with roots in the PAM space, BeyondTrust and Delinea. Both are investing heavily in the expansion into the NHI market and benefit from their good market presence. SSH and Akeyless also earned an Overall Leadership rating based on their good set of capabilities and relevance in this market segment.

Among the Challengers, we find a range of vendors. NHI specialist vendors such as AppViewX, Astrix, Axiad, Entro, or GitGuardian provide innovative solutions to the market, but do not yet cover the entire range of requirements for Enterprise Secrets Management. There are hyperscalers such as AWS and Google, with a strong solution portfolio, but are primarily focused on their own environments. HashiCorp, now part of IBM, is also a hyperscaler, with a strong presence as provider of secrets vaults for NHI use cases but has limitations beyond that. Saviynt is another vendor entering the market by expanding its PAM solutions. Entrust and HID Global are established players in the cybersecurity market, delivering a range of solutions that also support various of the use cases within Enterprise Secrets Management, but being more limited in the emerging NHI subsegment. The other vendors such as Cryptomathic, Intercede, Keeper Security, Nexus, and Versasec also provide specialized solutions that contribute to an Enterprise Secrets Management strategy, but do not yet cover all aspects we are looking for. With Enterprise Secrets Management being such a complex field, most customers will be best suited with a combination of a core solution that is complemented by specialized solutions for areas that are not covered by the core solution at the required level.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Akeyless
- BeyondTrust
- CyberArk
- Delinea
- SSH
- Thales

Product Leadership

Product leadership is the first specific category examined below. This view is based on the presence and completeness of required features as defined in the required capabilities section above. 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 in the center. Followers are in the lower section.

Figure 2: Product Leadership in the Enterprise Secrets Management market

In the Overall Leader section, we again find some of the established PAM players that are expanding into the NHI management subsegment, with CyberArk leading based on their product portfolio and the Venafi acquisition. The fact that all leaders being positioned in the lower half of the Product Leadership section indicates that there are no fully comprehensive solutions available on the market. Following CyberArk we find Thales, with a portfolio that

utilizes the technology of Akeyless, but also builds on a range of other capabilities. The other vendors in the Product Leader section, Akeyless, AppViewX, BeyondTrust, Delinea, and SSH are all placed close to each other.

In the Challenger section, we find a dense field of vendors. Saviynt is close to becoming a leader. Nexus, Entrust, Versasec, and Keeper Security follow, with more specialized solutions covering different aspects of Enterprise Secrets Management. Close to them, we find NHI specialists with leading-edge capabilities in that field such as Astrix, Axiad, and Entro Security, as well as the hyperscalers AWS and Google, and HashiCorp with their market-leading vault for developers. Intercede and HID Global are also placed in this section, delivering specialized solutions. GitGuardian is also positioned in that group, delivering leading-edge secrets discovery capabilities that can complement other vendors' solutions. Somewhat further down we find Cryptomathic, delivering a highly specialized solution for key management that allows managing symmetric and asymmetric keys at scale. This makes them an interesting complement to other solutions as well as for specialized high scalability use cases, while Cryptomathic does not cover the full breadth of Enterprise Secrets Management use cases.

Product Leaders (in alphabetical order):

- Akeyless
- AppViewX
- BeyondTrust
- CyberArk
- Delinea
- SSH
- Thales

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and emerging business requirements. Innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other innovative features, while maintaining compatibility with previous versions.

This view is based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

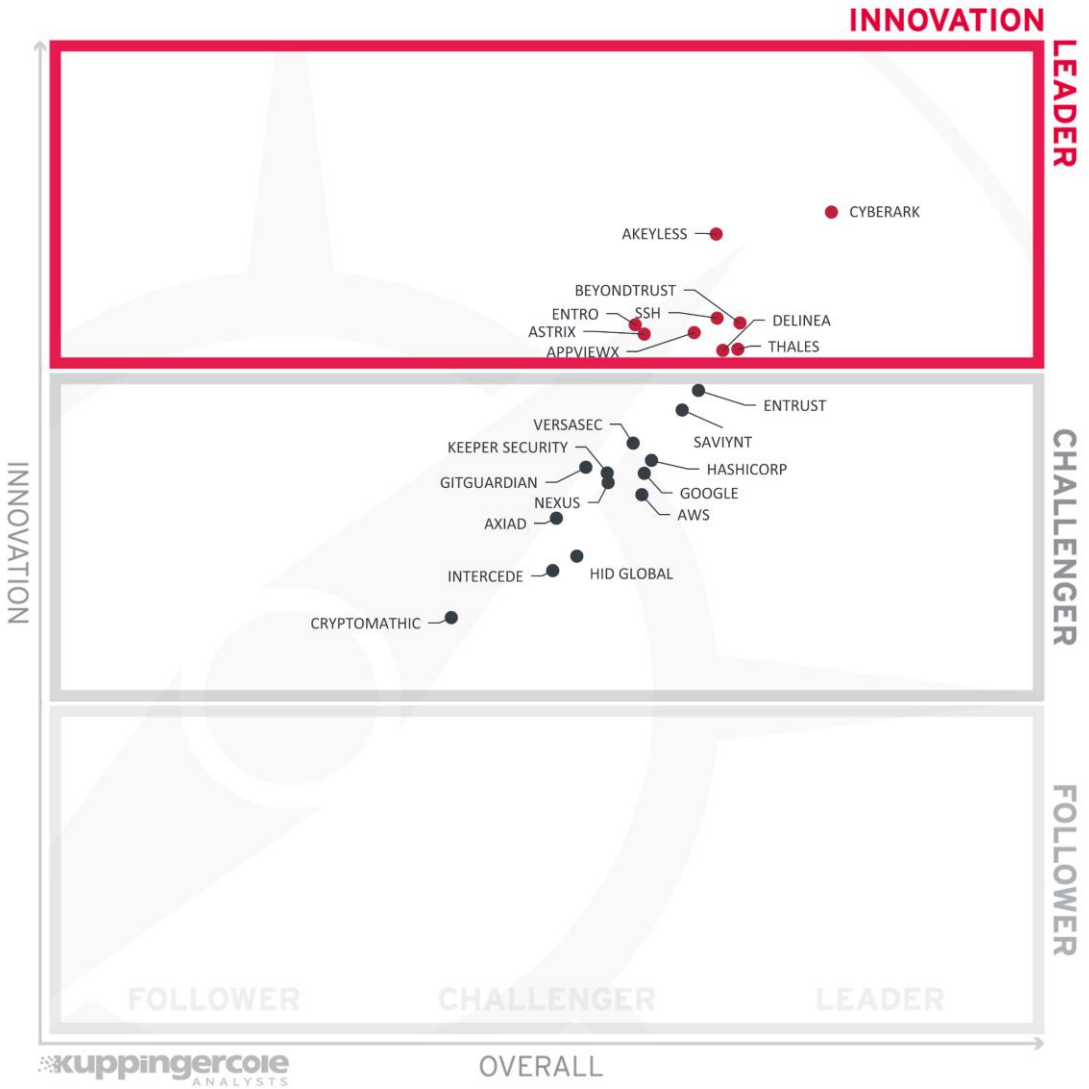


Figure 3: Innovation Leadership in the Enterprise Secrets Management market

Innovation Leaders are those vendors that are delivering innovative products, not only in response to customers' requests, but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are forward thinking and bring advancements to their customers.

A number of the vendors in the Challenger section already have achieved a KuppingerCole Rising Star rating, indicating strong innovation in a particular segment of the market and a strong product/market fit. These vendors are not yet Leaders in the Enterprise Secrets Management market but are an excellent choice in certain subsegments of this market. Further information on these vendors can be found in the KuppingerCole Research Library.

CyberArk again takes the top position here, closely followed by Akeyless. Thales, also using technology of Akeyless, scores lower because some of their innovation is derived from Akeyless. The other vendors are all close to each other, including AppViewX, Astrix, BeyondTrust, Delinea, Entro, and SSH.

In the Challenger section, we find the other vendors, spread across the section. Several of the established players such as Thales and vendors entering from the PAM space such as Saviynt take a good position. Behind them, we find a large group of other vendors, with only Cryptomathic being a bit further down. This is due to the specialization of Cryptomathic, where they provide strong capabilities in their domain, but not a broad coverage across the various use cases within Enterprise Secrets Management.

Innovation Leaders (in alphabetical order):

- Akeyless
- AppViewX
- Astrix
- BeyondTrust
- CyberArk
- Delinea
- Entro
- SSH
- Thales

Market Leadership

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

In this chart, 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 4: Market Leaders in the Enterprise Secrets Management Market

Market Leaders in this area are the leading PAM vendors that already provide good capabilities beyond human identities, but also the hyperscalers Google and AWS and also HashiCorp with their leading position in the secrets vault market for developers. Entrust and Thales, as exceptionally large security vendors, are also positioned in this segment.

The other vendors, many of them being specialist vendors and start-ups, are all in the Challenger section. All these vendors have a strong potential for growth based on the innovation and/or specialization they are demonstrating.

Market Leaders (in alphabetical order):

- AWS
- BeyondTrust
- CyberArk
- Delinea
- Entrust
- Google
- HashiCorp
- Thales

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. 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.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
AKEYLESS	strong positive	strong positive	positive	strong positive	positive
APPVIEWX	strong positive	strong positive	positive	strong positive	positive
ASTRIX	positive	positive	positive	positive	positive
AWS	strong positive	neutral	positive	neutral	positive
AXIAD	positive	positive	positive	positive	positive
BEYONDTRUST	strong positive	strong positive	strong positive	positive	positive
CRYPTOMATHIC	neutral	neutral	neutral	neutral	neutral
CYBERARK	strong positive	strong positive	strong positive	strong positive	strong positive
DELINEA	strong positive	positive	strong positive	strong positive	strong positive
ENTRO	positive	positive	positive	positive	positive
ENTRUST	strong positive	positive	positive	strong positive	positive
GITGUARDIAN	positive	neutral	positive	positive	positive
GOOGLE	strong positive	neutral	positive	neutral	positive
HASHICORP	positive	neutral	positive	positive	positive
HID GLOBAL	positive	positive	neutral	neutral	neutral
INTERCEDE	strong positive	neutral	neutral	neutral	positive
KEEPER SECURITY	strong positive	neutral	positive	positive	positive
NEXUS	positive	positive	positive	positive	positive
SAVIYNT	strong positive	positive	strong positive	strong positive	positive
SSH	strong positive	positive	strong positive	strong positive	strong positive
THALES	strong positive	strong positive	strong positive	strong positive	strong positive

VERSASEC	positive	positive	positive	positive	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
AKEYLESS	strong positive	positive	positive	positive
APPVIEWX	strong positive	positive	positive	positive
ASTRIX	strong positive	neutral	positive	neutral
AWS	positive	strong positive	strong positive	strong positive
AXIAD	neutral	neutral	neutral	neutral
BEYONDTRUST	positive	strong positive	strong positive	strong positive
CRYPTOMATHIC	neutral	neutral	positive	neutral
CYBERARK	strong positive	strong positive	strong positive	strong positive
DELINEA	strong positive	positive	strong positive	strong positive
ENTRO	strong positive	neutral	neutral	positive
ENTRUST	positive	positive	strong positive	strong positive
GITGUARDIAN	positive	neutral	neutral	neutral
GOOGLE	positive	strong positive	strong positive	strong positive
HASHICORP	positive	strong positive	strong positive	strong positive
HID GLOBAL	neutral	positive	strong positive	positive
INTERCEDE	positive	neutral	neutral	neutral
KEEPER SECURITY	positive	neutral	neutral	neutral
NEXUS	positive	neutral	positive	neutral
SAVIYNT	positive	positive	positive	strong positive
SSH	strong positive	positive	positive	strong positive
THALES	strong positive	positive	strong positive	strong positive
VERSASEC	positive	neutral	neutral	strong positive

Table 2: Comparative overview of the ratings for vendors

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

The spider graphs for each of the vendors provide insight into the particular strengths and challenges of the vendor's solution across eight different dimensions:

- Human Identity Support: Support for use cases of managing secrets associated with humans, such as x.509 certificates and FIDO2 tokens.
- IoT/IIoT Identity Support: Support for use cases of managing secrets for IoT and IIoT as well as connected devices. This includes specific support for these identity types and specific protocols as well as supporting the high scalability requirements that are typical for these environments.
- Workload Identity Support: Support for use cases in managing workload identities, also referred to as machine identity management or NHI management. This also includes integration with DevOps environments.
- Secrets Lifecycle Management: The generic capabilities for managing the lifecycles of secrets, across different types of identities.
- PKI Capabilities & Integration: Integrated PKI capabilities, PKI-as-a-Service, and integration to PKIs with CAs (Certificate Authorities).
- Secrets Discovery: Discovery capabilities for secrets of different type, specifically NHI secrets across the various vaults and other places these secrets can reside.
- Governance & Reporting: Governance across the secrets lifecycle, helping organizations to identify specific risks, but also reporting and dashboarding capabilities.
- Quantum Safe Encryption Support: Specific capabilities in discovering secrets and enabling organizations to prepare for QSE or even implement QSE capabilities.

This helps in identifying the specific strengths of vendors and provide insight into which combination of vendor solutions might deliver a comprehensive coverage of all requirements within Enterprise Secrets Management.

Akeyless – Secrets and Machine Identity Platform

Akeyless, founded in 2018 and headquartered in New York, NY, with R&D in Tel Aviv, Israel, has evolved into a leading player in the Enterprise Secrets Management market, delivering a comprehensive and unified Secrets and Machine Identity Platform that sets it apart. With its approach, Akeyless addresses the critical needs for managing secrets and machine identities, minimizing security risks introduced by disparate tools. The Akeyless solution helps bridge the gaps often found in siloed KMS and secrets management solutions, marking Akeyless as a key competitor against established players.

The platform delivers various outstanding capabilities, such as its unique Distributed Fragments Cryptography and an architectural approach using stateless Docker containers, which enhance both security and performance through Zero Knowledge principles. Its support for standards spans across a broad spectrum including OAuth and SPIFFE. The platform features Just-In-Time dynamic secrets, automated migration, and a wide array of connectors to varied environments, ensuring seamless integration and adaptability. Its user interface is particularly user-friendly, offering both UI and CLI/API utilizations, thus making sophisticated secrets management accessible and effective.

What further distinguishes Akeyless is its innovative edge and unique strengths like its Akeyless Gateway Architecture, which fosters enhanced security and the ability to manage the lifecycle and rotation of secrets at scale. However, potential areas for improvement lie in fine-tuning features such as Anomaly Detection and Response, and Secrets Scanning & Discovery—though these are already on the roadmap for future enhancements. Despite these areas for growth, its solution in ephemeral certificates and its detailed logging capabilities showcase a strong platform ready to address nuanced enterprise demands.

The Akeyless' platform is of particular relevance to organizations requiring a robust and flexible approach to secrets management, accommodating cloud, on-premises, and hybrid environments. Its capability to support a wide variety of standards such as above-mentioned SPIFFE and integration options position it well for enterprises across diverse sectors, especially those seeking to streamline their management of API keys, certificates, and more. This makes Akeyless a valuable option for businesses looking to enhance their security posture and address growing threats associated with secrets management comprehensively.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

Table 3: Akeyless's rating

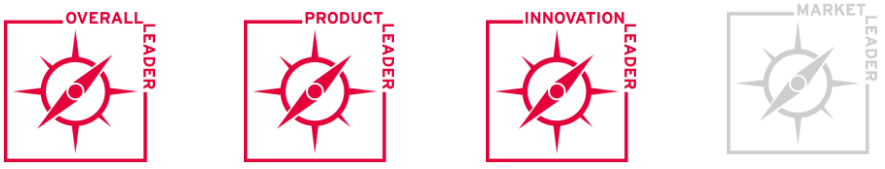
Strengths

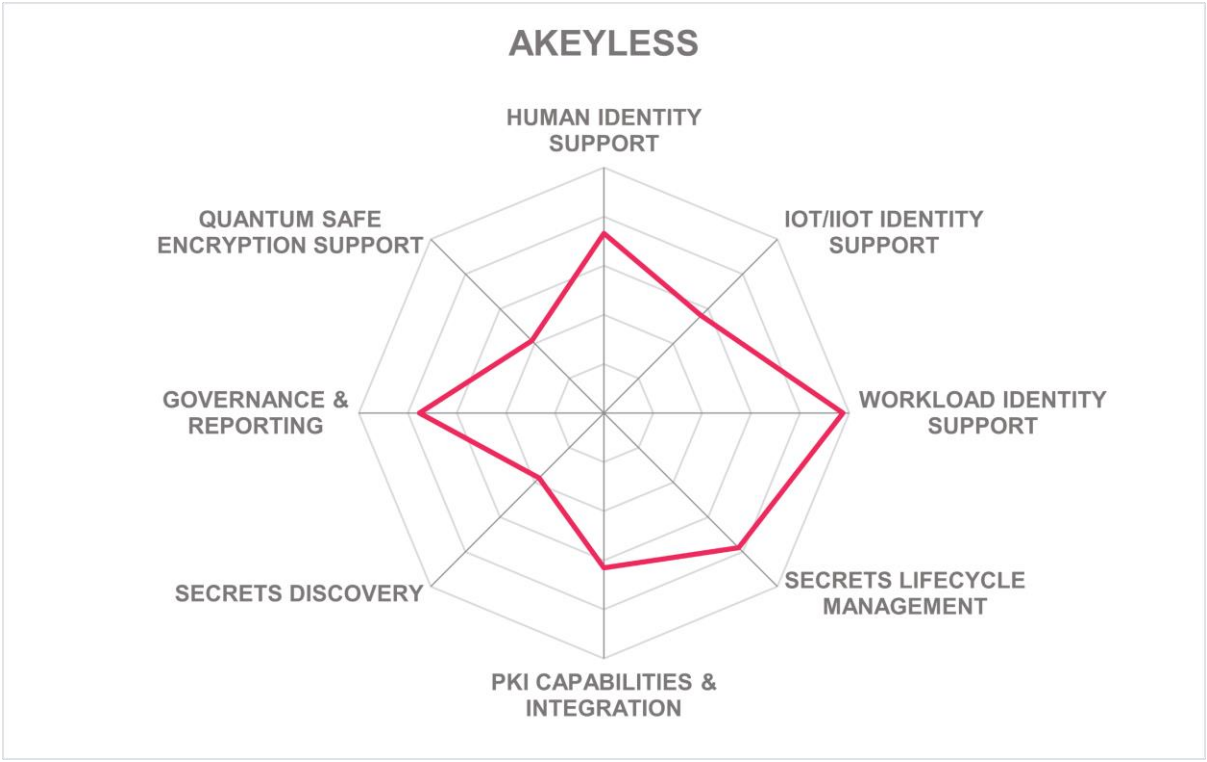
- Comprehensive secrets and machine identity management.
- Unique Distributed Fragments Cryptography.
- Broad and robust integration support.
- Cloud, on-premises, and hybrid deployment models.
- User-friendly UI with CLI/API options.
- Strong focus on Zero Knowledge security principles.
- Automated lifecycle management at scale.
- Wide standards support including OAuth and SPIFFE.

Challenges

- Need for enhanced anomaly detection and response.
- Further implementation of Secrets Scanning & Discovery.
- Improving risk posture management functionalities.
- Only baseline support for QSE, due to limitations in Secrets Scanning & Discovery.

Leader in





AppViewX – AVX ONE

AppViewX, founded 2004 and headquartered in New York, U.S., is a strong contender in the Enterprise Secrets Management market, especially with its capabilities in certificate lifecycle management and PKI automation. Operating with global reach from offices in New York, London, and India, AppViewX supports many active customers across numerous industries. It focuses on non-human identity management, addressing use cases for IoT and IIoT, cloud, and machine identities. Their AVX ONE platform is commonly delivered as SaaS but also provides alternative deployment options across private cloud and on-premises environments.

AppViewX' S AVX ONE platform combines extensive capabilities like closed-loop automation, smart discovery, and policy enforcement and governance, which contribute to their strong certificate lifecycle management solution. This enables end-to-end automation from issuance to renewal across hybrid multi-cloud environments, integrating with various public and private CAs, cloud services, DevOps tools, ITSM, MDM (Mobile Device Management), and SIEM. The platform also offers an innovative crypto resilience scorecard for continuous compliance and an infrastructure-aware approach that supports multiple environments, ensuring full management of crypto-agility and security compliance needs.

What sets AppViewX apart is its intelligent discovery mechanism, capable of identifying a wide range of certificates across various sources. This, alongside its out-of-the-box, extensible automation workflows and flexible deployment, makes it an effective choice for enterprises striving for complete lifecycle management. They provide a powerful workflow builder, which would benefit from some refinements around visualization of components. Nonetheless, its user-friendly interface provides detailed insights into certificate management.

AppViewX is particularly beneficial for large enterprises that need identity and access management across complex environments. Its ability to streamline PKI and certificate operations suits industries with high regulatory requirements, such as finance, healthcare, and telecommunications. Organizations seeking to manage secrets for human identities and, to some extent, non-human identities at scale and improve their cybersecurity posture would find AppViewX's solutions well-aligned with their strategic goals. AppViewX excels in managing digital certificates and establishing trusted identities across workloads and things. It also supports crypto agility.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

Table 4: AppViewX's rating

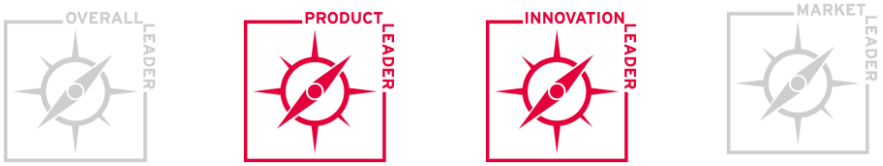
Strengths

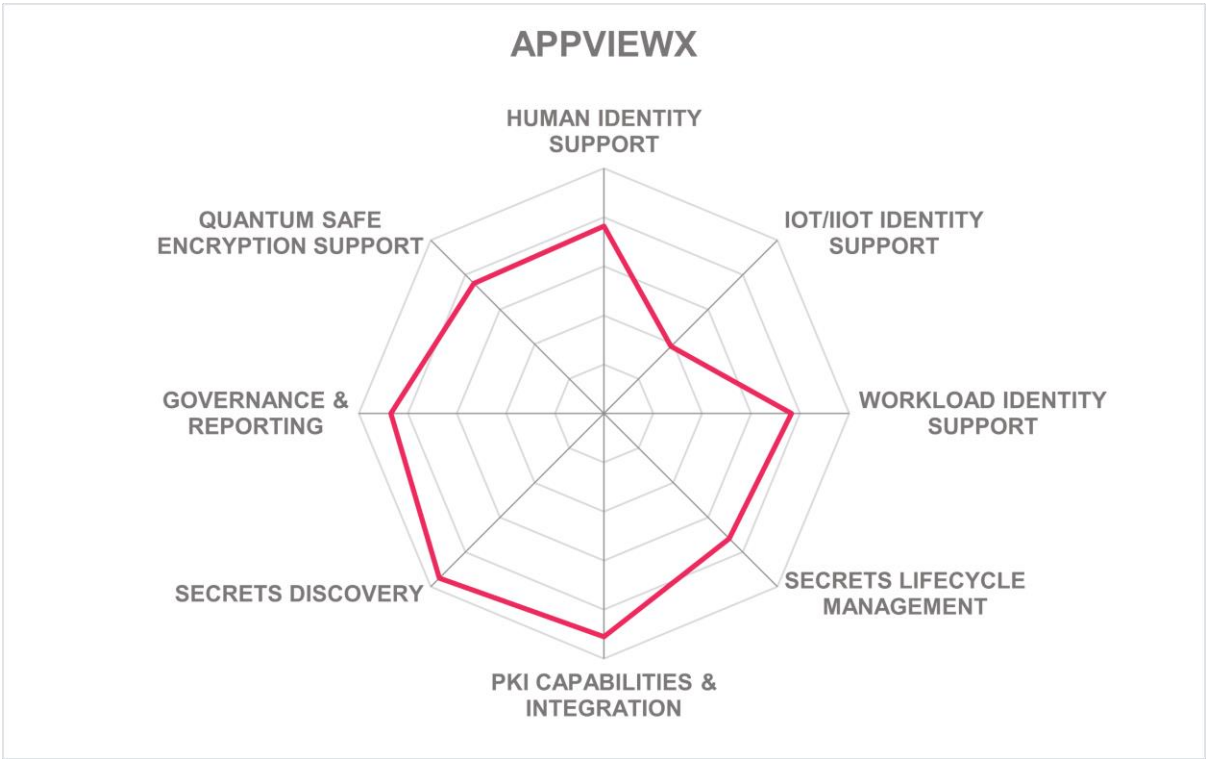
- Comprehensive certificate lifecycle management.
- Effective closed-loop automation.
- Broad and seamless integration capabilities.
- Good non-human identity management.
- Advanced intelligent discovery features.
- Excellent crypto-resilience tracking.
- Flexible deployment options.

Challenges

- Powerful workflow builder, but with potential for further improvement in visualization.
- Complexity in initial setup for large enterprises.
- Lack of capabilities for managing human identities.

Leader in





Astrix – Identity Security Platform

Astrix, founded in 2021 and headquartered in New York, U.S., concentrates on NHI security and management within the scope of Enterprise Secrets Management. Their mission centers on addressing the connectivity blind spots between services, workloads, and third-party environments. Astrix aims to secure NHIs, manage their permissions, and ensure controlled access to sensitive resources, especially when interfacing with potentially untrusted external parties. Delivered entirely as a SaaS solution, Astrix provides a modern UI, rich in information and structured through dashboards, aiding organizations in visualizing and managing NHIs more efficiently.

The Astrix platform encompasses seven fundamental areas: discovery and inventory management, security posture assessment, NHI incident detection and response, secret scanning, vault orchestration, lifecycle management, and workflows and remediation processes. With broad integration capabilities, the platform monitors NHIs across diverse environments and oversees the distribution of secrets among various channels and vaults. This also includes on-premises technologies such as Microsoft Active Directory. It also scans for secrets outside of the secured environments, for instance scanning Slack or Microsoft SharePoint. It also features workflow processes for remediation, which include human-assisted approaches for assessing risks associated with NHIs. Additionally, Astrix includes threat prevention, governance, and compliance enhancement.

The platform helps close the gap in ownership by tracing and mapping identities, while offering deep insights into access permissions as well as proposing least-privilege permissions, and the identity-related attack chain. It differentiates by providing behavioral analytics for NHIs. The connectivity map and identity graph deliver powerful visualizations for relationships between non-human and human identities, permissions, and other entities. However, while Astrix presents an intriguing focus on NHIs, the absence of a graphical workflow builder and some limitations in automated remediation highlight areas for enhancement. Broadening its scope beyond NHIs could further strengthen its position in the Enterprise Secrets Management field.

Astrix is particularly appealing to organizations which utilize cloud-first environments, where NHIs are critical for connecting services, platforms, and external partners. Its solutions are well-suited for industries where in-depth NHI governance and compliance are vital, such as finance, healthcare, and tech sectors. Companies with significant reliance on cloud-based infrastructure and platforms will find Astrix's capabilities valuable, especially given its potential overlap with Cloud Infrastructure Entitlement Management (CIEM) solutions for enhanced access and permission analyses.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 5: Astrix's rating

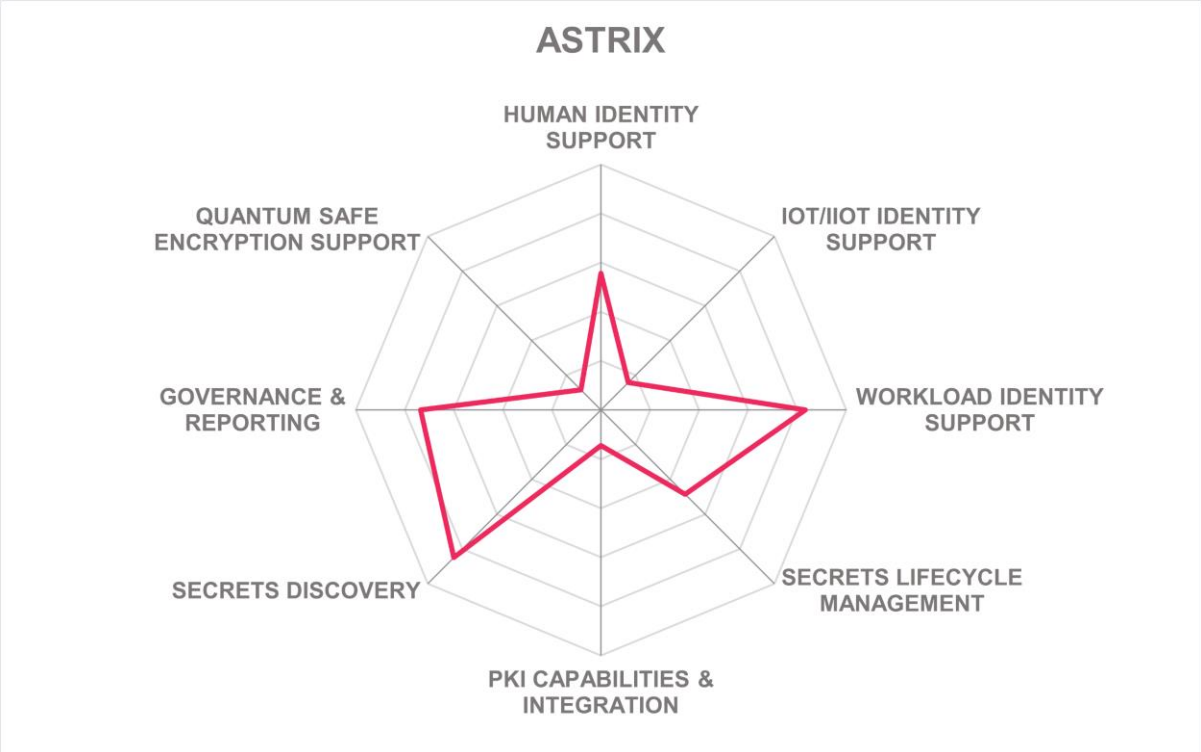
Strengths

- Excellent NHI management features.
- Advanced integration across platforms.
- Human-assisted remediation workflows.
- Detailed insights into entitlement access.
- User-friendly dashboards and UI.
- Embedded SOAR capabilities.

Challenges

- Narrowly focused on NHI security and management, thus limited support for broader Enterprise Secrets Management.
- Lack of graphical workflow builder.
- Will benefit from extending automated remediation capabilities.

Leader in



AWS – Secrets Manager, Certificate Manager & IoT Defender

Amazon Web Services (AWS), founded back in 2002 and headquartered in Seattle, U.S., is also, amongst its broad portfolio of cloud services, a significant player in the Enterprise Secrets Management market, there focusing on providing solutions for certificate lifecycle management, workload identity management, and IoT identity management. Central to their solution is the AWS Secrets Manager. Alongside this, AWS employs a broader strategy with services like the AWS Certificate Manager (ACM) for automating SSL/TLS certificate management and the AWS IoT Device Defender for IoT security. The integration across AWS services underscores their commitment to cloud-centric environments.

AWS Secrets Manager focuses on automating secret rotation, secure secret storage, and fine-grained access controls. It offers integration with AWS Key Management Service (KMS) for encryption and AWS Identity and Access Management (IAM) for access control management to the secrets. It provides FIPS 140-3 Level 3 backed encryption. Its AWS-native integration facilitates straightforward deployment within AWS environments, providing APIs and SDKs for automation in DevOps workflows. Additionally, AWS supports hybrid environments with capabilities like IAM Roles Anywhere, enabling non-AWS workloads to interact with AWS securely via x.509 certificates.

AWS differentiates itself by focusing on its expansive ecosystem, integrating with other AWS services, and enhancing the ease of use within its cloud infrastructure. However, this focus on AWS-centric use cases can limit its applicability across diverse multi-cloud or on-premises environments. While AWS provides good foundational capabilities, areas such as more extensive automated remediation and broader non-AWS integrations could use enhancement. Their market leadership is attributable to their overall dominance in the IaaS and PaaS markets.

AWS's Enterprise Secrets Management solutions primarily benefit enterprises entrenched in the AWS ecosystem. It appeals to firms seeking to leverage AWS’s expansive portfolio for streamlined secrets management, especially those aiming for integrated cloud solutions involving AWS managed databases, IoT identity, and workload management. AWS's services are crucial for sectors where scalability and compliance in highly regulated industries such as financial services and the public sector as well as integrations are paramount, although customers may need to evaluate additional solutions for comprehensive multi-cloud strategies.

Security	Strong Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 6: AWS’s rating

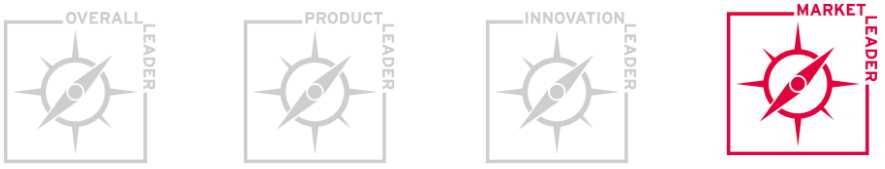
Strengths

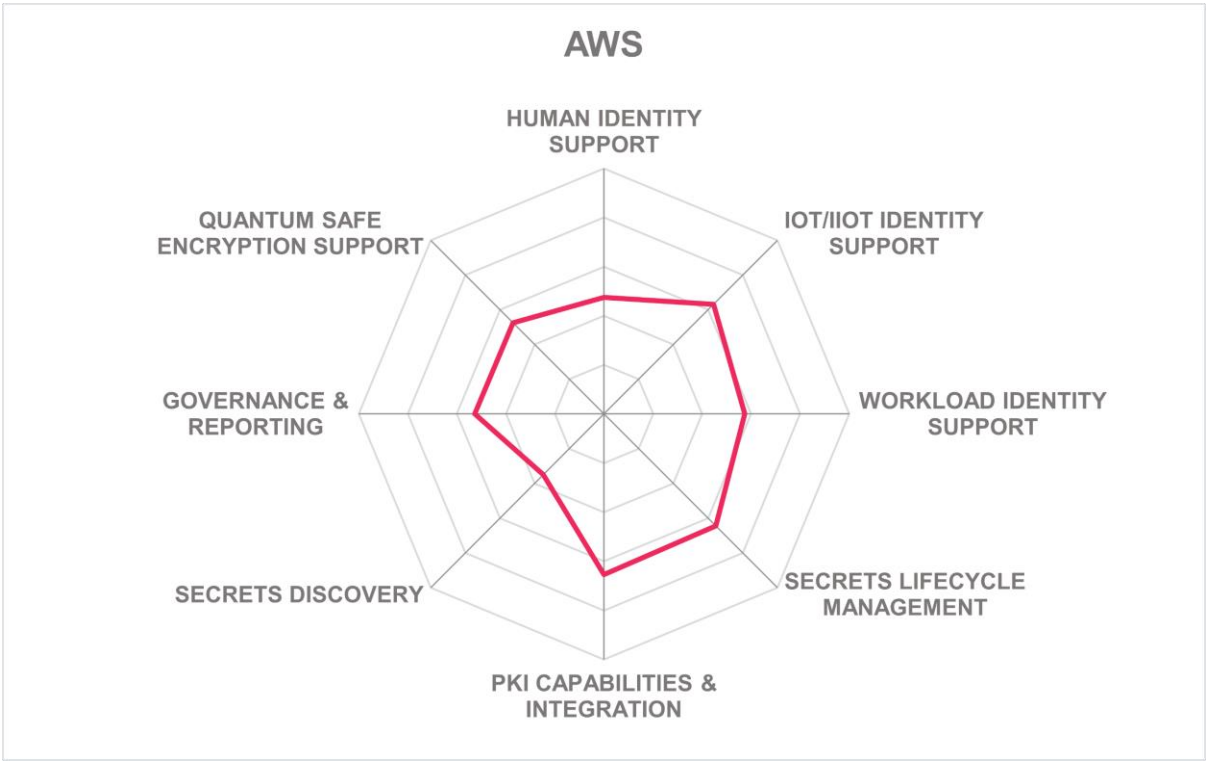
- Seamless integration with AWS services.
- Automated secret rotation and management.
- Secure storage with fine-grained access control.
- Extensive support for cryptographic operations.
- Some level of IoT identity management features.

Challenges

- Limited applicability in multi-cloud environments.
- Focused primarily on AWS-centric ecosystems, enhanced non-AWS integrations are desired.
- Good baseline capabilities for many use cases, but no leading-edge support for Enterprise Secrets Management.
- Needs broader automated remediation options.

Leader in





Axiad – Conductor

Axiad, founded 2010 and headquartered in Santa Clara, U.S., offers their PKI as a Service, specializing in credential management and multifactor authentication (MFA) to provide identity security solutions. The company has customers across a range of industry sectors including healthcare, technology, manufacturing, and oil and gas, managing hardware tokens and devices for its clients. With the flexibility to operate either as a fully managed service or in coordination with customer-maintained workflows, Axiad caters to diverse enterprise needs. Axiad places strong emphasis on crypto agility, adapting to evolving security demands.

Axiad's platform enables simplified credential management through a modern, unified user interface, minimizing dependency on command-line interfaces. It allows integration with various Certificate Authorities (CAs) and has broad standards support including ACME, CSP2, EST, OIDC, or SCEP, to name just a few, which assists customers in consolidating their PKI environments. With numerous connectors, including integration to Active Directory, Omnissa Workspace One, Intune, and many other types of applications, Axiad facilitates smooth certificate rollouts. Their service structure enables customers to test changes in dedicated environments before wide deployment.

Axiad stands out with its flexibility in deployment and integration capabilities for various CA/PKI environments. Along with CA management, Axiad Conductor also supports large-scale management of FIDO2 passkeys. However, its limitations include the absence of key management features like Bring Your Own Key (BYOK) support, focusing instead solely on certificate delivery. Future improvements could involve expanding to accommodate broader key management solutions, enhancing its role in the security landscape.

Organizations looking for a reliable PKI management solution that supports consolidation of CAs and hardware authenticator integration will find Axiad especially relevant. Axiad complements many of the other solutions in the Enterprise Secrets Management market with its specialization. Its strength in managing secrets at scale aligns with the needs of sectors such as healthcare and manufacturing. Enterprises seeking to refine their crypto agility and credential management strategies would benefit from considering Axiad's capabilities.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 7: Axiad’s rating

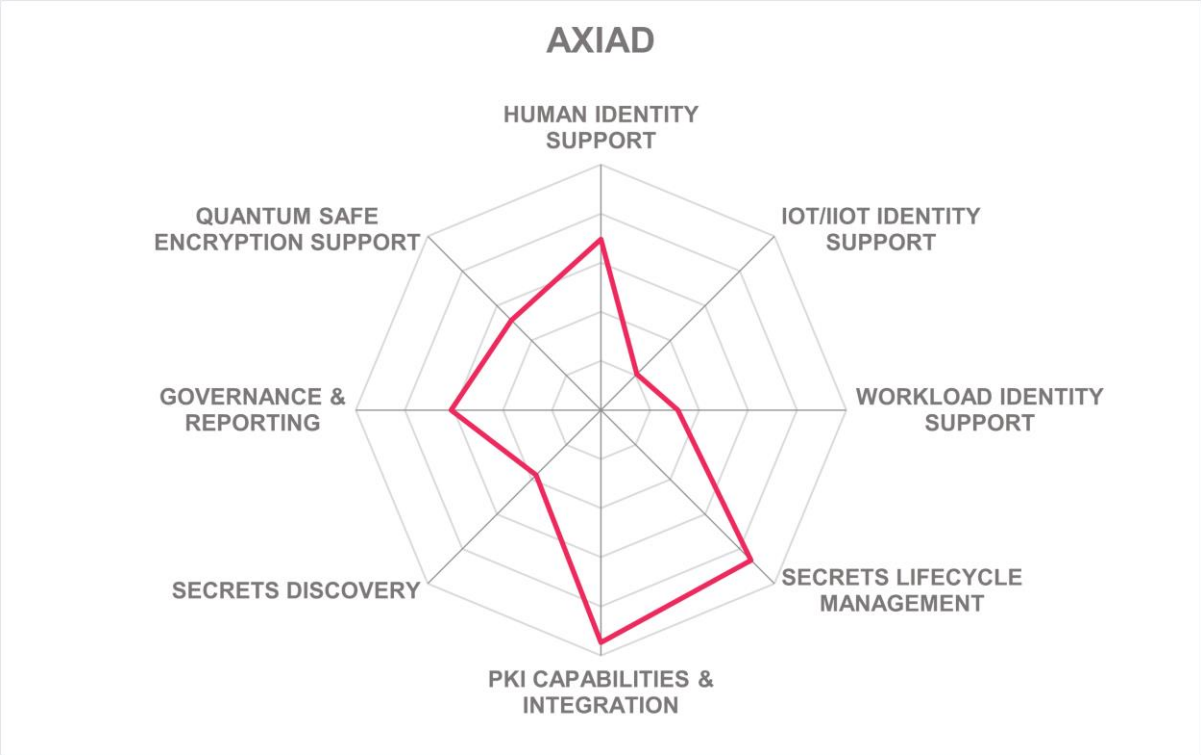
Strengths

- Robust PKI as a Service.
- Comprehensive credential management, particularly for X.509 certificates.
- Flexible deployment options, including SaaS and on-premises.

- Strong CA integration.
- Emphasis on crypto agility.
- User-friendly modern interface.
- Support for large-scale FIDO2 key management

Challenges

- Lack of key management solutions.
- Needs broader BYOK support.
- Lacks IoT/IIoT and workload identity support.
- Could use more governance and reporting features.
- Needs improvement on QSE.



BeyondTrust – BeyondTrust Platform

BeyondTrust, headquartered in Atlanta, U.S., a leading identity security provider, is a key player in PAM, but also increasingly in Enterprise Secrets Management. They have a global reach spanning thousands of customers in over 100 countries. Since its establishment in 2003, BeyondTrust has adeptly combined elements of privileged access and identity management into a unified platform. This platform not only provides insights into both human and machine identities but also offers a seamless experience through a centralized interface and extensive integrations, enhancing visibility, analytics, and compliance across many different IT environments.

The core of BeyondTrust's Secrets Management platform manages secrets and passwords optimized for both IT and DevOps usage. The platform includes integrations with essential DevOps tools like Terraform, Azure DevOps, Ansible, Kubernetes, and GitHub Actions, to enable management and security of API keys, tokens, and other sensitive information. Advanced features such as file encryption, secrets rotation, and automation enhance operational efficiency, supported by access via GUI and comprehensive API capabilities.

Among BeyondTrust's standout features is its focus on "paths to privilege," which illustrates the relationships between identities and the resulting permissions. This visualization aids in understanding the distribution of privileges and potential vulnerabilities. Despite its strengths, areas for optimization include further refinement of the automation processes and the user interface to maintain clarity as the platform's capabilities expand. An ambitious roadmap focuses on ongoing developments in CI/CD support, cloud tokens, and API management, which promises to fortify its solution. On the other hand, support for IoT/IIoT secrets, CA integration, and QSE is low.

BeyondTrust's solutions are particularly suited for enterprises demanding rigorous control over privileged and non-privileged accounts across complex environments. Organizations from sectors such as healthcare, finance, and higher education, which require streamlined identity management and security compliance, will find value in the integrated capabilities of BeyondTrust. Given its strategic enhancements and comprehensive roadmap, BeyondTrust remains a strong choice for enterprises seeking advanced identity management solutions.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

Table 8: BeyondTrust’s rating

Strengths

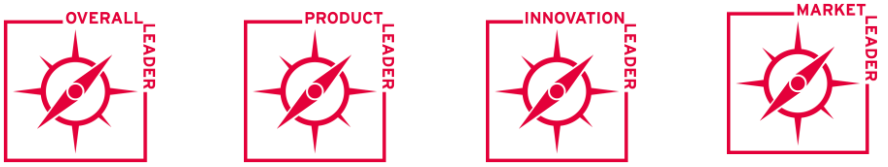
- Emerging platform for integrating PAM and Enterprise Secrets Management.
- Integration with major DevOps tools.
- Robust secrets management capabilities for humans and, increasingly, NHI.

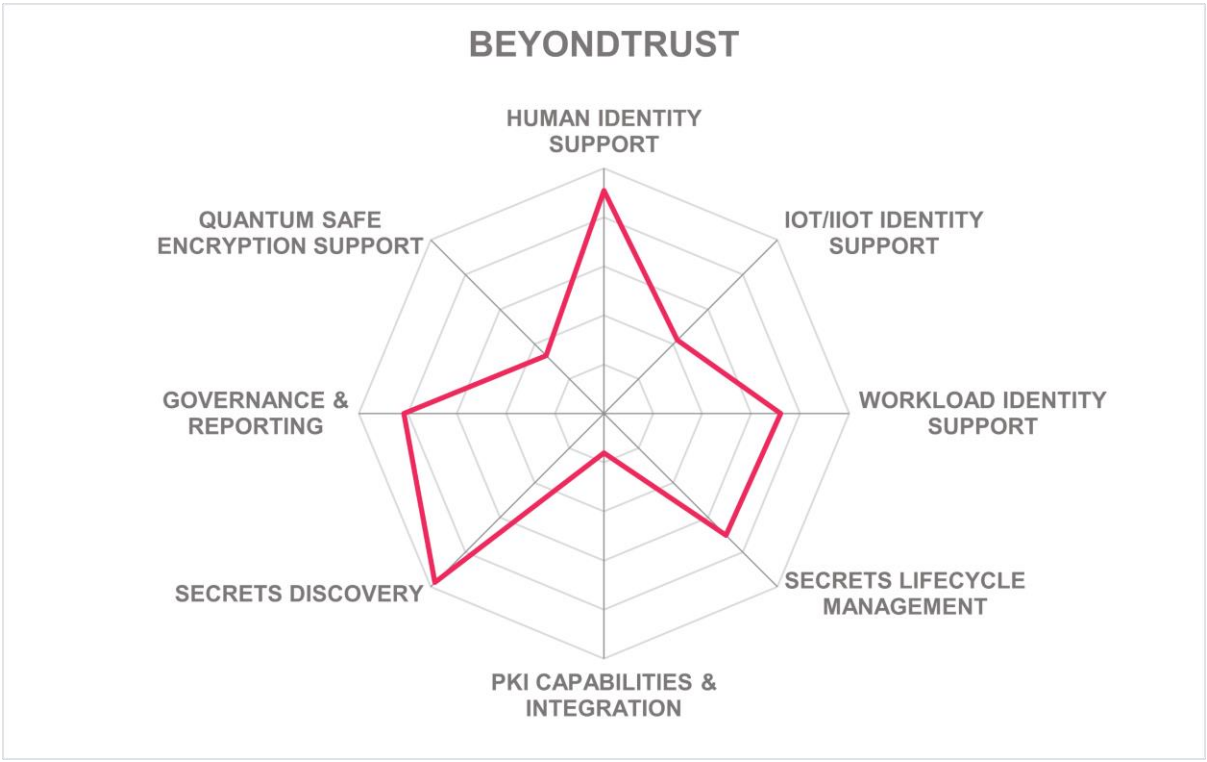
- Focus on paths to privilege visualization, mapping identities and entitlements.
- Extensive global reach and customer base.
- Strong support for compliance and governance with integrated dashboards and analytics.
- Full-featured API and GUI for management.

Challenges

- Need for further improvement of automation in secrets handling and remediation.
- UI complexity as features expand.
- Integration of features across capability areas such as PAM and NHI demonstrating strong process, but further integration required.
- Gaps in PKI and CA integration and limited support for QSE.
- Not focused on supporting IoT/IIoT use cases.

Leader in





Cryptomathic – CrystalKey 360

Cryptomathic, founded back in 1986 and headquartered in Aarhus, Denmark, a specialized vendor in the Enterprise Secrets Management domain, focuses on cryptographic solutions tailored to support key management, qualified electronic signatures for document signing and sealing, secure payments, secure mobile applications, securing data at rest, and initializing IoT devices. Having a rich history in cryptography, Cryptomathic addresses the complexities of managing encryption keys and their provision, distribution, renewal, and retirement efficiently and securely. Their solutions cater primarily to industries with high compliance and security demands such as finance, telecommunications, and manufacturing. The CrystalKey 360 platform offers a centralized approach to handling symmetric and asymmetric keys as well as certificates at large scales in geographically dispersed environments. The solution is commonly deployed on-premises, but also supports other deployment models including cloud deployments and operations in confidential computing environments.

The core capabilities of Cryptomathic's CrystalKey 360 platform include comprehensive key lifecycle management and centralized control over cryptographic assets. The platform supports cryptographic agility, ensuring adaptability as encryption and signing standards evolve, particularly with post-quantum cryptography readiness. CrystalKey 360 abstracts the definition from cryptographic resources from the consuming services and thus can manage the keys, their length, formats, algorithms and access rules and exchange these when needed. CrystalKey 360 also offers good integration with third-party tools and CA infrastructures and ensures compliance with global regulations such as DORA (Digital Operations Resilience Act) and NIS2, providing a unified interface for monitoring, governance, and automation of key management across complex IT infrastructures.

Cryptomathic differentiates itself with its experience in providing the foundation for crypto agility and its capability to deliver a single pane of glass experience for managing cryptographic security decisions such as shifting to new encryption standards. This approach allows organizations to rotate keys and swap algorithms efficiently, reducing the need for complex HSM infrastructures. While improving the user interface and adding automation capabilities by exposing all capabilities via APIs, the main focus remains on managing and optimizing cryptographic assets. CrystalKey 360 provides integration to CI/CD workflows as well as to other solutions such as CyberArk.

The Cryptomathic platform is well-suited for enterprises requiring rigorous cryptographic security measures, especially those in sectors demanding the highest security with QSE and looking for optimization of their Cryptographic Bill of Materials (CBOM) or having highly complex secrets deployment procedures. They do not focus on broader Enterprise Secrets Management use cases but deliver a specialized platform for key management and delivery that can be integrated with other identity and security solutions. Its solutions are particularly valuable for organizations needing a secure and adaptable environment for key lifecycle management and high-throughput cryptographic operations.

Security	Neutral
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Neutral

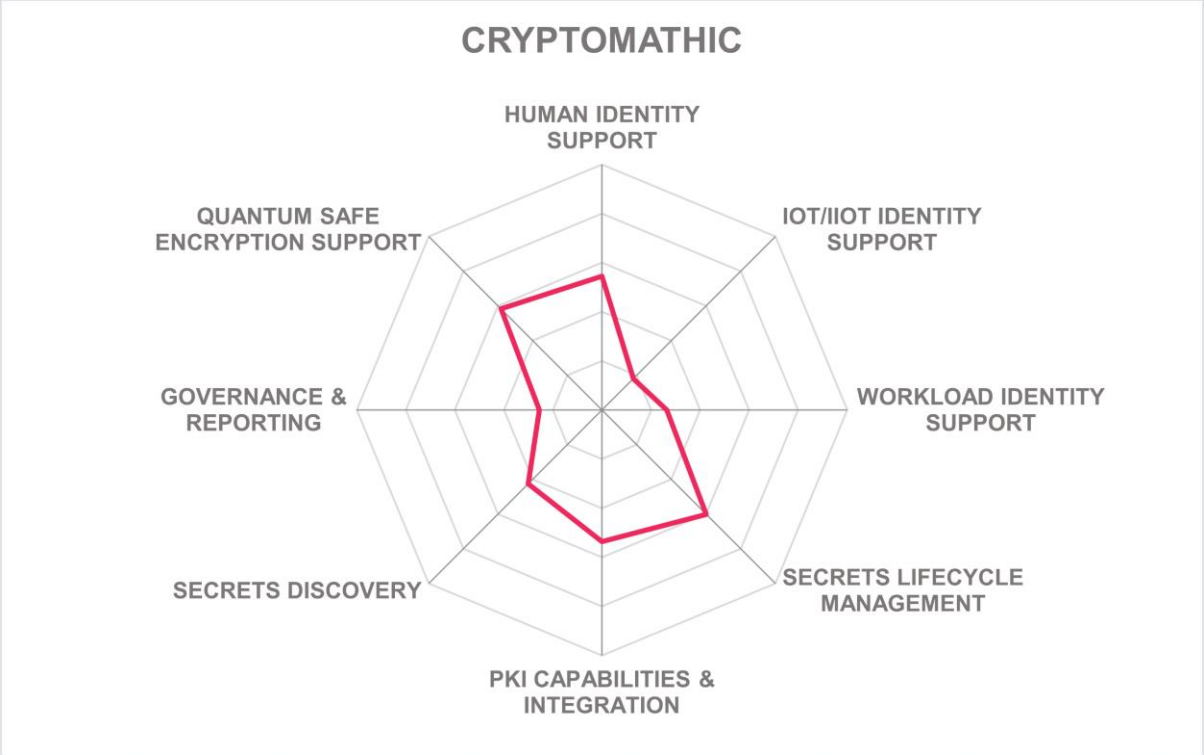
Table 9: Cryptomathic's rating

Strengths

- Comprehensive cryptographic key management, particularly around x.509.
- Post-quantum cryptography readiness and ability to adapt to other evolving cryptographic standards.
- Centralized control for enhanced governance.
- Robust compliance support for all cryptography related regulatory compliance requirements.
- Extensive third-party integration.
- Comprehensive exposure of capabilities via APIs.

Challenges

- Focused on technical users.
- Not a fullend-to-end solution for NHI and IoT/IIoT.
- Increased integration with DevOps workflows would enhance supported use cases.
- Focused solution with the ability for complementing other solutions within the broader Enterprise Secrets Management market.


CRYPTOMATHIC
HUMAN IDENTITY SUPPORT
IOT/IIOT IDENTITY SUPPORT
WORKLOAD IDENTITY SUPPORT
SECRETS LIFECYCLE MANAGEMENT
PKI CAPABILITIES & INTEGRATION
SECRETS DISCOVERY
GOVERNANCE & REPORTING
QUANTUM SAFE ENCRYPTION SUPPORT

CyberArk – Identity Security Platform

CyberArk, founded back in 1999 and headquartered in Newton, U.S., leads the Enterprise Secrets Management market, consistently holding top positions in product, innovation, and overall leadership. With a robust portfolio spanning machine identity security, secrets management, and PKI & CMS capabilities, CyberArk integrates its solutions cohesively within the CyberArk Identity Security Platform. This platform unifies services and security controls, enhancing identity management across human, machine, workload, and non-human identities, strengthened by the strategic acquisition of Venafi, aimed at expanding machine identity security capabilities.

CyberArk's Identity Security Platform includes the CyberArk Secrets Hub and Conjur Cloud, offering centralized secrets management with integrations into cloud-native and multi-cloud environments. Its dynamic secrets management supports the full range of secrets types, and the platform enhances security with robust audit trails and governance capabilities. Developers benefit from an API-rich environment with access to tools like Ansible and Terraform, making CyberArk well-suited for DevOps applications. Additionally, its newly integrated "zero touch PKI" and comprehensive machine identity controls provide utmost flexibility and security.

What sets CyberArk apart is its approach to identity security, closing gaps between machine and human identity management. Its strengths lie in its broad integrations, centralized management, and automated governance. The Venafi Control Plane extends capabilities further, though there is room for improvement in full UI integration. CyberArk continues to enhance its solutions, focusing on extending its automation, discovery, audit and governance capabilities for diverse types of secrets to maintain its leadership position. The platform's deep discovery and risk management capabilities, presenting risks via dashboards, form a critical part of its strategy, providing a holistic view of identity environments.

CyberArk is particularly beneficial for enterprises requiring extensive identity governance and secrets management across diverse ecosystems. Large organizations in sectors like finance, healthcare, and technology may benefit from their integrated management and security automation. Entities looking to streamline machine identity management, from IoT to cloud workloads, will find CyberArk's solutions align with their operational needs, supporting enhanced regulatory compliance and security postures across global operations.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 10: CyberArk's rating

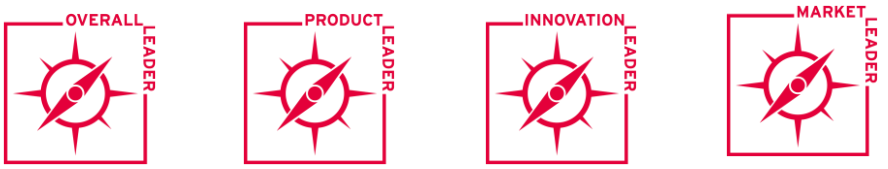
Strengths

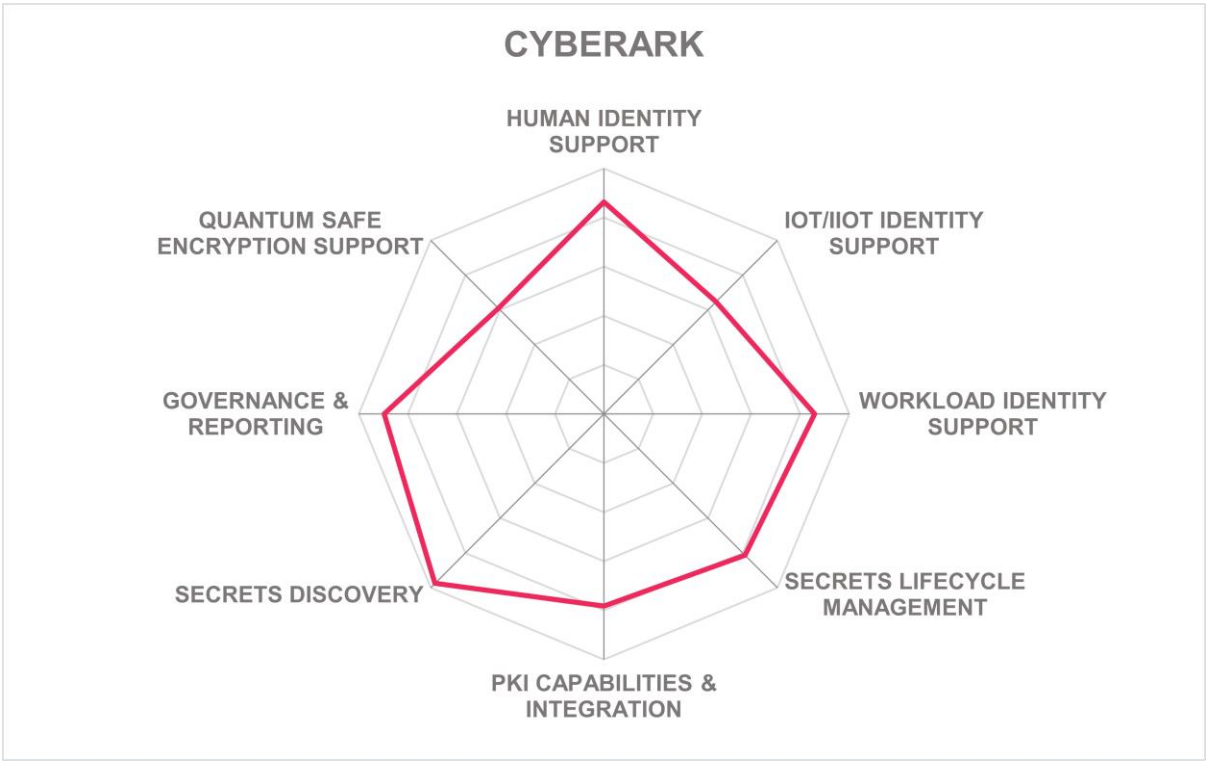
- Comprehensive identity and security platform.
- Robust Secrets Hub and Conjur Cloud integration.
- Industry-leading machine identity capabilities.
- Extensive API support for automation.
- Centralized management with strong governance.
- Innovative "zero touch PKI" approach.
- Deep discovery and insights features.
- Broad global presence and customer base.
- Strategic acquisitions enhance their portfolio.

Challenges

- Need for improvement in UI integration
- Complexity in managing multifaceted environments.
- Continuous enhancement required for evolving threats. IoT/IIoT capabilities deserve further enhancement.

Leader in





Delinea – Secret Server & DevOps Secrets Vault

Delinea, founded in 2004 and headquartered in San Francisco, U.S., has emerged from a PAM vendor towards being a contender in the broader Enterprise Secrets Management landscape, leveraging a unified cloud-native platform to address complex identity and data authorization challenges. Delinea has made considerable progress in integrating its acquisitions and enhancing their platform capabilities. The company in its recent investments focuses heavily on Non-Human Identity (NHI) management, tackling challenges like visibility, lifecycle governance, and security misconfigurations, aiming to provide comprehensive credential management across diverse environments.

Delinea's platform offers a comprehensive suite of features, including Privilege Control for Cloud entitlements and robust distributed vaulting capabilities plus excellent secrets discovery. The platform provides strong capabilities in discovering and mapping NHIs and other identities, offering graphical management tools to streamline operations. By focusing on minimizing credential lifetime and employing adaptive governance tools, Delinea empowers developers to adopt federation and eliminates credentials embedded in code. The platform's modern UI complements its extensive integrations and lifecycle management features, providing an intuitive admin user experience.

What differentiates Delinea is its strategic focus on cross use case and cross identity type credential management, particularly investing in NHI support, which it addresses through innovations such as just-in-time access and avoiding long-lived credentials. The platform’s ability to automate credential rotation and provide a consolidated view of distributed vaults highlights its strong capabilities. However, further development in full integration of all acquired technologies in the platform could strengthen its solution. The roadmap with its focus on further broadening depth and breadth of capabilities indicates an ongoing commitment to innovations supporting DevOps and cloud security.

Delinea's solutions are particularly beneficial to enterprises with complex, multi-cloud environments where credential sprawl is a challenge. Industries ranging from financial services to healthcare and technology would benefit from Delinea’s strong governance and security capabilities. With its focus on shortening credential lifetimes and improving governance for non-human identities, Delinea aligns well with enterprises seeking to improve security while reducing operational friction.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 11: Delinea’s rating

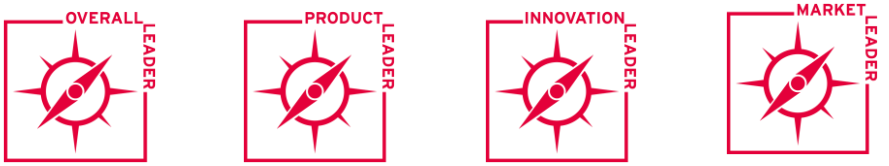
Strengths

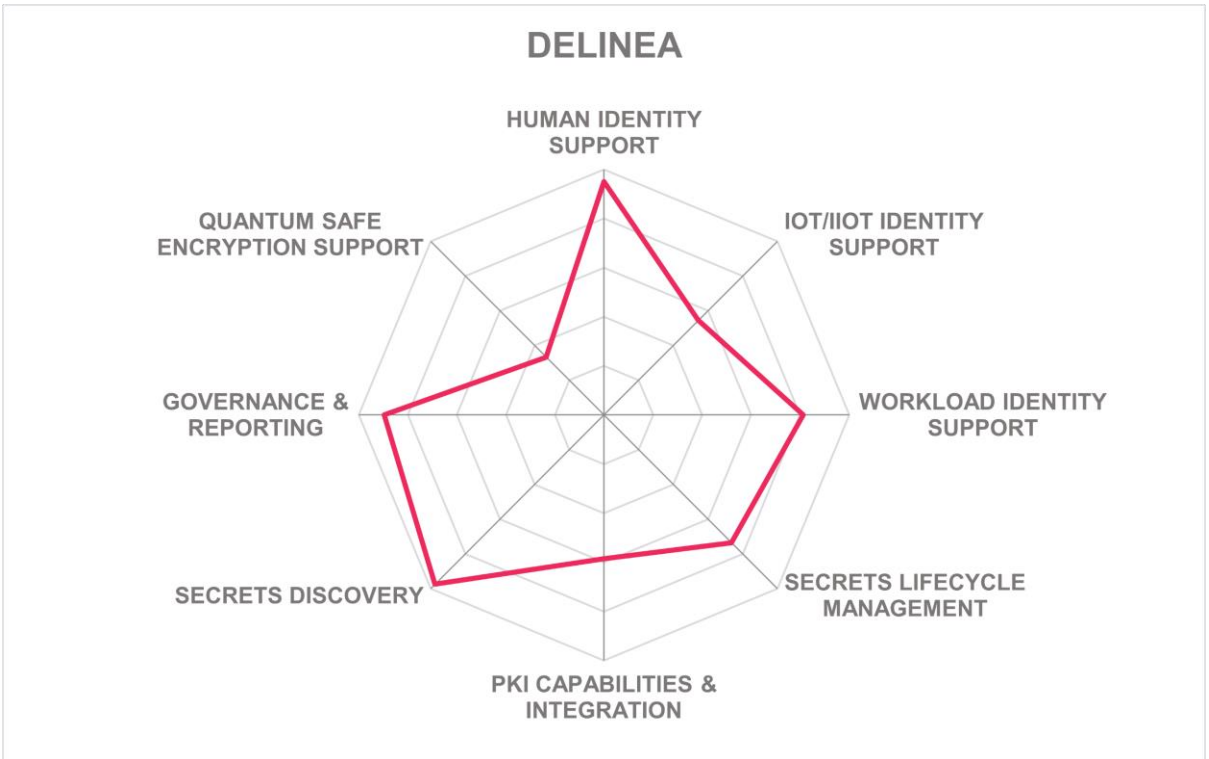
- Good NHI management capabilities.
- Strong secrets discovery capabilities.
- Extensive distributed vaulting features.
- Robust lifecycle management tools.
- Modern, integrated cloud-based platform.
- Strategic alignment with industry needs.
- Support for short-lived secrets.
- Effective automation and governance features.

Challenges

- Though CIEM and ITDR functionality has been fully integrated, further integration of the acquired IGA technology is needed.
- Growing NHI support, but further room for improvement.
- Continued investment in user experience, but still needing porting some of the solution to the new platform.
- Some level of IoT/IIoT secrets management, but needs to be rounded out as a holistic solution.

Leader in





Entro – NHI Management & Secrets Security

Entro Security entered the Enterprise Secrets Management space in 2022 and headquartered in Boston, U.S., focusing on non-human identities (NHIs) such as service accounts and application tokens. The founder's background as a CISO impacted their approach to managing secrets, focusing on an efficient, secure, and developer-centric workflow. Entro Security aims to address the challenges posed by the lack of lifecycle management and oversight of NHIs, providing solutions to prevent long lifespans and unauthorized access, which are common issues within distributed identity environments.

The platform's key capabilities include discovery and inventory of secrets, classification, NHI detection and response, risk-based prioritization, automated policy enforcement including secrets rotation and revocation, and posture management. It offers static analysis and risk assessment, coupled with non-human identity detection and response. Entro Security integrates with various APIs to analyze log activities and automate remediation processes. Users benefit from a dynamic UI that presents real-time analytical insights and facilitates semi-automated or manual handling of identified risks through flows or ticketing systems like ServiceNow, JIRA, and others.

Entro Security is distinct in its focused understanding of metadata surrounding secrets, particularly those authorized in developer environments. It actively secures NHIs through risk-based governance, threat detection, and security automation. Based on these powerful capabilities, further expansion of its automated remediation capabilities and enhanced workflows could strengthen its market position. Addressing these areas could further solidify Entro's position as a proactive tool for managing digital risks associated with non-human identities and secrets proliferation.

Organizations with substantial DevOps operations and the NHI risk occurring in these environments, or those heavily reliant on cloud-native applications will find Entro Security's platform especially beneficial. Its strengths lie in providing clear visibility and control over NHIs, making it an ideal choice for companies in tech, e-commerce, and cloud services. Its detailed risk assessment and mitigation capabilities are well-suited for sectors where security and efficient management of digital identities are paramount.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 12: Entro's rating

Strengths

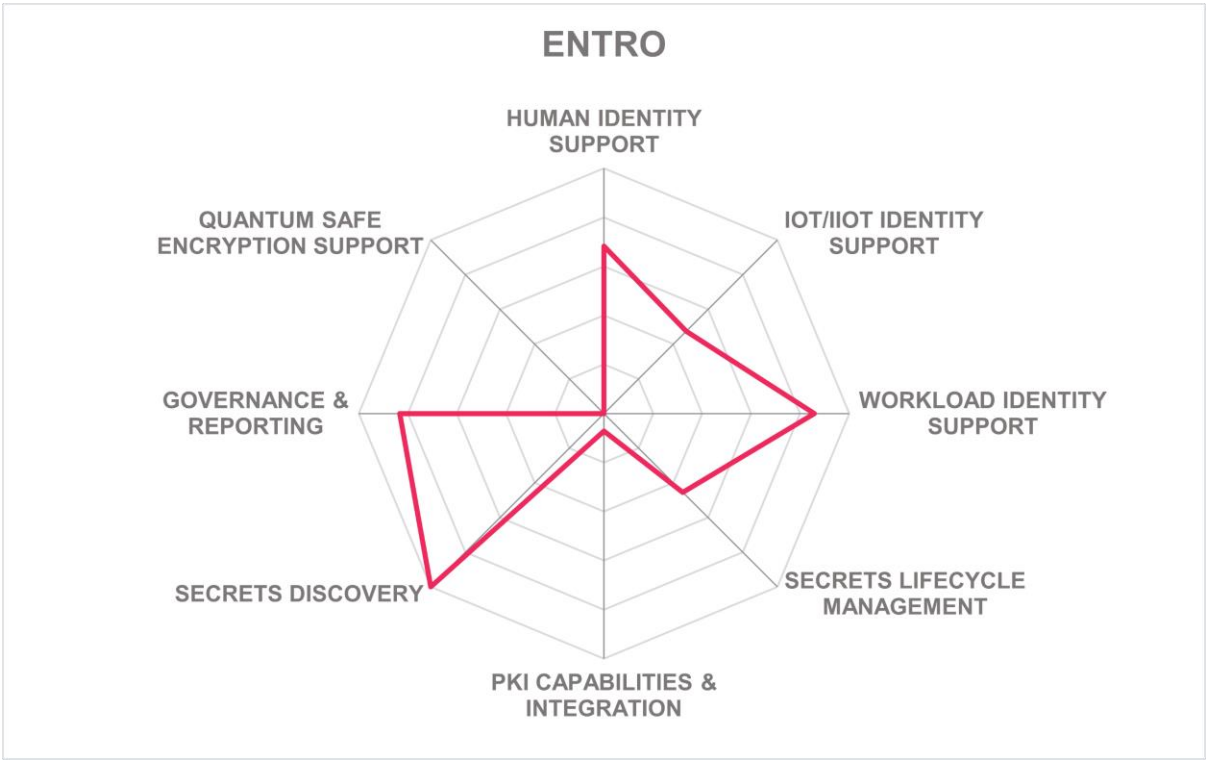
- Strong focus on non-human identities.
- Good discovery and inventory capabilities.
- Advanced risk assessment tools.

- Support for semi-automated and automated remediation workflows.
- Extensive API integration for insights.
- Dynamic user interface.
- Strong behavior analytics for secrets and NHIs
- Semi-automated remediation flows.

Challenges

- Small but growing vendor with a good partner ecosystem.
- Further enhancement of capabilities for visually defining workflows is recommended.
- Leading-edge support for workload identity support (NHI), but not for other identity types within Enterprise Secrets Management.
- Limited support for QSE and lack of PKI integration.

Leader in



Entrust – Key Control, IDaaS, CLM & PKIaaS

Entrust, founded back in 1969, and headquartered in Shakopee, U.S., counts amongst the established vendors in Enterprise Secrets Management market, acknowledged for its extensive solutions that span identity verification, machine identity, and key management. The company's broad portfolio serves not only traditional key management needs but also encompasses modern solutions like zero-trust encryption, certificate lifecycle management, and compliance management. Entrust combines NHI support with a robust infrastructure that can manage numerous vaults and integrate seamlessly across various environments. Their strong solutions position them as a market leader, addressing many different industry requirements.

Entrust's platform comes with a wide range of features that enhance scalability and security. It builds on a distributed vault infrastructure, ensuring high scalability and availability. The platform supports a wide range of integrations, with Entrust having long experience in supporting large enterprise use cases, offering REST API and CLI access for flexibility. It also includes advanced security controls that differentiate between local and central administrative rights, vital for organizations with significant local administration. In addition, Entrust's compliance manager adds risk management by maintaining logs that can be securely signed, ensuring governance and transparency across operations.

Entrust distinguishes itself with its broad portfolio of security solutions, covering a wide range of use cases, and its proven capability to manage complex environments through centralized and decentralized controls, including managing keys and supporting QSE requirements. While the scalability and range of integrations stand out, the user interface has room for improvement and could benefit from modernization for enhanced accessibility. Entrust is working on expanding its platform to offer more complete management solutions, aiming to consolidate encryption management further.

The Entrust platform is advantageous for organizations that need a sophisticated and scalable approach to key and secrets management, especially those operating across multiple administrative levels. Sectors such as government, finance, and healthcare that require strong security and compliance, may find value in Entrust’s solutions.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

Table 13: Entrust’s rating

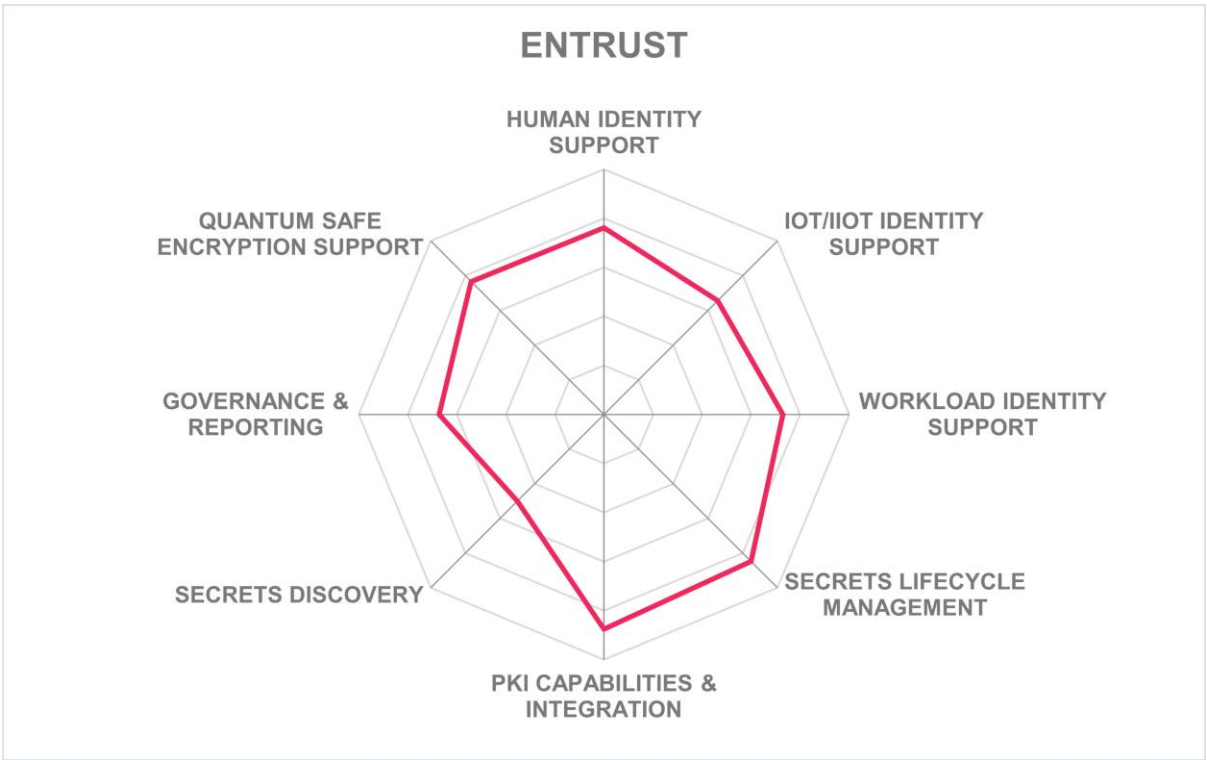
Strengths

- Extensive security and compliance capabilities.
- Wide range of integrations and API support.
- Distributed vault infrastructure supporting high scalability and failover.
- End-to-end encryption and management solutions.
- Scalable architecture supports growth and complexity.
- Strong market reach and customer base.
- Differentiation of admin rights enhances security.
- Focus on compliance and risk management.
- Strong capabilities for QSE.

Challenges

- Would benefit from more integrated NHI management capabilities.
- User interface requires modernization.
- Complex presentation of solutions available.
- Ongoing need for feature integration and enhancement.

Leader in



GitGuardian – GitGuardian Platform

GitGuardian, founded in 2017 and headquartered in Paris, France, positions itself as an enterprise-ready provider in the Enterprise Secrets Management sector, focusing on secrets discovery, security, and management for heterogeneous environments. Originating from a strong developer community base, GitGuardian excels in creating visibility around secrets sprawl, which can be a massive challenge driven by the proliferation of machine identities. Its solution includes secrets detection, public monitoring for leaked credentials, and honeytoken solutions to provide proactive breach alerts. These tools facilitate better secrets oversight alongside integration with major secrets managers.

GitGuardian supports over 450 types of secrets across varied environments such as Git, CI/CD platforms, collaboration tools, and container registries. With strong detection capabilities, the platform implements sophisticated alerting mechanisms and offers remediation pathways that leverage developer collaboration. Its system of severity scoring and automated playbooks makes incident management efficient and minimizes false positives, which aids in swift secret revocation and lifecycle management. The solution integrates with popular secret managers such as HashiCorp Vault to close the loop between secrets detection and management.

What distinguishes GitGuardian is its leading-edge secrets observability and proactive security measures, including its advanced detection and prevention capabilities. However, while it surpasses in discovery and observability, GitGuardian's functionality in comprehensive secrets lifecycle management is still developing, which presents integration opportunities. Enhancing its feature set to fully encompass lifecycle governance could strengthen its role in the broader secrets management space. The company’s roadmap promises enhancements in policy-based management and automated incident resolutions, indicating a drive towards broadening its solutions.

GitGuardian is particularly suited for organizations needing extensive secrets detection and remediation, especially those experiencing rapid growth in non-human identities. Its integration with existing infrastructures makes it a good choice for modern enterprises aiming to fortify their security postures. Companies that focus on development environments, collaboration tools, and containerized applications would benefit significantly from GitGuardian’s capabilities in detecting and addressing secrets sprawl effectively. GitGuardian is well-positioned for complementing other solutions in the Enterprise Secrets Management market.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

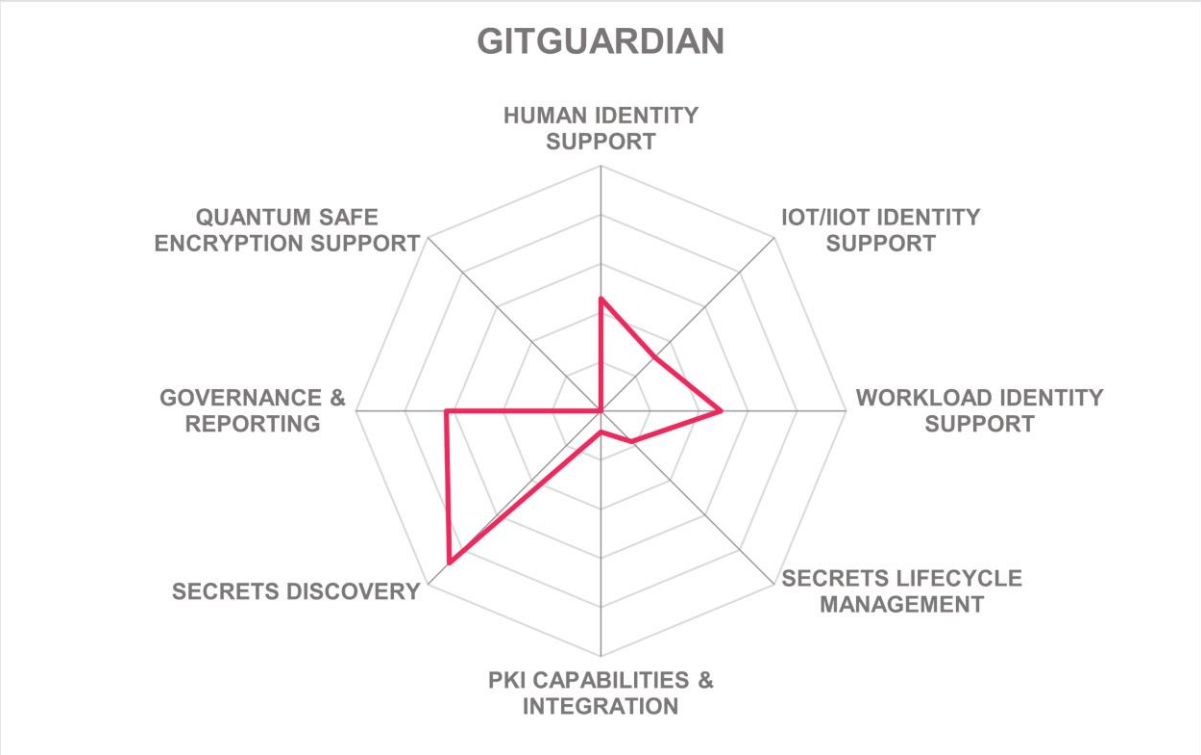
Table 14: GitGuardian’s rating

Strengths

- Advanced secrets detection capabilities.
- Extensive integration with major platforms.
- Robust alerting and remediation frameworks.
- Effective honeytoken implementation.
- Strong developer community backing.
- Innovative approach to secrets observability.

Challenges

- Needs expansion in secrets lifecycle management.
- Comprehensive integration and governance required.
- Scalable policy management for larger environments.
- Complementary product to other solutions in the Enterprise Secrets Management market.



Google – Secret Manager & Cloud Key Management Service

Google offers a range of solutions within the Enterprise Secrets Management domain, predominantly targeted at enhancing cloud-based services and infrastructures. Their portfolio includes tools like the Secret Manager, Cloud Key Management Service, and IoT support, reflecting their focus on supporting the management of secrets, cryptographic keys, and access controls within its ecosystem. Google stands out in the market leadership ranking due to its widespread cloud platform adoption and integration capabilities across different security services offered by GCP (Google Cloud Platform).

Among Google's key solutions, the Secret Manager serves as a primary solution for storing and managing API keys, passwords, and other secrets, fortified by fine-grained access control and audit capabilities. Meanwhile, Cloud KMS attends to cryptographic key management needs, facilitating encryption and rotation processes. These tools enable identity and secrets management, effectively supporting many security protocols across Google Cloud services.

Google provides integration within its vast cloud ecosystem, offering seamless interactions between Google's native tools and services. However, its focus primarily aligns with Google-driven environments, limiting usability outside its own platforms. Further enhancements in multi-platform integration and expanded lifecycle management features would enhance its standing within the broader Enterprise Secrets Management arena. Google's ongoing focus on post-quantum cryptography, investing in standards and innovation, and regulatory compliance demonstrates its commitment to future-proofing security measures.

Google Cloud Platform customers will find Google's solutions notably beneficial due to its inherent integration capabilities. Its solutions appeal strongly to sectors emphasizing cloud transformation, IoT development in combination with GCP IoT support, and large-scale data environments, such as technology and finance.

Security	Strong Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 15: Google's rating

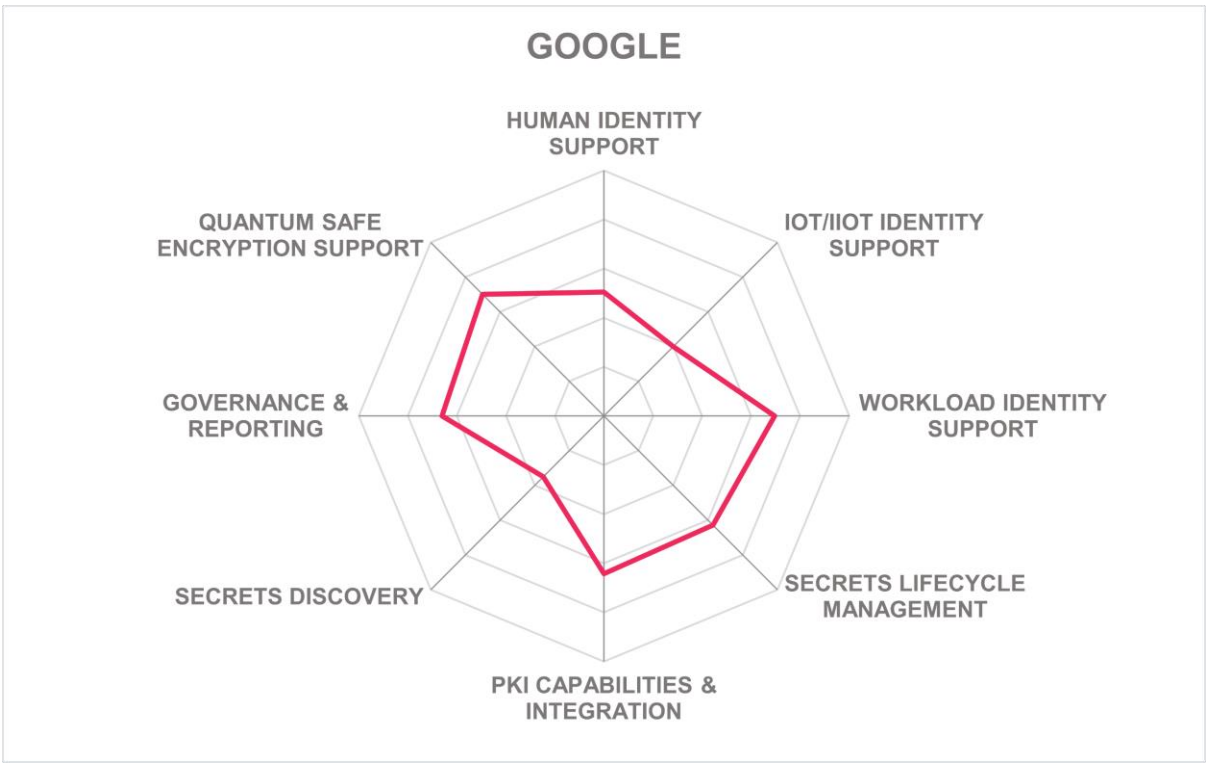
Strengths

- Integration within Google ecosystem.
- Many features for cryptographic key management.
- Emphasis on zero-trust principles.
- Support for IoT identity management as part of GCP.
- Compliance with security standards.
- Significant investments in QSE.

Challenges

- Limited multi-platform support.
- Need for expanded lifecycle management.
- Enhancements in cross-platform integrations.
- No full coverage of Enterprise Secrets Management use cases.

Leader in



HashiCorp – Vault

HashiCorp, founded 2012 and headquartered in San Francisco, U.S., plays a significant role within the broader Enterprise Secrets Management space, particularly with its Vault product, which is central to its cybersecurity solutions. Operating from San Francisco, USA, HashiCorp places a strong emphasis on securing dynamic, low-trust environments often found in cloud-native applications, focusing its efforts primarily on workload identities. With its recent acquisition by IBM, HashiCorp is well-positioned to grow its influence further, leveraging its strengths in managing secrets, certificates, and access controls for automated infrastructure provisioning.

Vault, HashiCorp's primary product in this domain, serves as a credential broker and a centralized platform for securing secrets and managing certificates. It supports just-in-time credential creation, providing automated key and certificate rotation, and integrates with identity providers via open standards to manage access policies effectively. Deployment options include self-managed, on-premises solutions or as a managed, cloud-based service via AWS, offering flexibility to enterprises. The platform supports a range of integrations, including DevOps tools, allowing organizations to unify their identity management landscape.

HashiCorp distinguishes itself with its strong focus on developer experience, supporting agile development through automation and just-in-time access. However, further enhancements in its user interface and expanded support for broader secrets lifecycle management capabilities would bolster its standing. With a forward-thinking roadmap, which includes streamlining maintenance and optimizing certificate management, HashiCorp demonstrates its competitive edge in a rapidly evolving market.

Enterprises focused on developing their own digital services running on a cloud-native infrastructure will find HashiCorp’s tools particularly beneficial, given their alignment with DevOps and agile development processes. Its solutions are an essential element of Enterprise Secrets Management environments, while not covering the full breadth of capabilities needed. They are suitable for organizations in technology, finance, and digital services sectors seeking enhanced security in agile development environments.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 16: HashiCorp’s rating

Strengths

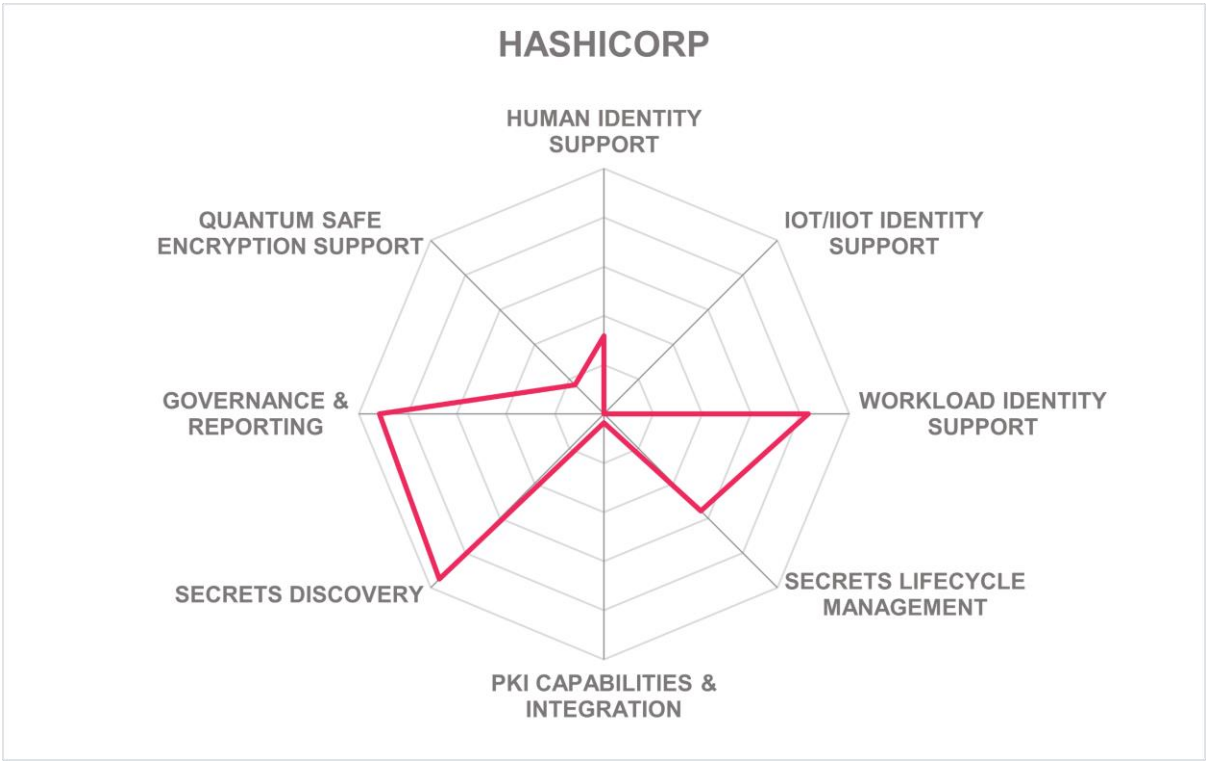
- Strong focus on workload identities.
- Many integrations with DevOps tools.
- Flexible deployment options.
- Dynamic secrets management, targeted at developers.

- Just-in-time access configurations.
- Centralized secrets and credential management.

Challenges

- No full Enterprise Secrets Management functionality.
- Need for further expanding lifecycle management features.
- Further enhancements in user-friendly automation.
- Stronger capabilities for enforcing governance across vaults.
- Lack of support for human and IoT/IIoT identities.
- Not focused on supporting QSE.

Leader in



HID Global – IAMS, PKI, CMS

HID Global, a part of ASSA ABLOY, was founded back in 1991 and is headquartered in Austin, U.S. It operates across various identity security segments, including PKI-as-a-Service. Their extensive portfolio emphasizes trust and security for across a wide range of applications, addressing enterprise needs for scalable certificate management. Leveraging acquisitions like IdenTrust and HydrantID, HID offers services like dedicated issuing CAs and private root PKI, providing full certificate lifecycle management. Their market focus includes sectors such as telecommunications, IoT, and financial services, with strengths in integrating digital and physical access controls.

The HID PKI-as-a-Service (PKIaaS) covers lifecycle management, auto-enrollment, and certificate discovery. Supporting standards like ACME, SCEP, and EST, it supports complex IT environments with seamless API access. The service extends to cloud platforms, enabling secure key management with options for auto-enrollment via Microsoft Intune and enterprise applications. Their centralized Certificate Manager supports broad integrations to CAs/PKIs and support for regulatory compliance requirements around cryptography.

HID Global stands out with a feature-rich, cloud-based PKI service. While the platform lacks certain NHI and workload identity capabilities, its emphasis on compliance, coupled with an extensive ecosystem, addresses common organizational PKI needs. They are currently implementing advanced support around crypto agility and offer code signing as a service including Kubernetes support, which strengthens its market stance. Opportunities for improvement involve expanding intuitive UI features and extending automation within PKI administration.

HID Global's PKIaaS is particularly beneficial for large organizations requiring a sophisticated approach to certificate management, such as banks and public sector units. Its ability to integrate with enterprise mobility and IoT/IIoT sectors makes it suitable for companies seeking scalable security models across geographies. Organizations in regulated industries, requiring stringent compliance and robust key management, should consider leveraging HID’s expertise to ensure the integrity and security of digital identities.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Neutral

Table 17: HID Global’s rating

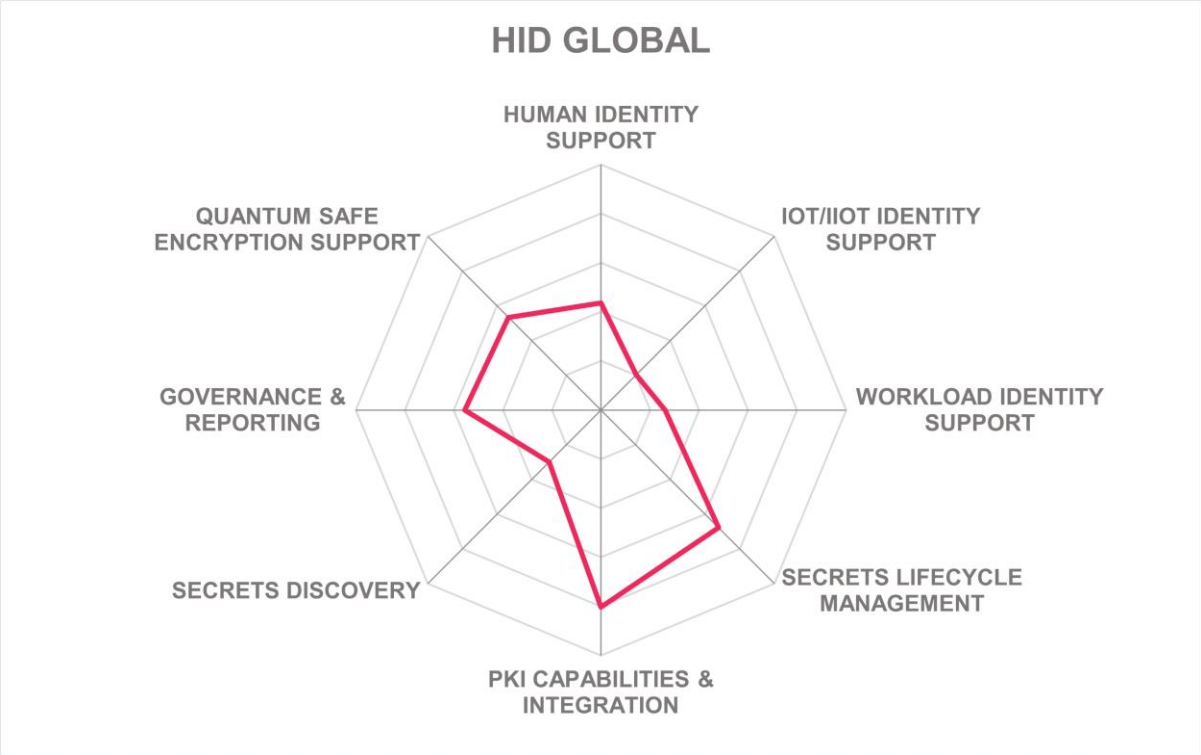
Strengths

- Comprehensive PKI lifecycle management.
- Broad standards and protocol support.
- Strong integrations with enterprise ecosystems.

- Secure, cloud-delivered certificate management.
- Support for IoT and IIoT workloads at scale.
- Active in delivering QSE and crypto agility support.
- Part of larger Assa Abloy group.

Challenges

- Limited NHI and workload identity support, beyond code signing.
- Need for UI integration across solutions.
- Capabilities spread across a range of individual solutions.
- Limited secrets discovery capabilities beyond TLS/SSL.



Intercede – MyID CMS, MyID MFA & MyID PSM

Intercede, a UK-based cybersecurity software company, founded in 1992, specializes in digital identity management with a focus on strong authentication through its MyID platform. While known for human-centric identity management, Intercede's core competency lies in issuing and managing credentials like PKI and FIDO passkeys at scale, often for government, aerospace, finance, healthcare, and industry sectors. The MyID system is crafted to support complex regulatory environments, ensuring secure credential lifecycle management for users and smart devices.

The MyID platform provides powerful capabilities, including issuing FIDO2 credentials with full lifecycle support. It integrates with certificate authorities, HSMs, smart cards, and various authentication means like OTPs, providing centralized auditing and reports. Its secure vault, set for release in Q1 2025, will enhance key management independence. MyID's architecture facilitates the retention and management of secure vaults and keys, supporting biometric and smart card enrollment, enabling secure, scalable digital identity management.

Intercede's strengths are rooted in its scalability and full credential lifecycle management that meet high regulatory requirements. While strong in human identity management, there is potential for expanding capabilities towards machine identities and high-certification-environment compatibilities. Further innovations such as extending onboarding for workload identities and improving reporting functionalities would further strengthen Intercede's position in the secrets management landscape. Support for new platforms and technologies highlights their capacity for adaptation and growth.

Intercede's solutions are particularly beneficial for enterprises needing secure identity management within regulated frameworks, such as government and defense organizations. The platform’s robust PKI and FIDO integration make it well-suited for sectors demanding reliable and scalable credential management systems. Organizations seeking to enhance their security posture with advanced authentication technologies may find Intercede's solutions a suitable choice.

Security	Strong positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

Table 18: Intercede’s rating

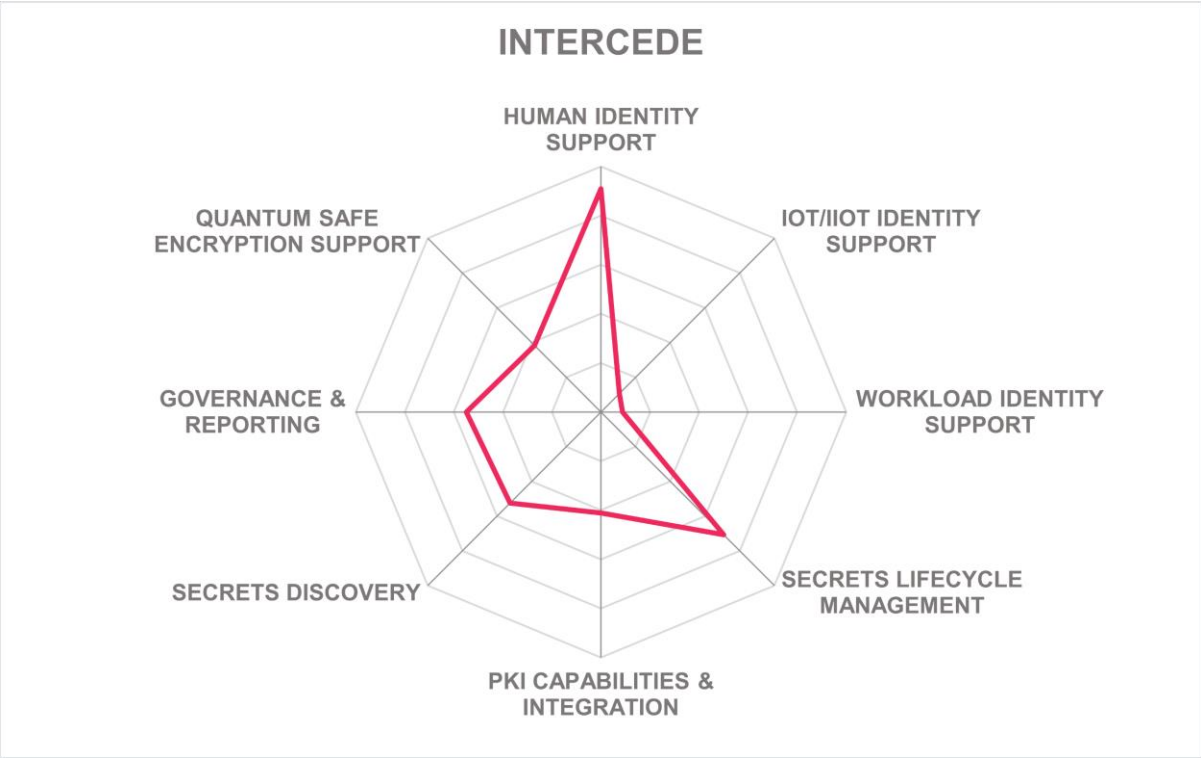
Strengths

- Comprehensive credential lifecycle management for human identities.
- Strong regulatory compliance support.
- Extensive PKI and innovative FIDO2 integration, filling common gaps in enterprise environments.
- Robust integration capabilities.

- Centralized auditing and reporting features.

Challenges

- Expanding support to machine identities.
- Enhancing user interface elements.
- Further innovation in onboarding processes.
- Lacks significant support for IoT/IIoT and workload identity support.



Keeper Security – KeeperPAM

Keeper Security, founded in 2011 and headquartered in Chicago, U.S., is a well-known player from the password management and PAM market segments and has an increasingly strong presence in the Enterprise Secrets Management domain, with a focus on advancing from password to secrets management for DevOps environments. The platform's core solutions center around a unified admin console and control plane, catering to a spectrum of security needs including SSH key management, automated password rotation, and third-party application access.

The Keeper platform's capabilities include encryption within a zero-trust and zero-knowledge architecture, ensuring security for credentials across devices and locations. It integrates smoothly with Single Sign-On (SSO) systems, remote browser isolation, and various DevOps platforms. Administrative tasks are streamlined through its modern UI, which provides session management, event logging, and compliance reporting.

Keeper distinguishes itself through its user-centric admin perspective, leveraging well-structured folders for credential management. Despite its strengths, the current discovery features remain basic and could benefit from further development to enhance management capabilities across more complex DevOps environments. .

Enterprises with needs spanning from traditional PAM to modern DevOps environments will find Keeper Security’s solutions particularly appealing due to their support for both traditional, password-centric use cases and increasing NHI support. Its focus on these areas makes it suitable for organizations seeking a cost-effective yet comprehensive tool to manage their secrets and access management. Industries with regulatory demands, such as finance and healthcare, can leverage Keeper’s detailed auditing and compliance features to strengthen their security posture within IT ecosystems.

Security	Strong Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

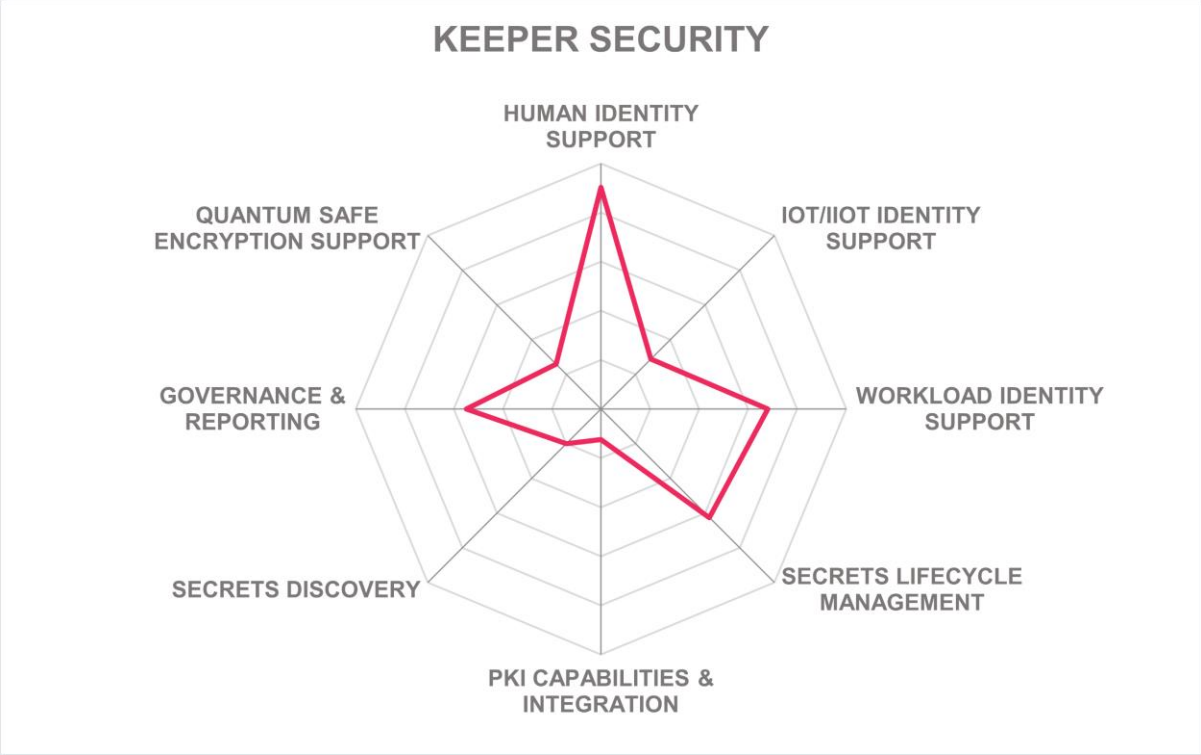
Table 19: Keeper Security’s rating

Strengths

- Good credential management capabilities, including strong password management support.
- Good integration with SSO and DevOps platforms.
- Based on zero-trust and zero-knowledge architecture.
- Streamlined workflows for credential management.
- Modern UI and admin console.

Challenges

- Basic secrets discovery features require enhancement.
- Expanding management capabilities across secrets and identity types needed.
- Further integration of AI/ML for risk management.
- Lacks PKI integration capabilities.
- Not yet working toward QSE.
- Needs more support for IoT/IIoT identity management.



Nexus – SmartID

As part of IN Groupe, Nexus, a company founded 1997 and headquartered in Stockholm, Sweden, benefits from a rich heritage and a robust infrastructure, allowing it to deliver identity solutions across physical and digital domains. Their solution encompass workforce and IoT identities, secure rights management, and certifications, integrating technologies like smartcards, FIDO keys, and biometrics to enable robust identity management and authentication processes.

The Nexus platform boasts a suite of capabilities, especially in areas like PKI and certificate management, with a wide range of integrations. Its Certificate Manager supports automation and complies with industry standards through protocols like SCEP and ACME. Nexus also excels in integrating multiple technologies to manage both physical and digital identities, providing a secure platform that includes HSM secured keys and multi-tenant capabilities, thereby facilitating robust access control and authentication across varied business needs.

Nexus differentiates itself through its strong PKI capabilities and their support for physical identity management. This is particularly evident in its SmartID framework, which optimizes identity lifecycle management by taking a holistic perspective across all managed identity types. However, the company's current focus shows less emphasis on the evolving DevOps environment, with opportunities to strengthen its solutions in that area. Future developments and a broader engagement with DevOps environments will be necessary to enhance Nexus's position in the rapidly advancing IT landscape.

The Nexus platform is especially valuable for enterprises requiring sophisticated identity management solutions, including government entities and organizations with a high dependency on interoperable identity verification systems. Businesses in telecommunications and automotive sectors, which rely on robust PKI solutions for secure communications, will find Nexus’s solutions capable of meeting their complex security requirements.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 20: Nexus’s rating

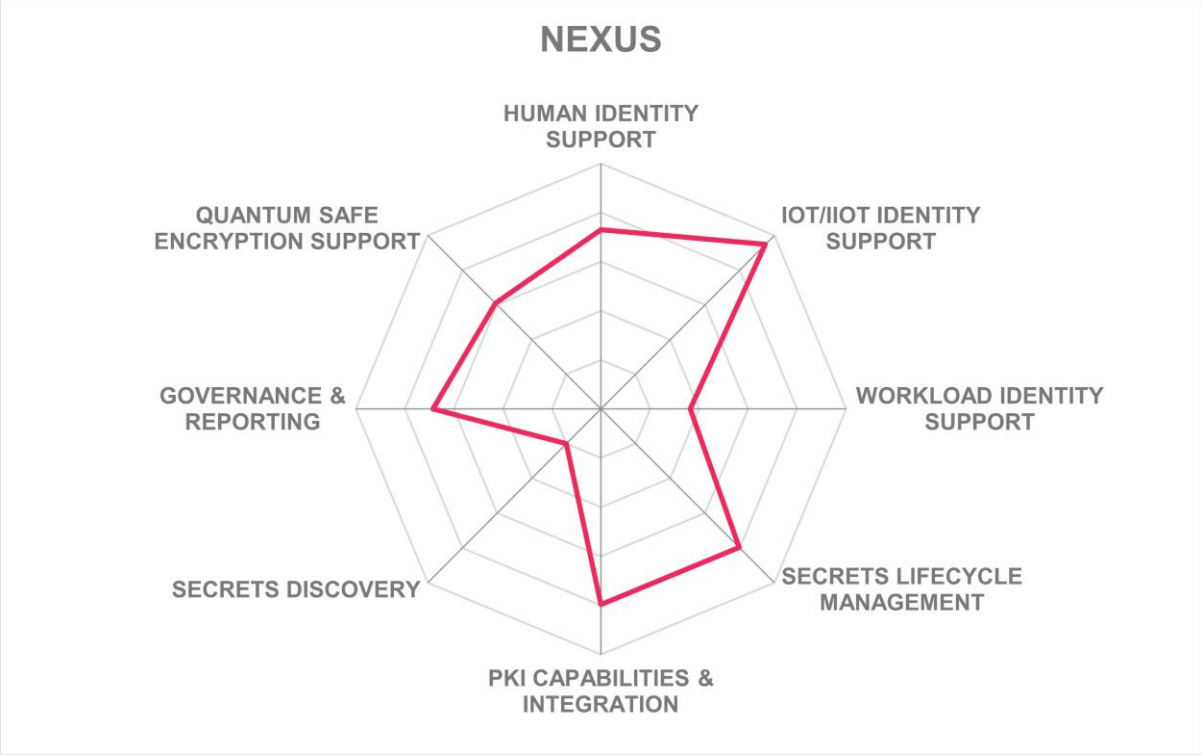
Strengths

- Strong PKI and certificate management.
- Robust integration of physical and digital identities.
- Support for IoT/IIoT device identity use cases.
- Advanced multi-tenant and access control features.
- Proven track record with government and large enterprises.

- Extensive protocol support, including ACME, CMPv2, CRL, SCEP, and many others for diverse environments.

Challenges

- Limited focus on DevOps integration.
- Need for enhancements in detecting secrets, particularly in the NHI field.
- Expanding support towards modern developer environments.
- Overall gap in supporting workload identities.



Saviynt – Identity Cloud

Saviynt, founded in 2010 and headquartered in El Segundo, U.S., is entering the field of Enterprise Secrets Management by developing on its foundation in Privileged Access Management (PAM) and moving into the areas of Machine Identity Management and Non-Human Identity Management. As a firm showing strong growth, Saviynt has customers in many industries, from government agencies to enterprises across sectors such as finance, healthcare, and technology.

The Saviynt platform performs discovery, vaulting, rotation, and auditing of both human and machine secrets. It provides identity lifecycle and access management, integrating with all major cloud platforms for onboarding and inventory management. Saviynt's solution comes with advanced analytics for governance and regulatory compliance, offering continuous monitoring and auditing functionalities to support both real-time and retrospective analyses.

Saviynt is distinguished by their identity security and machine identity management capabilities, with a strong focus on access governance. The integration across multi-cloud environments allows for dynamic onboarding and management of secrets. By expanding machine identity management features and advancing its secrets lifecycle capabilities could further solidify Saviynt's market position. Their roadmap is focused on enhancing governance and intelligent automation.

Well-suited for enterprises seeking identity and secrets management across a wide range of use cases, Saviynt's platform is particularly beneficial for organizations in regulated industries such as finance and healthcare. With its scalable architecture, it supports complex environments requiring intricate auditing and compliance mechanisms. Enterprises looking to integrate advanced identity management with an easy-to-use and secure experience will find Saviynt's solutions well-aligned with their strategic goals.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

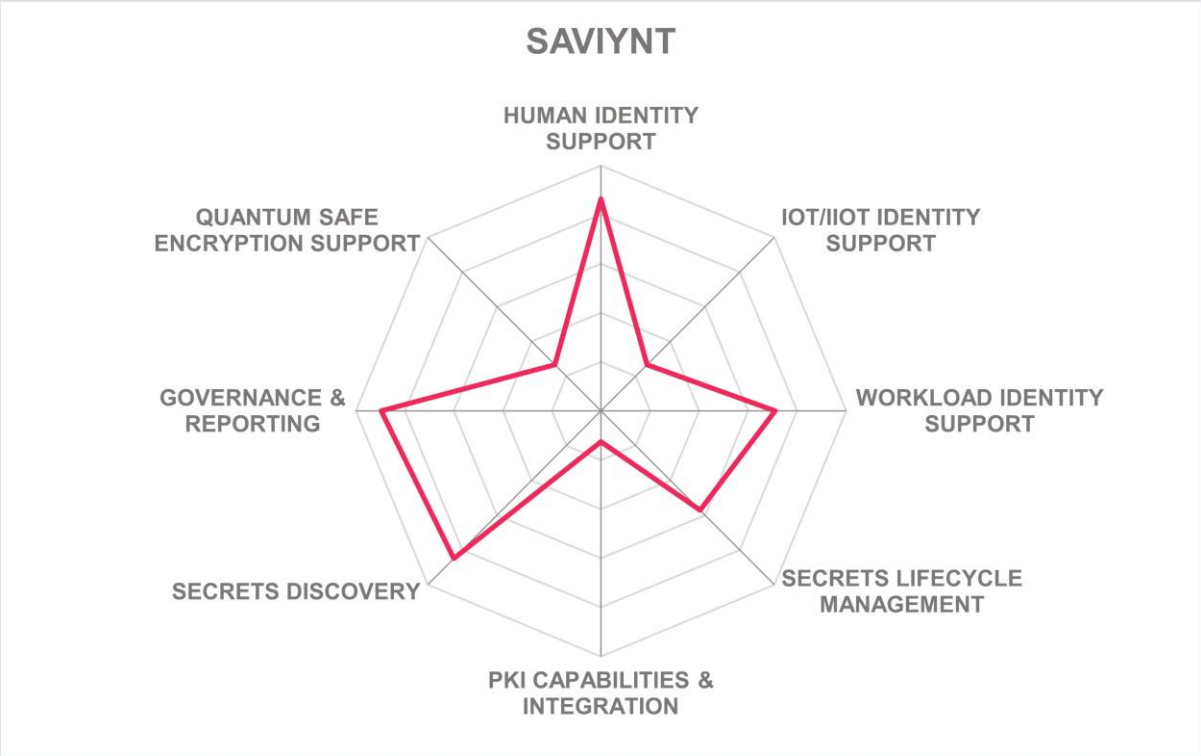
Table 21: Saviynt's rating

Strengths

- Good secrets management capabilities, with strong support for human users including PAM use cases and growing support for NHI.
- Focused on SaaS deployments, but with flexibility for specific customer requirements.
- Leading-edge Identity lifecycle management focused on human users.
- Advanced governance and compliance features.
- Extensive customer and partner network.

Challenges

- Enhancement needed in machine identity management, especially IoT/IIoT devices.
- Further development of secrets lifecycle capabilities.
- Expanding automation and integration features.
- Further enhancements in secrets discovery needed.
- Lacks PKI integration.
- Needs more work on quantum safe encryption technologies.
- Further improvement needed for workload identity management.



SSH – PrivX

SSH Communications Security (SSH), founded in 1995 and headquartered in Helsinki, Finland, is an established vendor in the Enterprise Secrets Management field with its focus on secure communications and privileged access management, particularly through its Zero Trust Suite. SSH's SalaX, PrivX, and NQX platforms secure systems, human communications, and network connections. Their customers include organizations from finance, retail, manufacturing, defense, healthcare, government, semiconductor, and other sectors, protecting critical applications that handle millions of SSH sessions daily using ephemeral access.

Central to SSH's platform is the PrivX solution, which, in addition to PAM features, is designed for discovering and managing SSH keys and securing their lifecycle. It supports passwordless and keyless access, integrating with modern authentication methods to eliminate the risks associated with static credentials. The platform's capabilities include automated key rotation, policy-based access control, as well as robust compliance and governance features. PrivX supports integration with CI/CD pipelines and various identity management systems such as SailPoint or Microsoft Entra, offering microservices architecture for scalability and operational efficiency without downtime.

While SSH has leading-edge features, their product is specialized, focusing heavily on SSH key management and security. Some potential areas for future growth include expanding support for broader TLS lifecycle management and enhancing DevOps integration to handle a wider array of secrets management needs. A key strength is their innovative approach to reducing credential risks through Zero Trust principles and keyless management.

Organizations looking for robust SSH key management and secure access solutions, particularly those in sectors with stringent security requirements including finance and technology, will find value in SSH's solutions. Their emphasis on scalable, secure communications makes their solutions highly relevant for enterprises seeking to streamline SSH key lifecycle and incorporate modern secure access methodologies across diverse IT environments.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 22: SSH's rating

Strengths

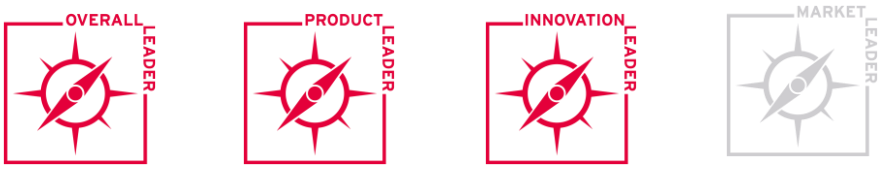
- Leading-edge SSH key management.
- Zero Trust-based access principles.
- Modern microservices architecture.
- policy-based controls.

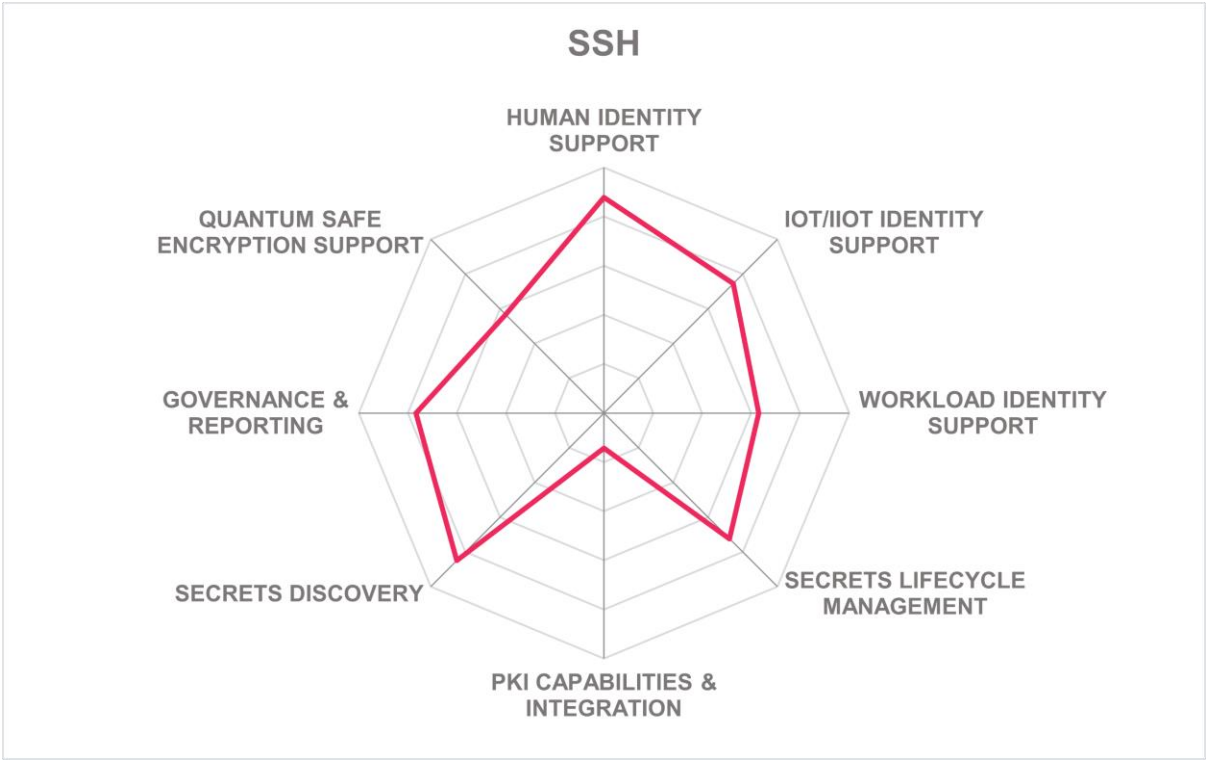
- Migration to passwordless and keyless access enforcement through ephemeral, certificate-based authentication.
- Scalable solutions for large enterprises.
- Taking steps toward quantum safe encryption.

Challenges

- Need for broader TLS lifecycle support.
- Expansion in DevOps integration and broader NHI management support beyond SSH focus needed.
- Enhancements in multi-protocol support needed.
- Could use more PKI integration.
- More features for workload identity protection would be beneficial.

Leader in





Thales – CipherTrust Secrets Management

Thales, founded in 2000 with its roots dating back to 1968, headquartered in Paris, France, counts amongst the leaders in the Enterprise Secrets Management domain, based on its CipherTrust Data Security Platform. Thales has made significant acquisitions across the data security industry in recent years, and thus its solutions span multi-cloud key management, encryption, secrets discovery, classification, and tokenization. Their approach includes extensive capabilities in a unified platform, which provides a good experience for managing secrets, keys, and credentials across diverse IT environments.

Key capabilities of Thales' platform include secure management of credentials and secrets through Distributed Fragments Cryptography™ (DFC), provided by Akeyless, which ensures zero knowledge operations for key management by fragmenting keys across various locations. The CipherTrust platform can handle lifecycle management with features such as Just-In-Time and dynamic rotation. Thales also provides extensive audit and governance tools. Their platform offers good integrations with popular DevOps tools such as HashiCorp Vault.

Thales differentiates itself with its flexible deployment models spanning from traditional on-premises deployments to modern cloud deployments and integration capabilities, alongside the sophisticated use of DFC for enhanced security and operational clarity. The integration of Thales' own HSMs with CipherTrust provides a highly secure and scalable, multi-layered security architecture. However, opportunities for improvement include further refinement in the admin UI integration between Thales and Akeyless environments. Expanding the management of complex DevOps requirements within the same console could further refine their solution.

Thales' solutions are well-suited for globally operating enterprises that demand secure, compliant, and efficient secrets and key management across complex environments. Industries with high security requirements, such as finance, telecommunications, and government sectors, will find Thales' solutions particularly advantageous. As businesses increasingly embrace multi-cloud architectures, Thales positions itself as a go-to provider for comprehensive security solutions that bridge traditional and modern IT landscapes.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 23: Thales's rating

Strengths

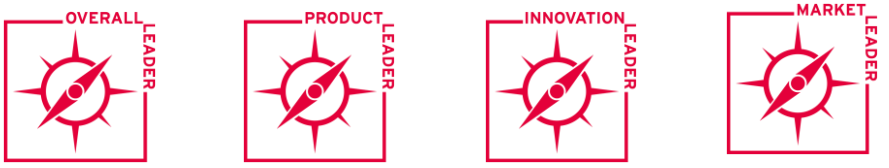
- Excellent secrets and key management.
- Distributed Fragments Cryptography for enhanced security (by Akeyless).
- Support for multi-cloud integrations.

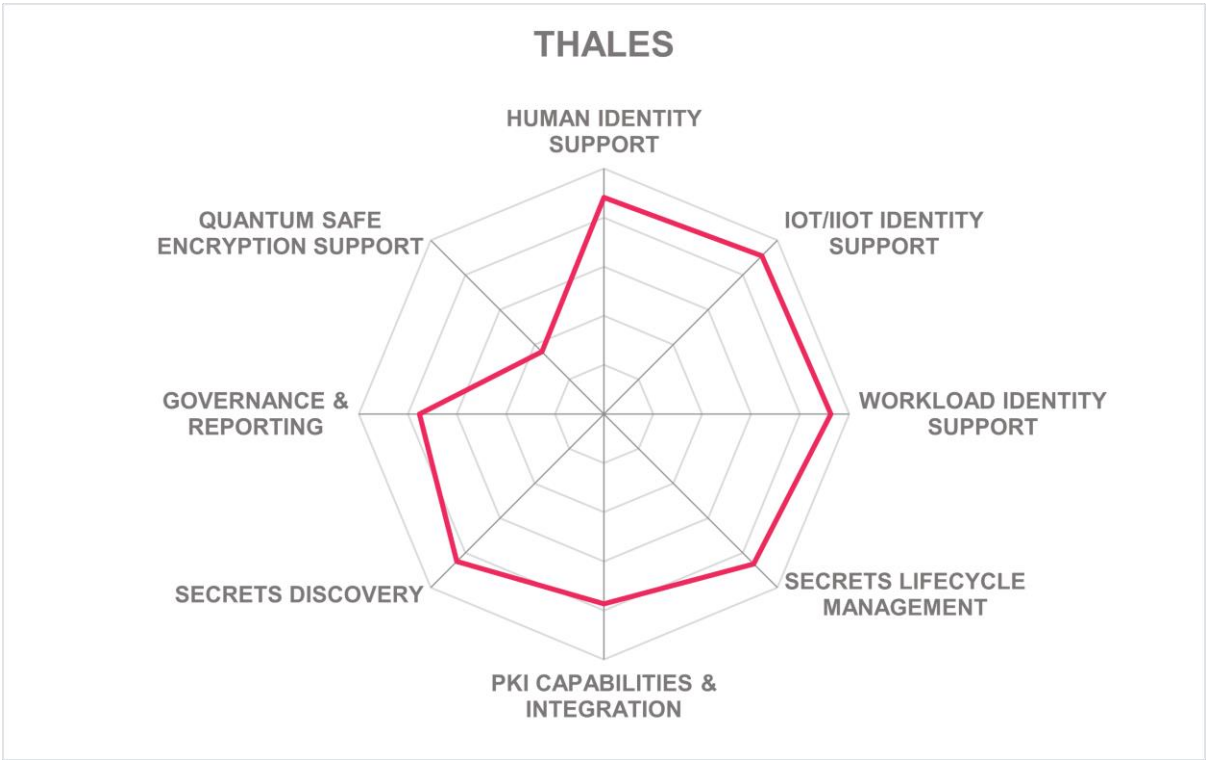
- Extensive audit and governance capabilities.
- Strong HSM integration for security.
- Flexible and scalable deployment models.
- Extensive partner and customer network.
- Efficient compliance monitoring tools.

Challenges

- Showing progress on admin UI integration across Thales and Akeyless components.
- Expanding support for complex DevOps needs, more integrations on the roadmap.
- Further support for quantum safe encryption on the roadmap.

Leader in





Versasec – vSEC:CMS & vSEC:CLOUD

Versasec, founded in 2007 and headquartered in Stockholm, Sweden, provides solutions for credential management. Based in Sweden, with a global presence that includes offices in the USA, France, and several other countries, Versasec integrates phishing-resistant credentials compliant with government regulations into its solutions. Their vSEC:CMS and vSEC:CLOUD products enable organizations to adopt modern authentication measures, such as PKI and FIDO, while orchestrating identity management processes effectively.

Versasec's platform offers robust capabilities in managing a wide range of credentials, including RFID, virtual smart cards, and FIDO2, enhancing passwordless identity solutions for modern authentication. The platform supports automatic certificate management through ACME and facilitates orchestration and lifecycle management of credentials. It integrates with identity solutions like Microsoft, Okta, and others, and supports integration with hardware security modules.

The key strengths of Versasec lie in its credential management, including PKI and FIDO life cycles, within a single administrative interface. Its ability to integrate with multiple credential and identity providers distinguishes it as a flexible solution. However, while Versasec effectively manages a broad array of identity components, the user interface could benefit from further refinement, and there is room for improvement in enhancing automation features for complex environments. These enhancements would cater to the evolving needs of enterprises as they expand their digital identity frameworks. However, Versasec lacks support for NHI management.

Organizations looking for strong credential management centered on human identities with a focus on PKI and FIDO will find Versasec's platform potentially beneficial. This is particularly useful for several industry sectors, including government, finance, and healthcare, where regulatory compliance and secure identity management are essential. Versasec’s solutions are frequently complementary to other vendor’s solutions, due to their strengths in supporting edge use cases around human secrets management.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 24: Versasec’s rating

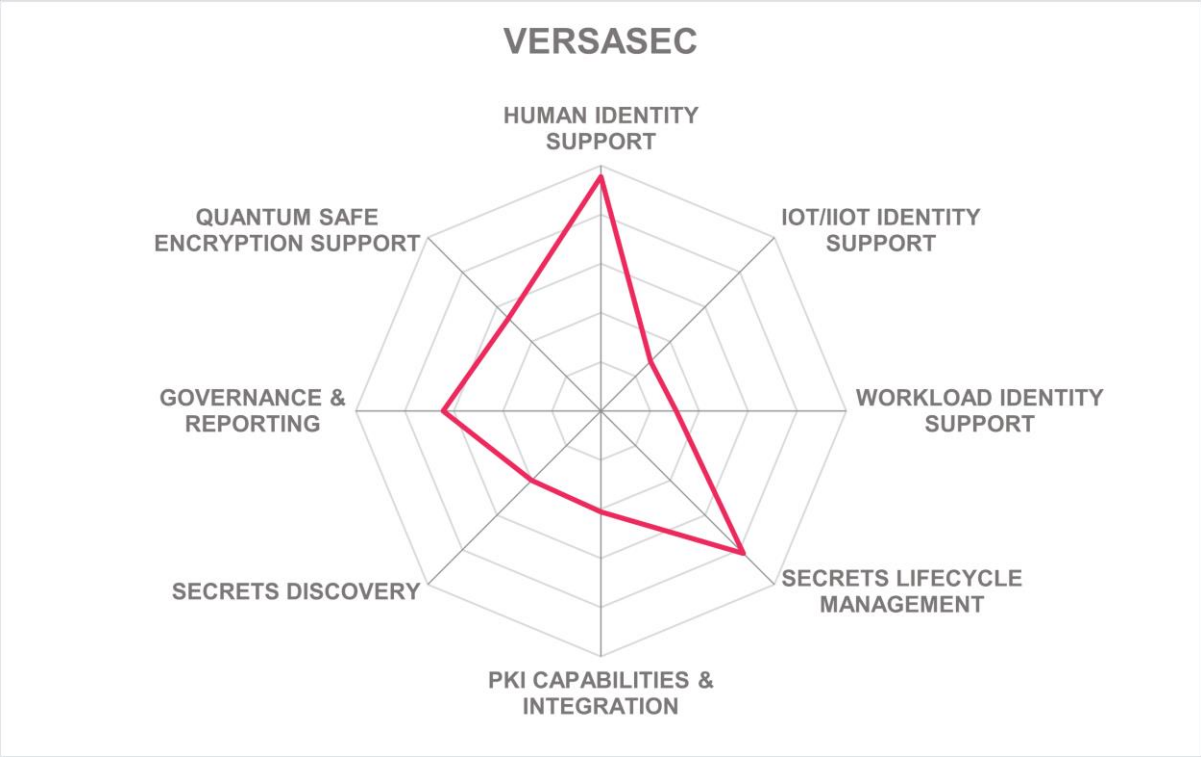
Strengths

- Very good credential lifecycle management for humans.
- Leading-edge support for FIDO2 key management.
- Integration with multiple identity providers.
- Phishing-resistant credential solutions.
- Secure, government-compliant operations.

- Rich API and automation capabilities.

Challenges

- User interface needs refinement.
- Enhanced automation for complex environments.
- Improved scalability in dynamic settings.
- Lack of NHI Management support.
- Small vendor, but good partner ecosystem.
- Additional capabilities in secrets discovery and governance and reporting would be helpful.



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

Aembit

Aembit offers an identity-based access management solution designed to secure machine-to-machine communications. Its platform focuses on providing granular control over service-to-service access, reducing the risks associated with over-permissioned environments. By providing continuous authorization and fine-grained policies, Aembit helps organizations streamline secure access in complex architectures.

Why worth watching: Aembit's approach to identity-based authorization for services highlights a shift toward more dynamic, context-aware access control mechanisms.

Andromeda Security

Andromeda Security specializes in protecting sensitive data through advanced encryption techniques and secure key management. Its solutions integrate with a wide range of environments, offering flexibility without compromising security. The platform is designed to address challenges in secret distribution and lifecycle management across modern infrastructures.

Why worth watching: Andromeda Security's focus on adaptable encryption and key management makes it relevant for organizations seeking streamlined secrets governance.

AxisNow

AxisNow delivers enterprise-grade access solutions that simplify secure credential management. Its platform provides centralized oversight, reducing administrative overhead while enhancing security posture. With automation features to manage secrets lifecycle efficiently, AxisNow aims to improve operational resilience.

Why worth watching: AxisNow’s emphasis on automation within secrets management offers a practical approach to reducing human error and maintaining secure access controls.

Britive

Britive focuses on privileged access management, offering dynamic permissioning capabilities designed for fast changing environments. Its platform enables just-in-time access provisioning, minimizing standing privileges and enhancing security. Integration with cloud services further supports organizations in managing identities across complex ecosystems.

Why worth watching: Britive’s dynamic permissioning approach aligns with the growing need to minimize persistent access risks in enterprise systems.

Clarity Security

Clarity Security provides tools for managing secrets and credentials with an emphasis on visibility and compliance. Its solution supports granular auditing capabilities, helping organizations maintain regulatory requirements while securing sensitive data. The platform’s flexibility supports a range of deployment scenarios.

Why worth watching: Clarity Security’s focus on auditability and compliance adds value for organizations with strong regulatory obligations.

Corsha

Corsha offers a dynamic API security platform with built-in secrets management to protect machine identities, especially in OT and IIoT environments. Its technology leverages rotating credentials to enhance security for API communications, reducing the attack surface for credential-based threats.

Why worth watching: Corsha’s use of dynamic, rotating credentials introduces an effective method for mitigating API security risks in the complex world of OT and IIoT.

Cross Identity

Cross Identity delivers identity-centric security solutions that integrate with enterprise environments. Its platform supports secure credential storage, fine-grained access control, and real-time monitoring to detect and respond to unauthorized activities.

Why worth watching: Cross Identity's integration of real-time monitoring with secrets management provides a solution to address evolving security threats from a central tool.

Mtg.de

Mtg.de specializes in cryptographic key management solutions tailored to enterprise needs. Its products focus on secure key generation, distribution, and lifecycle management, supporting compliance with industry standards for data protection.

Why worth watching: Mtg.de’s expertise in cryptographic key management addresses requirements for secure data handling in regulated industries.

Natoma

Natoma develops secure identity and secrets management solutions with a focus on scalability. Its platform supports complex deployment scenarios, providing policy enforcement and automated secrets rotation to reduce administrative burden.

Why worth watching: Natoma's emphasis on scalability and automation makes it suitable for organizations managing large, dynamic environments.

Oasis Security

Oasis Security offers a comprehensive secrets management platform designed to secure sensitive information across distributed systems. Its solution integrates with a variety of development pipelines, enabling consistent secret governance throughout the software lifecycle.

Why worth watching: Oasis Security’s integration with development workflows supports consistent and secure management of secrets from code to production.

Oracle

Oracle Key Vault provides a centralized key management solution optimized for Oracle environments. It facilitates secure key storage, sharing, and lifecycle management, ensuring strong encryption practices within enterprise databases and applications.

Why worth watching: Oracle Key Vault's deep integration with Oracle technologies makes it a strong choice for enterprises invested in Oracle ecosystems.

P0 Security

P0 Security focuses on securing machine identities and secrets with a platform that emphasizes policy-driven access controls. Its approach minimizes risks associated with hard-coded credentials and unmanaged secrets.

Why worth watching: P0 Security’s policy-driven framework addresses the growing concern over unmanaged machine identities in complex infrastructures.

SlashID

SlashID offers a unified platform for managing secrets and identity credentials. Its solution supports strong authentication methods and secure secret distribution, enhancing security across cloud and on-premises environments.

Why worth watching: SlashID’s unified approach simplifies the management of both identities and secrets, reducing complexity in enterprise security operations.

Smallstep

Smallstep focuses on simplifying certificate management and secure communications for modern infrastructures. Its tools help automate the issuance, renewal, and revocation of certificates, supporting secure connections across diverse systems.

Why worth watching: Smallstep’s automation capabilities in certificate management offer practical benefits for organizations aiming to reduce manual security processes.

SPIRL

SPIRL delivers a secrets management solution designed for ease of use and strong security, building on the SPIFFE standards and SPIRE solution. Its platform integrates with existing

DevOps workflows, enabling secret distribution and lifecycle management without disrupting development processes.

Why worth watching: SPIRL's developer-friendly approach makes secrets management accessible without compromising on security controls.

Teleport

Teleport provides secure access solutions for infrastructure, including secrets management as part of its broader security platform. It supports secure credential handling, session recording, and policy enforcement across cloud and on-premises environments.

Why worth watching: Teleport's integrated approach to access and secrets management offers comprehensive security for complex enterprise infrastructures.

TrustFour

TrustFour focuses on securing digital identities and managing secrets with a platform that emphasizes transparency and control. Its solution provides detailed auditing capabilities and strong encryption to safeguard sensitive information.

Why worth watching: TrustFour's transparency-driven design supports organizations with high compliance and auditing requirements.

Unosecur

Unosecur offers a security platform for managing credentials and secrets in distributed environments. Its tools provide automated secret rotation, granular access controls, and real-time monitoring to detect potential security issues.

Why worth watching: Unosecur's focus on automation and real-time monitoring aligns with the need for proactive security in dynamic infrastructures.

Whiteswan Identity Security

Whiteswan Identity Security delivers secrets management solutions designed to protect sensitive data at scale. Its platform emphasizes secure storage, access governance, and continuous compliance monitoring to meet enterprise security demands.

Why worth watching: Whiteswan Identity Security's focus on continuous compliance monitoring helps organizations maintain strong security postures in regulated environments.

Related Research

Leadership Compass Secrets Management

Leadership Compass Privileged Access Management

Leadership Compass Cloud Infrastructure Entitlement Management

Leadership Brief Managing Non-Human Identities

Advisory Note Machine Identities

Advisory Note The 2025 Identity Fabric and Reference Architecture

Rising Star SPIRL

Rising Star Corsha

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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