kuppingercole ANALYSTS

Non-Human Identity Management

Nitish Deshpande

November 25, 2025

LEADERSHIP COMPASS 2025

This report provides an overview of the Non-Human Identity Management market and a compass to help you find a solution that best meets your needs. It examines solutions that provide comprehensive lifecycle events for managing and governing non-human identities. It provides an assessment of the capabilities of these solutions to meet the needs of various sizes of organizations.

Contents

Executive Summary 4
Key Findings 6
Market Analysis 6
Delivery Models 7
Required Capabilities 7
Leadership 9
Overall Leadership 9
Product Leadership 10
Innovation Leadership 12
Market Leadership 14
Product/Vendor evaluation 16
Spider graphs 16
Aembit – Aembit Workload IAM Platform 18
Akeyless – Akeyless Secrets & Non-Human Identity Platform 20
Andromeda Security – Andromeda Identity Security Platform 23
AppViewX – AVX ONE 25
BeyondTrust – Pathfinder Platform 27
Britive – Britive Cloud Identity Security Platform 29
Clutch Security – Universal Non-Human Identity Security Platform 31
CyberArk – CyberArk Identity Security Platform 34
Defakto – Non-Human IAM Platform 37
Delinea – Delinea Platform 40
Entro Security – Entro Security NHI and Secrets Platform 43
Evolveum – midPoint 46
GitGuardian – GitGuardian Platform 48
HashiCorp, an IBM company – HashiCorp Vault 51
Keeper Security – Keeper Secrets Manager 54

KRON – KRON PAM 57
Microsoft – Entra ID 60
One Identity – One Identity Manager 63
Pathlock – Pathlock Cloud 66
SailPoint – Identity IQ, Identity Security Cloud 68
Saviynt – Saviynt Identity Cloud 70
Silverfort – NHI Security 73
Teleport – Teleport Infrastructure Identity Platform 76
Token Security – NHI Security Platform 78
Veza – Veza Access Platform 80
Whiteswan – Whiteswan ITDR 82
Vendors to Watch 84
Astrix 84
AWS 84
Axiad 84
Axis Now 84
Clarity Security 85
Corsha 85
Cycode 85
Google 85
P0 Security 86
SlashID 86
Thales 86
TrustFour 86
Unosecur 87
Widas 87
WSO2 87
Related Research 87
Copyright 88

Executive Summary

The concept of identity in digital systems has expanded beyond the traditional scope of human users. Today, a wide range of systems including applications, containers, scripts, APIs, service accounts, and backend processes operate autonomously, interacting with infrastructure and data across cloud-native, SaaS, and on-premises environments. These systems, collectively referred to as non-human identities (NHIs), form the backbone of modern IT architectures. In many environments, NHIs outnumber human identities by several orders of magnitude, creating a complex and often unmonitored identity landscape. These identities typically hold significant levels of access and, without proper oversight, introduce substantial operational and security risk.

The explosion of NHIs presents both unprecedented opportunities and significant security challenges. As enterprises increasingly embrace Internet of Things (IoT), AI, and cloud-native architectures, the demand for strategic governance of these identities has never been more critical. NHIs, by their nature, require meticulous management practices distinct from human identity governance. It demands an approach that integrates with existing cybersecurity frameworks.

The shift toward automation, continuous deployment, microservices, and infrastructure-as-code has further accelerated the creation of NHIs. A strategic governance approach for NHIs requires leveraging automated identity lifecycle management, enhanced monitoring, and policy enforcement across many different identity types. Such an approach demands frameworks that support interoperability between different identity management ecosystems, ensuring consistent application of access policies and security protocols. Furthermore, it underscores the importance of integrating advanced technologies such as machine learning for real-time threat detection and behavioral analytics to proactively identify and mitigate potential security breaches.

The current state of NHI governance is often fragmented as many organizations lack cohesive strategies to manage these identities effectively. Traditional IAM and PAM systems were not designed to handle the dynamic and large-scale nature of these entities, especially when short-lived and ephemeral in nature. They also do not adequately address the security complexities of device and system accounts. This gap in governance not only poses significant security risks but also hampers organizational agility and innovation by impeding operations across interconnected environments. As a result, organizations are turning to purpose-built NHIM solutions to introduce lifecycle governance, enforce least privilege, and reduce operational risk.

By prioritizing strategic governance for NHIs, organizations can enhance their security postures while fostering innovation and operational efficiency. This involves not only deploying state-of-the-art identity solutions but also adopting a culture of continuous improvement and adaptation to the ever-evolving technological landscape. As NHIs continue to play a pivotal role in digital transformation, comprehensive governance frameworks will be critical in securing the future of digital enterprises.

A key driver is the need to eliminate hardcoded credentials and unmanaged secrets, which remain prevalent across infrastructure-as-code repositories and CI/CD pipelines. The ability to programmatically manage access based on identity, policy, and runtime context, is increasingly viewed as foundational to securing machine-to-machine communication in multi-cloud and hybrid environments. Moreover, regulatory and compliance frameworks are beginning to emphasize accountability for machine access in the same way as for human users, adding further pressure on organizations to implement formal controls for NHIs.

The market for NHI Management (NHIM) solutions is evolving quickly. A mix of specialized vendors and broader IAM or secrets management providers are developing or extending their offerings to address the lifecycle and risk associated with machine identities. Some vendors focus on discovery and classification, helping organizations gain visibility into unmanaged or shadow identities. Others concentrate on automation, embedding identity logic into DevOps pipelines, or enforcing granular policy controls through integration with workload orchestration systems. The shift toward containerized applications, distributed microservices, and ephemeral workloads has exposed the limitations of legacy identity governance models. NHIM solutions address this gap by enabling real-time identity provisioning, policy-based access enforcement, and the secure handling of machine credentials throughout their lifecycle.

While not yet a universally adopted practice, NHIM is increasingly seen as an essential extension of identity-first security strategies and Zero Trust architectures. Vendors in this space are differentiating through support for cloud-native integrations, workload identity federation, and automated rotation of credentials. Although precise market sizing is still emerging, analyst estimates suggest high growth potential due to its critical role in cloud and DevOps security. The relevance of NHIM is further supported by its alignment with enterprise priorities such as digital modernization, compliance readiness, and reduction of attack surface in hybrid environments.

NHIM solutions are primarily being adopted by enterprises operating in complex, regulated, or highly automated environments. These include sectors such as financial services, healthcare, telecommunications, manufacturing, and technology, where operational scale and security obligations converge. To summarize it, the relevance of NHIM extends to any organization operating in a cloud-native or hybrid context, particularly those embracing Zero Trust principles or pursuing compliance with frameworks such as ISO 27001, NIST SP 800-53, or CIS controls. Stakeholders typically include CISOs, identity architects, DevSecOps leads, and cloud security teams tasked with reducing operational risk and maintaining governance across a sprawling identity landscape.

While larger organizations tend to drive early adoption due to the scale of their non-human identity footprint, vendors are also developing lighter-weight offerings to meet the needs of mid-market buyers. The adoption is global, though initial traction has been strongest in North America and parts of Europe. From a maturity standpoint, early adopters include organizations that have implemented or are actively pursuing Zero Trust architectures, have embraced infrastructure-as-code and CI/CD methodologies, and are seeking to standardize workload identity management across cloud and on-premises deployments.

As the technology matures, broader adoption is expected among enterprises modernizing legacy IAM frameworks or consolidating fragmented secrets and machine identity practices under a unified governance model.

Key Findings

- The Non-Human Identity Management (NHIM) market has evolved into a distinct and rapidly maturing segment of the Identity and Access Management (IAM) ecosystem.
- NHIs outnumber human identities by 25x-50x
- NHIs includes various types of identities such as workloads, service accounts, applications, containers, APIs, bots, scripts, and devices.
- Poor governance of NHIs such as unmanaged secrets, over-privileged, hardcoded credentials, and lack of ownership mapping creates a significant attack surface.
- Vendors are moving toward integrated lifecycle management which includes discovery, classification, policy enforcement, rotation, ephemeral credential issuance, and deprovisioning.
- Integration with DevOps pipelines, CI/CD workflows, and infrastructure-as-code is now a core required capability.
- Behavioral analytics, context-aware access, and dynamic risk scoring prove to be the some of the advanced capability differentiators between NHIM vendors.
- NHIM solutions are increasingly relevant to regulated and security-sensitive industries such as finance, healthcare, manufacturing, and critical infrastructure.
- The market is trending toward convergence between NHIM, Cloud Infrastructure Entitlement Management (CIEM), and secrets management platforms, forming a more unified and policy-driven identity security layer for non-human entities.
- Future success for vendors will hinge on the ability to deliver scalable, multi-cloud, and developer-friendly solutions that provide full lifecycle governance, strong integrations, and high automation to meet the growing scale of machine identities.
- Overall Leaders in this report are AppViewX, BeyondTrust, CyberArk, Delinea, HashiCorp, an IBM company, Keeper Security, Kron, Microsoft, and One Identity.

Market Analysis

The market for NHIM is undergoing accelerated transformation, driven by the expanding scale and complexity of machine-to-machine interactions in cloud-native environments. What was once considered a feature within secrets management or privileged access tools has evolved into a distinct category of identity and access management.

NHIM now represents a foundational requirement for organizations modernizing security in DevOps pipelines, distributed systems, and hybrid cloud infrastructures. The rise in non-human actors, ranging from containers and APIs to service accounts and bots, has forced enterprises to reevaluate how identity is defined, governed, and secured across systems. As enterprises shift toward Zero Trust architectures, the demand for lifecycle management, credential governance, and real-time access control for machine identities is no longer optional.

Vendor momentum within the NHIM space reflects both strategic repositioning and organic innovation. Several major identity and security vendors have entered the market through acquisitions or capability extensions, integrating NHIM into broader IAM, PAM, or secrets management platforms. This has created a highly dynamic competitive environment where startups continue to differentiate by offering cloud-native architectures, policy-driven identity automation, and deeper DevOps alignment. Integration into developer workflows such as through APIs, SDKs, or CI/CD plugins is a key requirement.

The baseline feature set such as identity discovery, ephemeral credentials, and policy enforcement has matured significantly. Some vendors emphasize secretless authentication using ephemeral credentials injected at runtime. Others offer advanced policy engines that enable context-aware access controls, such as conditional enforcement based on workload type, geographic region, or runtime behaviour.

However, many traditional vendors are still adapting their platforms to handle the unique lifecycle and governance needs of NHIs. While the market is maturing, new entrants are successfully carving out specialized niches by focusing on context-aware access, behavioural analytics, or tightly scoped compliance use cases. As NHIM becomes a strategic layer in identity security, the market is expected to consolidate around platforms that demonstrate both horizontal integration and vertical depth in machine identity governance.

Delivery Models

Non-Human Identity Management solutions are delivered through various models to meet diverse organizational requirements:

Cloud-Based Services: Almost all NHI management solutions support cloud deployments. This option offers scalability and ease of deployment, particularly suited for organizations with dynamic, distributed environments. These services support multi-tenant architectures and provide robust API integrations.

On-Premises Deployments: These are 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.

Hybrid Models: These combine on-premises and cloud capabilities, allowing organizations to maintain sensitive operations locally while leveraging cloud efficiencies for broader management tasks.

Required Capabilities

NHIM includes a range of controls and capabilities designed to address this growing segment. It includes the discovery, classification, provisioning, credentialing, policy enforcement, monitoring, and decommissioning of digital identities that operate without human interaction. While adjacent solutions such as secrets management, privileged access management (PAM), and certificate lifecycle management have addressed components of

this problem, NHIM introduces a unified approach to securing machine-to-machine interactions in both cloud and hybrid infrastructures. The emergence of NHIM reflects a broader evolution within identity-centric security frameworks such as Zero Trust and the Identity Fabric, where all identities are treated as subjects of governance and security controls.

The capabilities required for NHIM solutions are categorized as key capabilities, additional capabilities, and innovative capabilities.

Key Capabilities

- Non-human identity lifecycle management
- Secrets management
- Rotation and expiry
- Support for cloud and on-premises applications
- Automated and continuous discovery of NHIs
- Relationship mapping NHIs with owners
- Secure vaulting of credentials
- Integration with DevOps pipelines, CI/CD tools
- Policy-based access controls
- Support for diverse software workloads (VMs, Docker images, Kubernetes
- containers, etc.)
- Behavioral analytics and monitoring
- API and SDK support
- Auditing, reporting and dashboarding
- Connectors to identity providers and directories
- Flexible, modern software architecture and deployment

Additional Capabilities

- Service account and token governance
- Delegated administration
- Assigning dynamic risk score to NHIs based on behavior, exposure, and context
- Password synchronization
- Workflow capabilities
- Privileged Access Management capabilities
- Integration with secrets scanning tools
- Just-In-Time (JIT) secrets generation

Innovative Capabilities

- Zero Standing Privileges (ZSP) for NHIs
- Applied AI/ML for behavioral risk scoring
- Applied AI/ML for adaptive authentication
- Data access governance
- API management and security

These capabilities must align effectively across various models, ensuring comprehensive protection and adaptability to the evolving security landscape. The ability to integrate with existing systems and adapt to multi-channel environments remains a core consideration as email-based threats continue to escalate.

For information about the Leadership Compass process, see our KuppingerCole Leadership Compass Methodology

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 a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

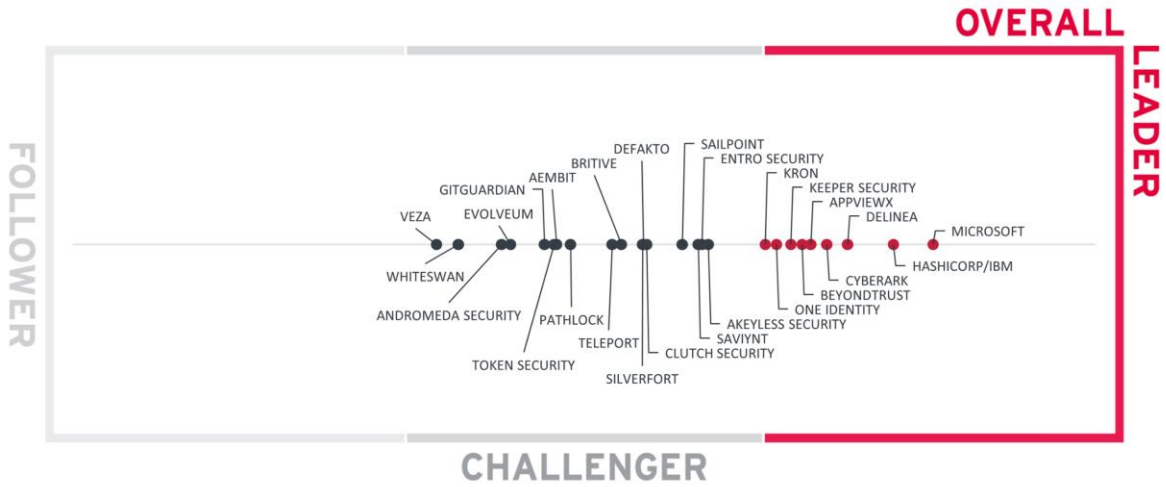


Figure 1: Overall Leadership in the Non-Human Identity Management market

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.

The NHI market is up and coming yet a fast-evolving market with a significant number of vendors. All the vendors in the rating deliver innovative solutions that are helping customers in addressing the challenges around managing NHIs. The solutions differ in breadth and depth of basic and advanced capabilities.

Among the Overall Leaders we can find AppViewX, BeyondTrust, CyberArk, Delinea, HashiCorp, an IBM company, Keeper Security, Kron, Microsoft, and One Identity. These vendors cover all the base required capabilities as well as provide advanced capabilities related to automation.

Among the Challengers, we observe the remaining 19 vendors, which includes a mix of NHI specialists, startups, unified platform providers, and established vendors. These vendors offer strong product capabilities but may lack the same level of market penetration or vice versa. Other features which are limiting these vendors is their ecosystem integration, or advanced features as compared the leaders. Many of these challengers are evolving rapidly and could shift into the leadership segment with continued innovation and product enhancements.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- AppViewX
- BeyondTrust
- CyberArk
- Delinea
- HashiCorp, an IBM company
- Keeper Security
- Kron
- Microsoft
- One Identity

Product Leadership

Product leadership is the first specific category examined below. This view is mainly 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.

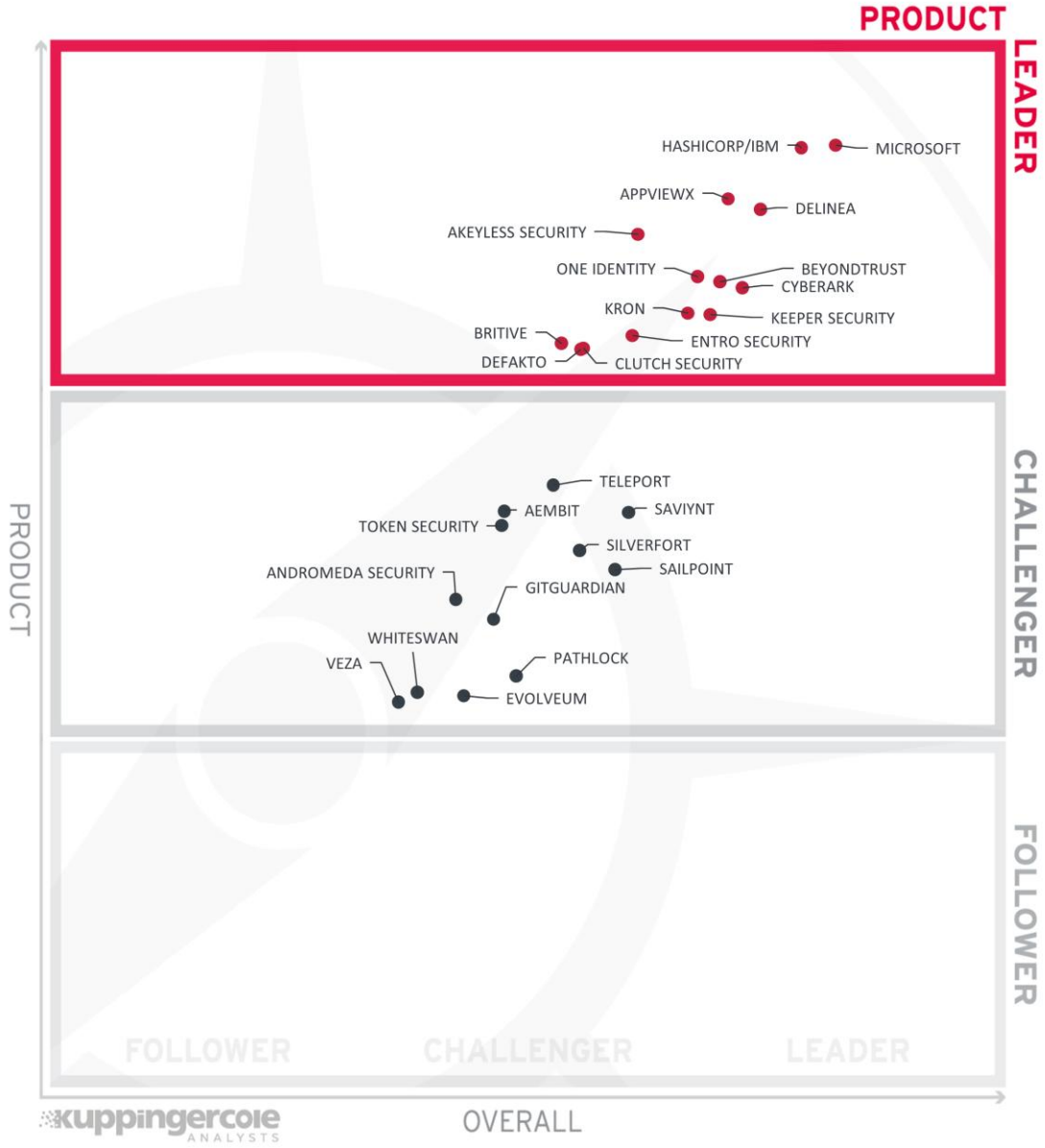


Figure 2: Product Leadership in the Non-Human Identity Management market

Among the Product Leaders we can find a mix of established IAM vendors as well as the emerging NHI specialists. These vendors have all the major required capabilities and are evolving and innovating at a rapid pace. They have strong capabilities in NHIM, DevOps and CI/CD integration, analytics, automation and intelligence and audit, monitoring and compliance.

The other vendors, many of them being specialist vendors and start-ups as well as established IAM vendors 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.

Product Leaders (in alphabetical order):

- Akeyless Security
- AppViewX
- BeyondTrust
- Britive
- Clutch Security
- CyberArk
- Defakto
- Delinea
- Entro Security
- HashiCorp, an IBM company
- Keeper Security
- Kron
- Microsoft
- One Identity

Innovation Leadership

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

This view is mainly 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 Non-Human Identity Management market

Innovation Leaders are those vendors that deliver cutting-edge 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 looking over the horizon to bring advancements to help their customers.

Microsoft again takes the top position here as the innovation leader, closely followed by HashiCorp, an IBM company. Delinea is a distance from the top two vendors, however it is rapidly developing with strong items on its roadmap. The other vendors which are towards

the end of the leaders' segment are Akeyless Security, AppViewX, BeyondTrust, CyberArk, Entro Security, Keeper Security, and One Identity.

In the Challenger section, we find the other vendors, spread across the section. These vendors lack some advanced features as the leaders. Many of these challengers are evolving rapidly and could shift into the leadership segment with continued innovation and product enhancements. A number of the vendors in the Challenger section already have been the subjects of KuppingerCole Rising Star reports, indicating strong innovation in a particular segment of the market and a strong product/market fit. These vendors are not yet Leaders in the NHI 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.

Innovation Leaders (in alphabetical order):

- Akeyless Security
- AppViewX
- BeyondTrust
- CyberArk
- Delinea
- Entro Security
- HashiCorp, an IBM company
- Keeper Security
- Microsoft
- One Identity

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, 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 Non-Human Identity Management Market

The market leaders in this space are mainly established IAM vendors and Hyperscalers. Microsoft and CyberArk take the first two spots in the innovation leadership closely followed by SailPoint, BeyondTrust, Delinea, and HashiCorp, an IBM company. Saviynt and Keeper Security complete this list.

In the Challenger area, Pathlock, Silverfort, Kron, One Identity, Evolveum and AppViewX are placed as growing players in the NHI market. There is a big cluster of vendors in the bottom half of the challenger segment. This is mainly the emerging vendors in the NHI market. These companies offer competitive solutions but lack global reach or do not have enough

enterprise customer base using their products. However, they are gaining traction as organizations seek more agile and cloud-native entitlement management solutions.

Andromeda Security, Token Security and Whiteswan complete the follower segment.

Market Leaders (in alphabetical order):

- BeyondTrust
- CyberArk
- Delinea
- HashiCorp, an IBM company
- Keeper Security
- Microsoft
- SailPoint
- Saviynt

Product/Vendor evaluation

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

Spider graphs

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

NHI Lifecycle Management: Capabilities for managing the full lifecycle of NHIs from creation and registration to rotation, revocation, and deprovisioning. This includes the ability to assign ownership, apply policy, and ensure secure and automated transitions throughout the identity's operational phases.

Architecture & Deployment: Architectural principles and delivery models supported by the solution, including SaaS, on-premises, container-based, and hybrid deployments. Evaluates the flexibility, scalability, and modularity of the system as well as support for microservices, APIs, and infrastructure extensibility.

Secrets Management: Centralized management of credentials and secrets associated with NHIs, including API keys, tokens, certificates, SSH keys, and passwords. Includes capabilities for generation, storage, access control, rotation, revocation, and secretless or ephemeral credential workflows.

Audit, Reporting & Compliance: Capabilities for tracking and logging access, usage, and policy enforcement related to NHIs and associated secrets. Includes support for audit trails,

compliance reporting, dashboarding, integration with SIEM tools, and alignment with regulatory or internal audit requirements.

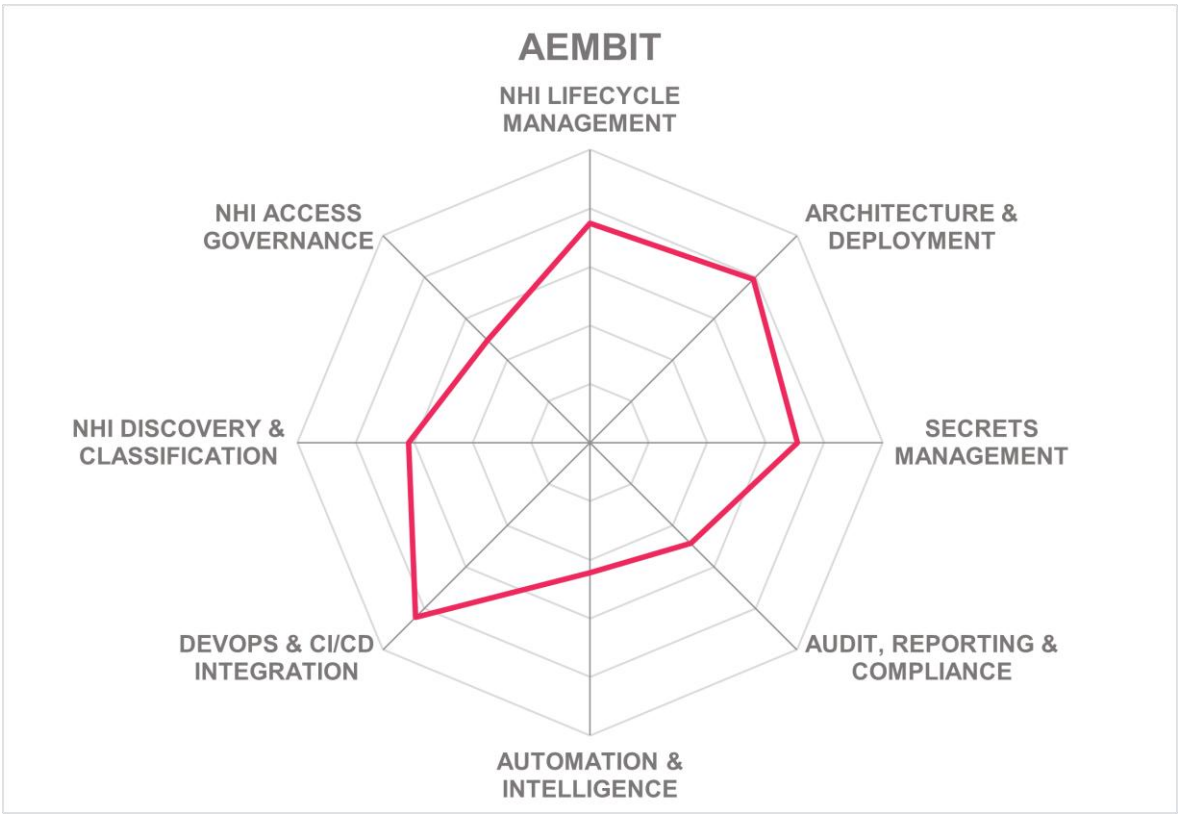
Automation & Intelligence: Use of policy-driven automation and applied intelligence to streamline the management of NHIs. This includes behavioural analytics, risk scoring, automated remediation, anomaly detection, and AI/ML-enhanced decision-making for lifecycle and access control operations.

DevOps & CI/CD Integration: Integration with DevOps tools, pipelines, and CI/CD platforms to enable secure, programmatic management of NHIs. Includes plug-ins or native support for tools like Jenkins, GitHub Actions, Terraform, Kubernetes, and infrastructure-as-code workflows.

NHI Discovery & Classification: Automated discovery of NHIs and related credentials across infrastructure, cloud, and code repositories. Includes classification based on identity type, criticality, usage, or compliance posture, helping organizations to identify unmanaged or orphaned identities.

NHI Access Governance: Capabilities that enforce access control for NHIs. Includes mapping identities to resources, owners, and roles; defining and enforcing least privilege; and implementing controls such as Zero Standing Privileges (ZSP), just-in-time access, and delegated administration.

Aembit – Aembit Workload IAM Platform



Aembit, established in 2021, is a privately held, venture-backed company based in North America. The company primarily serves the North American market, with plans to expand geographically. Aembit's flagship product is the Aembit Workload IAM Platform, which focuses on managing identities and access for non-human entities. The platform can be deployed across various environments, including on-premises, public, and private clouds, as well as hybrid configurations. Licensing is typically offered on a per-node and per-transaction basis.

Aembit adeptly manages nearly all types of NHIs, supporting extensive lifecycle activities such as discovery, inventory, classification, and posture management. The platform also addresses machine identities by providing mechanisms like workload identity federation and service account scoping. Their solution’s main function is a policy engine that allows security teams to control access from AI agents and workloads to sensitive data and resources. This is done through identity-based policies and just-in-time delivery of credentials. Their solution also supports just-in-time identity creation and infrastructure-as-code (IaC) integrations. Its platform facilitates cloud identity support, enabling integration with major cloud providers like AWS, Azure, and GCP.

Aembit's platform offers robust support for sidecar injection and serverless functions, with an emphasis on API support. SDKs for languages such as Go and JavaScript are available,

enabling deeper developer integration. The platform's DevOps and CI/CD integrations, including support for Jenkins, GitHub Actions, and GitLab CI/CD, highlight its flexibility in modern development environments. This thorough support enables secure and efficient handling of secrets and identities.

Aembit's secrets management system includes dynamic secrets support and integrates with third-party vaults like AWS Secrets Manager and HashiCorp Vault. The platform ensures secrets are encrypted at rest and in transit, with role-based access controls in place. Secrets are managed with features such as automated rotation and secure storage for various types, including API keys and OAuth tokens. Aembit's approach underscores its adaptability and focus on minimizing risk.

Audit and compliance are core functionalities of Aembit's platform, offering tamper-evident logs and audit trails for NHIs. The platform integrates with SIEM platforms like Splunk for centralized log analysis. While real-time monitoring of NHI behaviour is not available, Aembit provides session-level detail for secrets access and supports lifecycle and policy enforcement reports.

Aembit's roadmap includes advanced observability, behavioural analysis, and audit applied to Agentic AI Identity and expansion of credential lifecycle management support across cloud services. The platform holds ISO/IEC 27001 and SOC 2 Type 2 certifications. Aembit demonstrates strengths in eliminating legacy security concerns while focusing on innovation, making it a viable choice for organizations aiming to improve their NHI management and security posture.

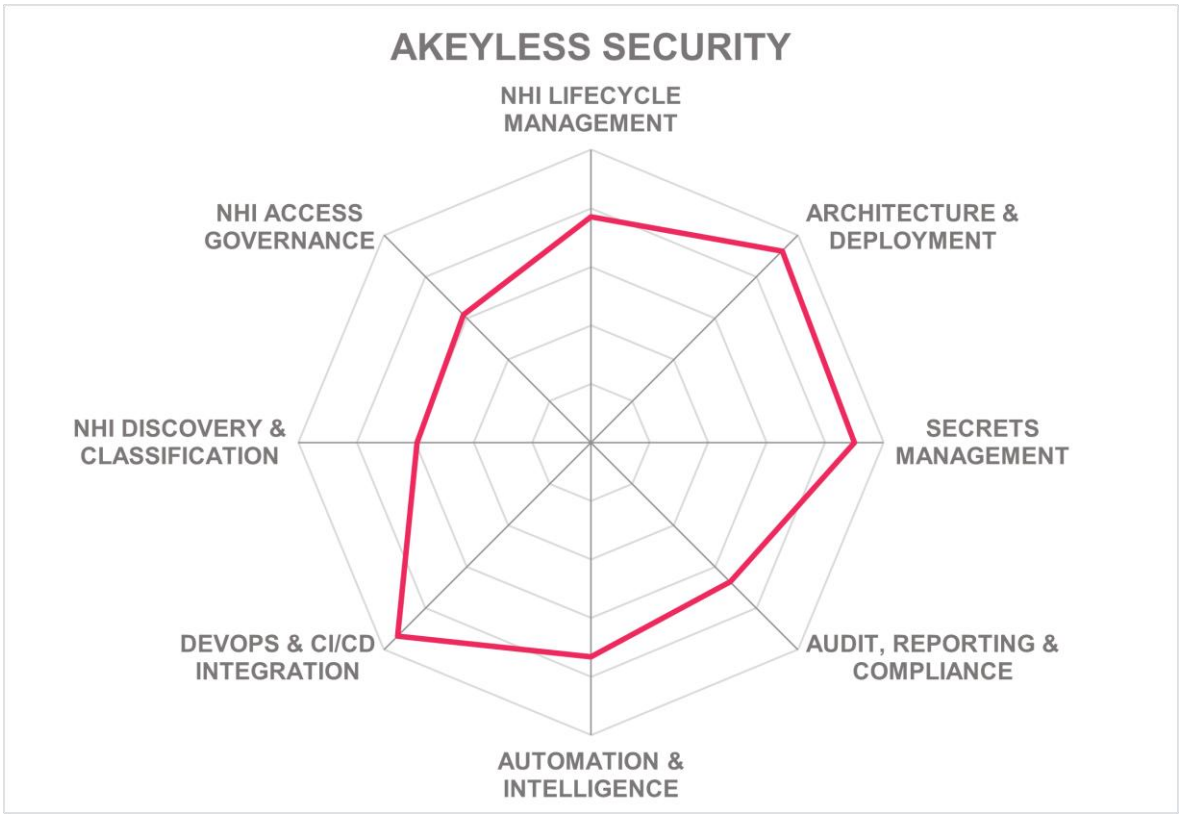
Strengths

- DevOps and CI/CD integration capabilities include injecting secrets securely into CI/CD pipelines.
- Secretless authentication and policy-driven access management reduce credential-related risks.
- Focused on securing workload-to-workload interactions, a rapidly growing security concern.
- Flexible deployment options supported.
- Supports NHI lifecycle management capabilities.
- Backing from leading cybersecurity investors, highlights industry confidence in Aembit's technology.

Challenges

- As a newer vendor, Aembit lacks market presence.
- Solution lacks several automation and intelligence capabilities.
- NHI access governance missing several important capabilities such as support for detecting orphaned accounts and adjusting privilege levels based on behavioral risk.

Akeyless – Akeyless Secrets & Non-Human Identity Platform



Leader in

Akeyless was founded in 2018 and is a privately held company backed by venture capital. It has active operations primarily in North America and EMEA. It is a SaaS-based solution. Akeyless Secrets & Non-Human Identity Platform delivers the combined functionalities of encryption, secrets management, and secure remote access. The solution is available as SaaS and can be installed in public cloud, private cloud, hybrid, and on-premises environments, facilitated by the Akeyless Gateway.

Akeyless supports most of NHI types. Their lifecycle management includes credential rotation, vaulting, and decommissioning but lacks discovery or posture management. These are planned enhancements. Akeyless supports just-in-time NHI creation and Infrastructure-as-Code (IaC) tools, while cloud ID systems are supported with integrations across major providers like AWS, Azure, and GCP. Template-based and bulk import functionalities help streamline provisioning, while delegated lifecycle management and inactivity detections aid effective oversight. The platform provides lifecycle status reporting and supports mapping identities to their respective owners.

In terms of integration, Akeyless supports sidecar injection for seamless secrets delivery in Kubernetes and managing secrets in serverless functions. It offers extensive API and SDK support across multiple languages, including Python and Java. The platform has strong capabilities for DevOps integration, supporting dynamic secret injection and broader CI/CD pipeline integration tools such as Jenkins and GitHub Actions. Well-documented APIs and CLI tools can support developers with automation capabilities without mandating hard coding of secrets.

Akeyless provides a strong secrets management system through its proprietary Distributed Fragments Cryptography (DFC™), a novel cryptographic schema leveraging Zero Knowledge principles. This ensures that no complete encryption key is ever fully visible or stored in a single location, thereby significantly minimizing exposure to attacks and improving resilience against both insider and external threats. It supports both static and dynamic secrets along with full lifecycle management and offers integration with external vaults to centralize secrets governance. The platform supports encryption, automated rotation, and credential management, with extensive compliance controls like versioning and expirations.

Akeyless supports JIT dynamic secrets capability issuing temporary, expiring credentials on demand to eradicate risks associated with long-lived credentials. Its gateway architecture offers secure access and policy enforcement without the need for secrets to transit or reside within its cloud infrastructure.

The platform's audit and compliance functionalities are mature and include detailed, tamper-evident logging which can be integrated with SIEM tools for centralized analytics. Native analytics capabilities such as anomaly detection and dynamic risk scores are currently limited; however, these are part of Akeyless' plans for future enhancements.

Akeyless plans to improve its platform through better discovery, detection, and response mechanisms by extending its machine identity management capabilities. It holds certifications such as FIPS 140-2 and ISO/IEC 27001. The platform supports incident analysis and offers remote support services with a focus on rapid response times. Akeyless' strength lies in its zero-knowledge encryption and, SaaS-native approach to identity management, positioning it as a strong player in environments managing complex, non-human identity landscapes.

Strengths

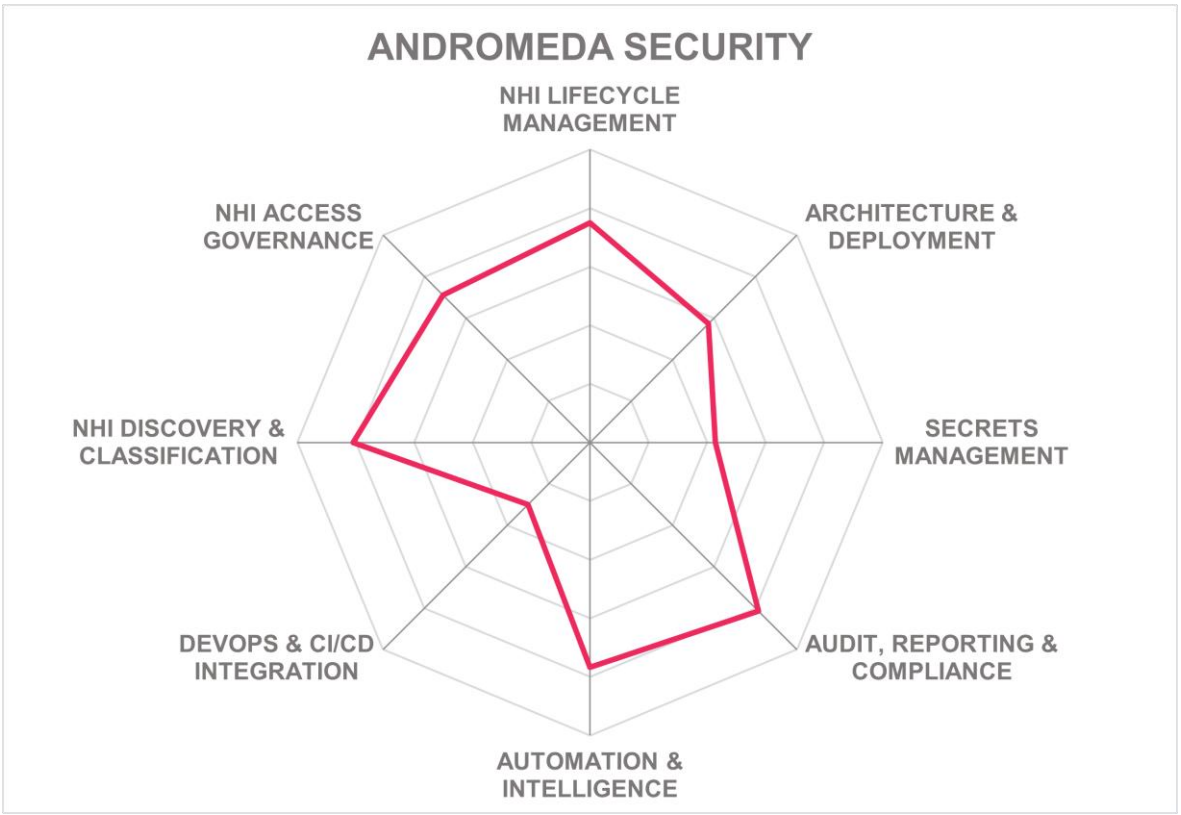
- Very good secrets and machine identity management
- Unique Distributed Fragments Cryptography technology
- Broad integration support
- Cloud, on-premises, and hybrid deployment models
- User-friendly UI with CLI/API options
- Strong focus on Zero Knowledge security principles
- Automated lifecycle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

Challenges

- Relatively new vendor with ongoing development of anomaly detection features
- Enhancement of Quantum-Safe Encryption practices required for full coverage

- Needs to improve risk posture management and contextual analysis
- Some automation and intelligence capabilities are missing but planned for roadmap in 2026
- Continuous discovery across environments is not supported but planned for 2026 roadmap

Andromeda Security – Andromeda Identity Security Platform



Andromeda Security, a venture-capital-backed company established in 2023 and based in San Franciso, USA, is a provider of NHI security solutions. Currently active in North America, its Andromeda Identity Security Platform is a cloud-native solution that supports public cloud deployments only. The platform is offered as a standalone SaaS solution, with licensing models based on human user and non-human identity counts.

Andromeda Security's platform supports management of non-human identities such as virtual machines, CI/CD tools, containers, microservices, cloud-native service accounts, integration bots, AI/ML pipelines, and various backend applications, with lifecycle events including discovery, posture management, classification, rotation, vaulting, and decommissioning. Just-in-Time (JIT) NHI creation and Infrastructure as Code (IaC) integrations are available. Andromeda Security provides good logging, metadata mapping, and identifies orphaned identities to streamline management workflows. Automated de-provisioning is supported so that unused identities do not become security risks.

Although sidecar injections are not supported, the platform manages secrets in serverless environments. It boasts full API and SDK support for Python and Go. It's architected to

enable secure secrets management within CI/CD pipelines through Terraform and AWS CloudFormation integrations.

The platform does not offer built-in secrets management, relying instead on compatible third-party vaults like AWS Secrets Manager and HashiCorp Vault. Automated secrets rotation and tagging are supported, ensuring secure, streamlined operations. Andromeda focuses on providing automated lifecycle management of secrets.

Andromeda's audit and compliance capabilities ensure non-human identity activities are well-monitored. The platform integrates with SIEM tools for centralized analysis. Behavioural analytics leverage AI/ML to detect abnormalities and adjust permissions dynamically. Identity performance and risk scores are part of Andromeda's insights portfolio, which support automated risk assessment and adaptive security measures.

Looking ahead, Andromeda plans to enhance JIT account creation and access governance functionalities. While it currently lacks major security certifications and multilingual support, the platform's unique contextual analysis and automation stand out. Organizations aiming to enhance their overall NHI security posture by managing permissions and entitlements at scale will find Andromeda's solutions well-suited to their strategic objectives. The platform excels in delivering identity security and real-time risk management.

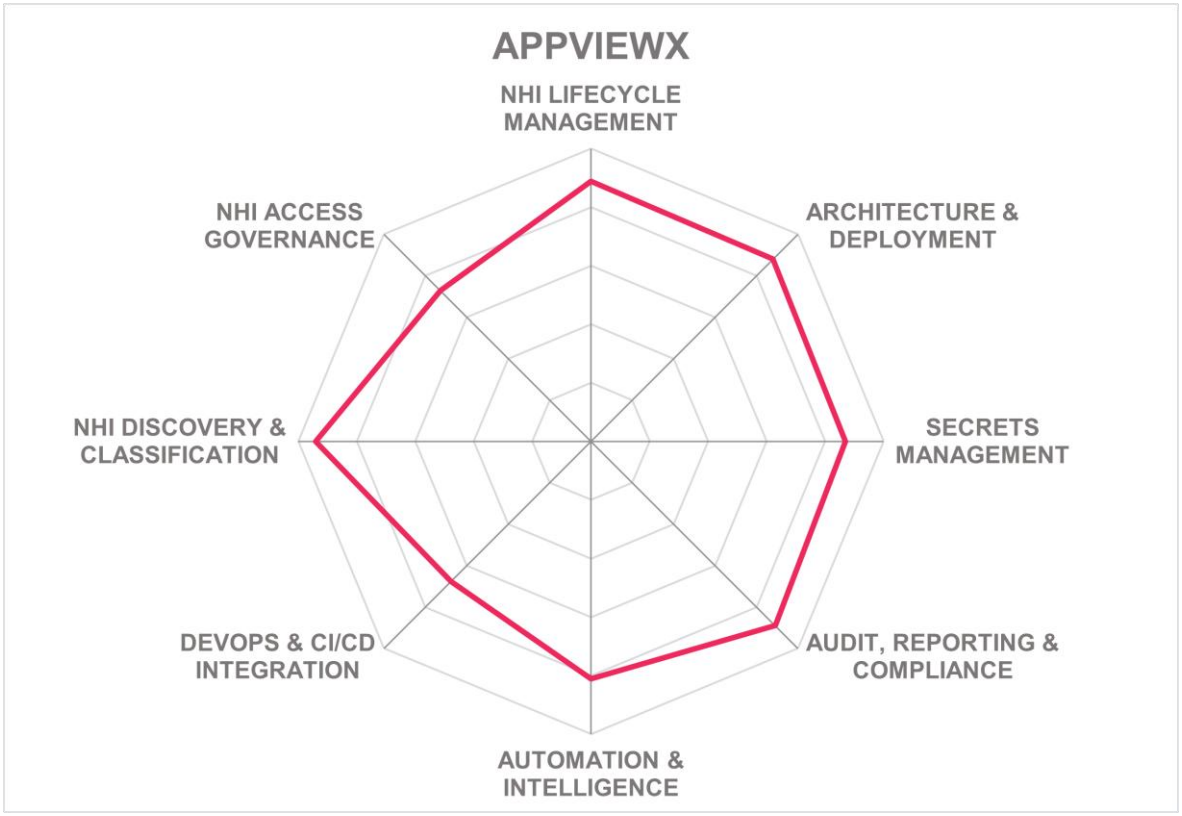
Strengths

- Extremely granular contextual mapping of identities.
- Good integration of human and non-human identity management.
- Strong support for Infrastructure as Code through Terraform and AWS CloudFormation.
- Supports JIT provisioning.
- Extensive API and SDK support for customization and integration.
- AI-driven analytics provide actionable insights into identity behaviors.
- Compatibility with leading secrets vaults.
- Continuous discovery and orphaned identity detection.
- Dynamic risk scoring adapts access controls to evolving security needs.

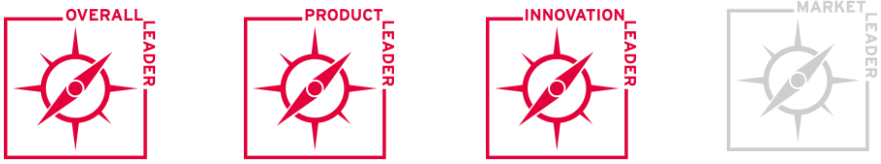
Challenges

- Secrets management is missing but planned in roadmap
- Customer presence is currently limited to USA but expansion into EU is planned for 2026
- DevOps and CI/CD integration capabilities are missing
- Integration with deeply customized legacy systems can be challenging

AppViewX – AVX ONE



Leader in



AppViewX, founded 2016 and headquartered in New York, U.S., is a strong contender especially with its capabilities in certificate lifecycle management and PKI automation. Operating with global reach from offices in New York, Boston, London, and India, AppViewX supports many active customers across numerous industries. It focuses on NHIM, addressing use cases for IoT and IIoT, cloud, and machine identities. Deployment methods are varied, supporting on-premises, public and private cloud, SaaS, virtual and container-based environments. Licensing models are flexible, aligning with customer needs via per user, transaction, time period, and node options.

The AVX ONE platform supports a wide range of non-human identities, including virtual machines, CI/CD tools and pipeline agents, containers, microservices, web and backend applications, service-mesh components, mobile applications, cloud-native service accounts, integration bots, AI/ML pipelines, IoT devices, connected edge systems, custom automation scripts, API clients, and various devices. Its lifecycle management capabilities extend from discovery and status reporting to inactivity detection and automated de-provisioning. The

platform supports JIT identity creation and IaC integrations, ensuring compatibility with major cloud providers like AWS, Azure, and Google Cloud Platform. Custom workflows, policy templates, and metadata-driven insights contribute to NHI governance.

AppViewX provides sidecar injection, serverless function management, and strong API availability, including REST and SCIM protocols. The platform offers SDKs across multiple programming languages and support for DevOps environments, integrating with popular CI/CD tools like Jenkins and GitLab. It emphasizes secure secret handling but does not support dynamic secrets injection into builds or automated secret provisioning within CI/CD jobs.

AppViewX's approach to secrets management includes built-in secrets protection, securing API keys, tokens, and credentials. It offers encrypted storage and rotation of secrets, with integration capabilities for external solutions like AWS Secrets Manager and HashiCorp Vault.

AppViewX facilitates audit and compliance by enabling exhaustive logging of NHI activities and lifecycle events such as supporting detailed audit trails and reporting capabilities, while its secrets vault supports customer-managed encryption keys and provides logging and access scoping by role, application, and environment, emphasizing a strong commitment to granular control and security. The solution integrates with SIEM platforms like Splunk and IBM QRadar. Though it lacks a behavioural analytics engine, it facilitates identity lifecycle monitoring and supports risk-based access policies.

AppViewX's plans to target compliance-driven use cases and AI-centric identity management in its technical roadmap. AppViewX has achieved ISO/IEC 27001, SOC 2, and PCI DSS certifications. Incident response support is available 24/7 globally. Documentation and support are provided in English. AppViewX's holistic approach makes it well-suited for organizations requiring extensive NHI lifecycle management with strong integration capabilities.

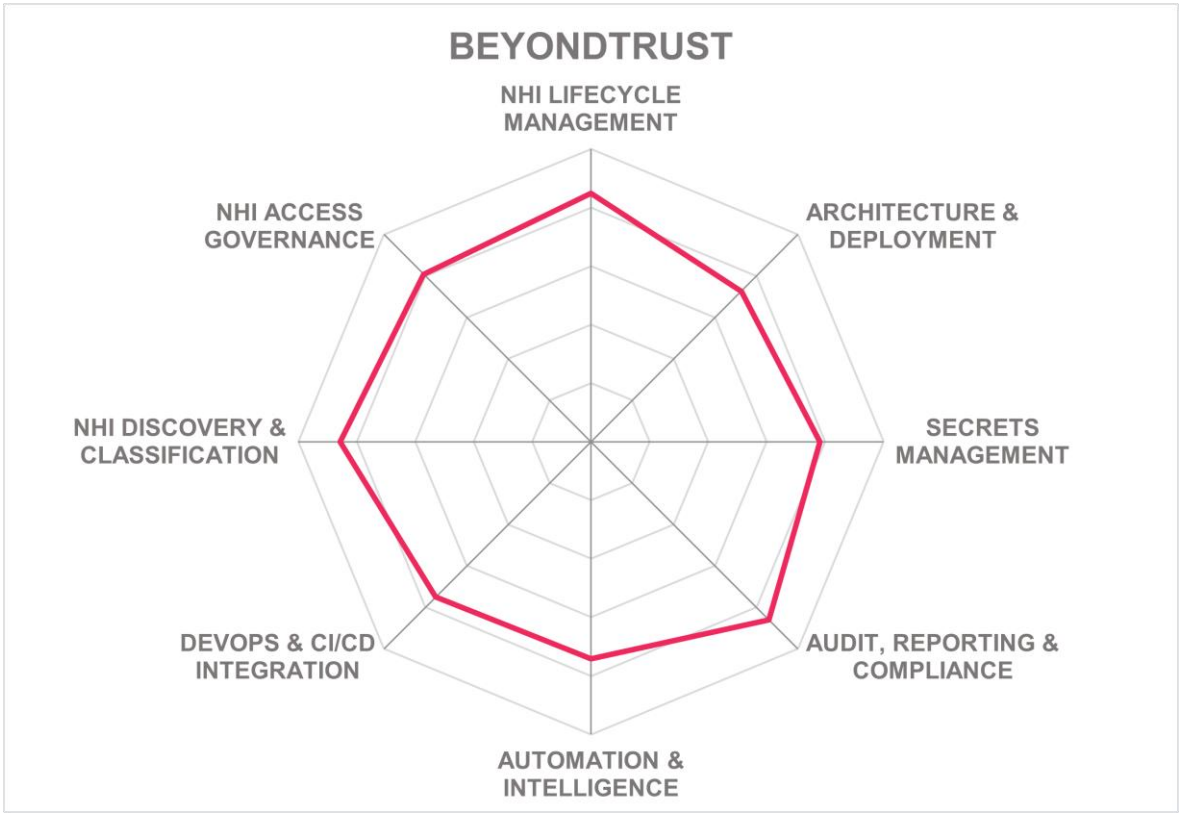
Strengths

- Certificate lifecycle management.
- Strong NHI discovery and classification capabilities.
- Closed-loop automation framework that integrates discovery, orchestration, and remediation
- Broad integration capabilities with major cloud providers (AWS, GCP), CI/CD tools (Jenkins, GitHub), ITSM platforms (ServiceNow)
- Good NHI management.
- Advanced intelligent discovery features.
- Excellent crypto-resilience tracking.
- Good audit, reporting and dashboarding capabilities

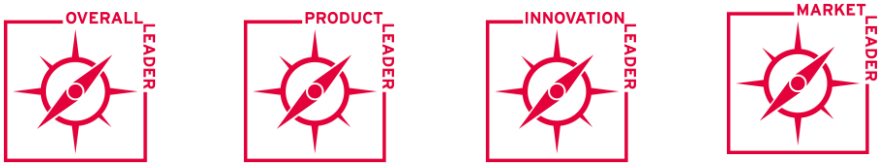
Challenges

- Some analytics capabilities are missing such as a behavioral analytics engine and evaluating risk scores based on context.
- Some DevOps CI/CD integration capabilities are missing such as injecting secrets into CI/CD pipelines.
- Support for some SDKs and container-based platforms is missing.

BeyondTrust – Pathfinder Platform



Leader in



BeyondTrust, established in 2003, remains a privately held entity without venture capital backing. The company is headquartered in the United States and is extensively engaged across North America, EMEA, APAC, and Latin America. BeyondTrust's product suite focuses on privileged identity protections, from access management to endpoint security. Their deployment options are expansive, supporting on-premises, public and private clouds, as well as managed services.

BeyondTrust addresses a broad range of NHIs and supports managing the entire lifecycle from discovery and inventory to posture management and decommissioning. Their machine identity capabilities ensure credential and secrets protection. The solution supports Just-In-Time (JIT) creation and integrates with infrastructure-as-code tools for streamlined processes. With broad support for major cloud platforms, BeyondTrust facilitates customizable onboarding workflows and delegated lifecycle management. Enhanced reporting and metadata enrichment boost their lifecycle management functionality, enabling thorough identity mapping and monitoring.

BeyondTrust enables integration with container orchestration systems to deliver secrets securely. The platform offers extensive API capabilities, SDKs for multiple programming languages, and robust DevOps integrations, including CI/CD pipeline support. The robust CLI and extended support for Docker and Kubernetes environments ensure smooth operational workflows and enhanced automation capabilities crucial for modern IT infrastructure.

BeyondTrust provides an integrated system facilitating secure storage, management, and rotation of secrets across various endpoints. Their hardened vault supports a wide array of secret types, ensuring complete lifecycle and access management. By leveraging a zero-trust architecture, BeyondTrust employs strong authentication methods like MFA and FIDO2 to maintain security integrity.

The company's Identity Security Insights tool provides a full view of NHIs, ranging from service accounts and service principals to AWS access keys. Identity Security Insights is implemented as microservices and delivered as SaaS to the customers. As they pivot toward ephemeral credentials management, BeyondTrust's insights technology is not only built upon but also enhances the existing ITDR landscape, ensuring clients have visibility, control, and governance over their identity infrastructures.

BeyondTrust's approach includes integrated AI insights designed to address complex security patterns, such as identifying rogue AI agents and managing service accounts that require rotation or other interventions. BeyondTrust offers visibility across the entire identity fabric.

Looking forward, BeyondTrust aims to enhance capabilities in NHI and secrets management with upcoming advancements in cloud and AI integration. BeyondTrust has obtained ISO/IEC 27001 and SOC 2 Type 2 certifications. By leveraging significant strengths in identity and access control, it remains well-suited for enterprises looking to secure NHIs efficiently.

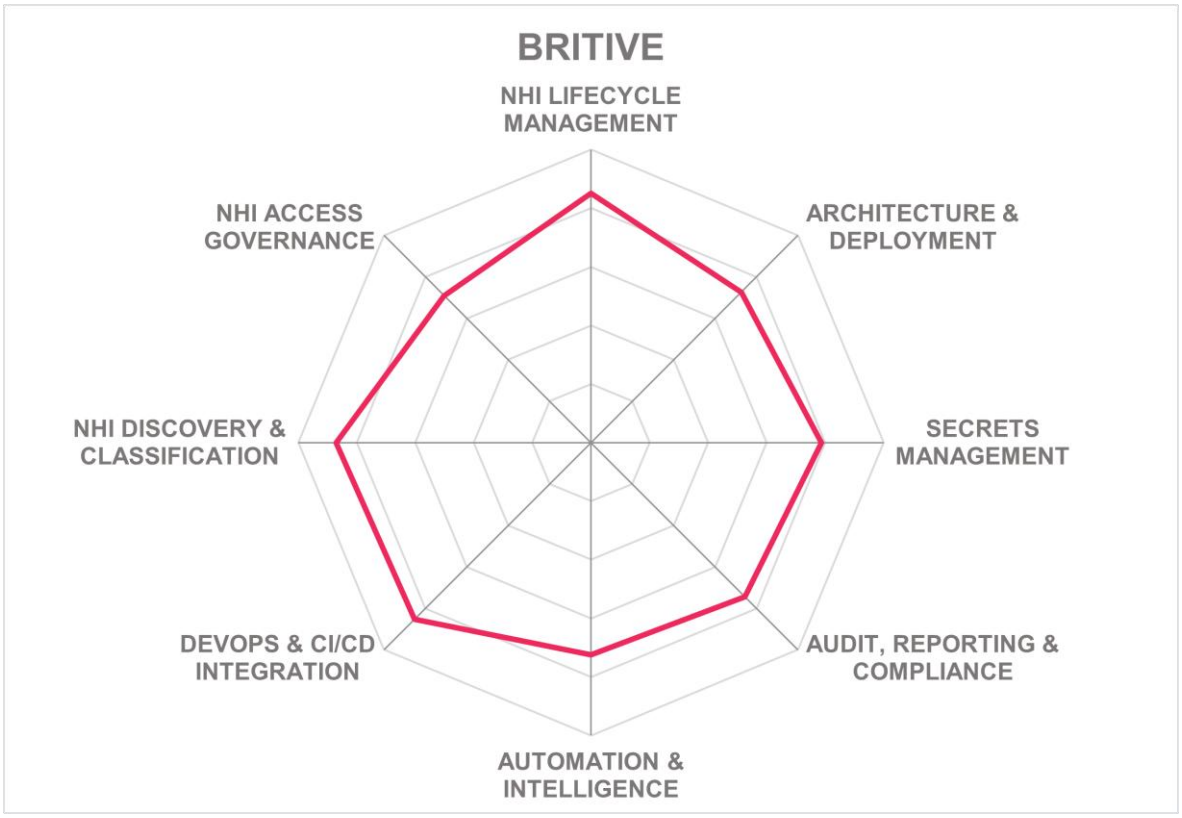
Strengths

- Visibility across multiple identity environments with support for many identity types.
- Supports real-time decision-making and risk management for identity security.
- Flexible deployment options supported.
- Extensive secrets management capabilities.
- Strong presence in the ESM and NHI market.
- Secrets vault provided.
- Supports reports for wide range of major compliance frameworks such as GDPR, HIPAA, NIST, etc.

Challenges

- Support for ultra-customized legacy environments could pose operational challenges.
- Some DevOps and CI/CD integration capabilities are missing.
- Some advanced automation and intelligence capabilities are missing but planned in roadmap.
- Adaptive authentication for NHIs is missing.

Britive – Britive Cloud Identity Security Platform



Leader in

Britive, founded in 2018, and based in US is a venture-backed company specializing in PAM solutions for cloud, on-premises and hybrid environments. It offers a cloud-native solution designed to provide automated entitlement governance, identity risk mitigation, and temporary privilege escalation across AWS, Azure, Google Cloud, Oracle Cloud Infrastructure and multiple SaaS applications. Britive provides support for human, machine (and other NHI types), and agentic AI identities. Britive has leveraged its core technology, the Just-in-Time (JIT) Zero Standing Privilege (ZSP) access platform, to support identity management across multi-cloud and hybrid environments. Britive utilizes a licensing model based on per identity managed annually, with differing rates for human and non-human identities.

Britive's platform supports managing a wide range of NHIs across various environments and addressing key lifecycle elements. It supports JIT creation and provisioning via IaC, integrates with major cloud identity systems, and provides adaptable workflows and templates.

The Britive platform unifies human, non-human, and Agentic AI identities in a single control plane enhanced by a shared policy framework. Britive supports real-time, policy-enforced access management and visibility across infrastructures.

Britive's platform does not support sidecar and serverless integrations but does provide extensive API support and SDK support in Python. For DevOps and CI/CD integration, Britive provides a CLI tool and native integrations with popular tools such as Jenkins, GitHub Actions, and GitLab CI/CD. This integration supports secure secrets injection, automation of policy management, and role-based access controls within CI/CD workflows.

In terms of secrets management, Britive offers an integrated enterprise-grade vault for secure storage of various secret types such as SSH keys, API tokens, and encrypted data. Secrets are encrypted both at rest and in transit, with configurable, role-based access policies. Moreover, the platform includes capabilities for fine-grained policy control, versioning, and expiration management to ensure secure secrets handling and usage.

Britive provides audit and compliance capabilities with detailed logging and monitoring to aid security analysis. However, it does not detect anomalies in the logs. Britive's platform includes audit trails for NHIs, associating secret access with workload origins and full lifecycle event logging. The platform also enables automated workflows for remediation. However, its analytics are not currently enhanced with ML detection models

Moving forward, Britive aims to enhance its platform with ML-based anomaly detection. Britive has to SOC Type 2 certification. It does not currently offer language support beyond English. Britive’s strengths lie in its API-first approach and cross-platform identity management capabilities, though its analytics and AI/ML functionalities remain under development. Its platform is particularly suitable for organizations within North America that are seeking NHI security, particularly for DevOps environments.

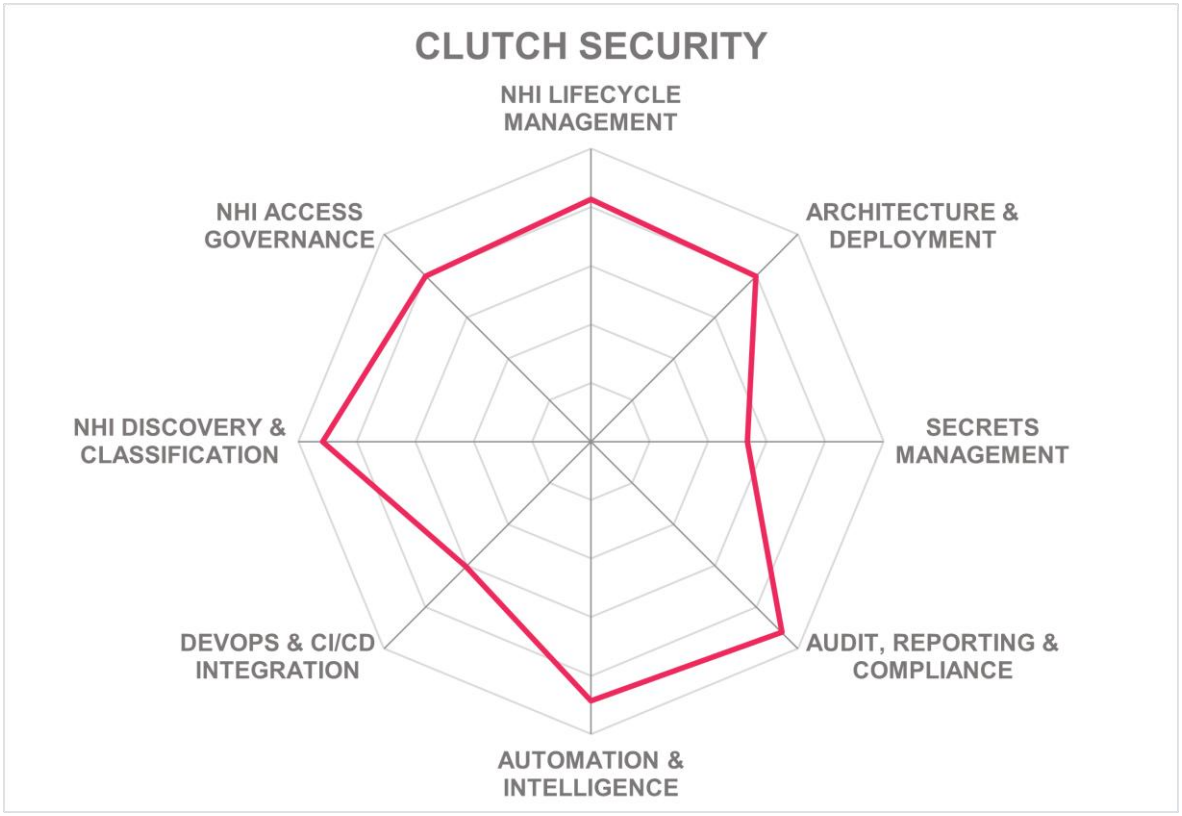
Strengths

- Modern zero trust identity security and privileged access management integration for NHIs.
- Core technology is focused on JIT Zero Standing Privilege (ZSP) to remove unnecessary privileges.
- Strong NHI discovery and classification capabilities.
- Excellent visibility and lifecycle management across cloud, hybrid, and on-prem environments.
- API-first design enables integration with existing enterprise systems and workflows.
- Very good DevOps and CI/CD integration capabilities.

Challenges

- AI/ML features for enhanced risk analysis, dynamic risk scoring, and automated remediation workflows are not available
- Missing support for NHI decommissioning and detection and response.
- Market presence is currently limited to mainly North America
- Does not offer secret scanning capabilities

Clutch Security – Universal Non-Human Identity Security Platform



Leader in

Founded in 2023, and based in Tel Aviv, Israel, Clutch Security is a specialized player in the field of NHI Lifecycle Management. Their Universal Non-Human Identity Security Platform is delivered as a managed SaaS solution with deployment options spanning public and private cloud environments, including on-premises installations. Licensing is flexible, covering per-user, per-time period, and per-server models.

Their Universal Non-Human Identity Security Platform manages a wide range of non-human identities, including virtual machines, CI/CD tools, containers, microservices, web and backend applications, service-mesh components, mobile applications, cloud-native service accounts, integration bots, AI/ML pipelines, and various API-related identities like access keys, tokens, and managed identities. The platform supports lifecycle activities such as discovery, inventory, posture management, and monitoring. JIT creation and IaC are not currently supported.

Clutch's proprietary Identity Lineage technology provides a unique capability to map and understand the relationship between NHIs in order to understand identity dependencies and

ownership attribution. This is complemented by Clutch's Zero Knowledge Architecture the prevents secrets from leaving customer networks.

It supports cloud-native integration across AWS, Azure, and GCP, facilitating workflows customizable by identity through a Governance Policy Engine. The system supports delegated lifecycle management and provides versatile import capabilities, enriched metadata, and extensive mapping features for improved identity management.

Clutch does not provide sidecar support but does have extensive capabilities for API integrations via REST and GraphQL, though it currently lacks SDKs. The platform integrates with DevOps and CI/CD tools through native plugins for Jenkins and GitHub Actions and can scan for secrets within Docker files and IaC templates.

In terms of secrets management, Clutch interfaces with existing vaults, including AWS Secrets Manager and HashiCorp Vault, but does not have its own dedicated vault. Automated risk and behavioural analysis which is powered by ML algorithms to detect anomalies and potential threats.

Clutch Security offers extensive audit, compliance, and monitoring capabilities for managing NHIs. Logs are cryptographically signed to ensure integrity and to provide an audit trail of lifecycle events. The platform supports automated remediation, privilege escalation detection, and integrates with SIEM platforms such as Splunk and Microsoft Sentinel. Customizable alerts and dashboards provide real-time insights into identity behaviour, access events, and policy violations.

The platform delivers contextual intelligence and prioritization by leveraging advanced ML and behavioural analytics to continuously monitor NHIs and detect anomalies. This is supported by Clutch's Zero Trust Engine which adapts to organization-specific security patterns and provides AI-driven remediation workflows with automated response orchestration through SOAR.

Clutch plans to expand its AI/ML capabilities and integration with DevSecOps toolchains. The planned features include enhanced shadow AI detection and advanced compliance automation. The platform currently holds ISO/IEC 27001 and SOC 2 Type 2 certifications, ensuring its commitment to security. With a focus on providing around-the-clock incident support and offering documentation in English and Hebrew, Clutch poses a noteworthy option for NHI security management for diverse operational environments while addressing modern security challenges.

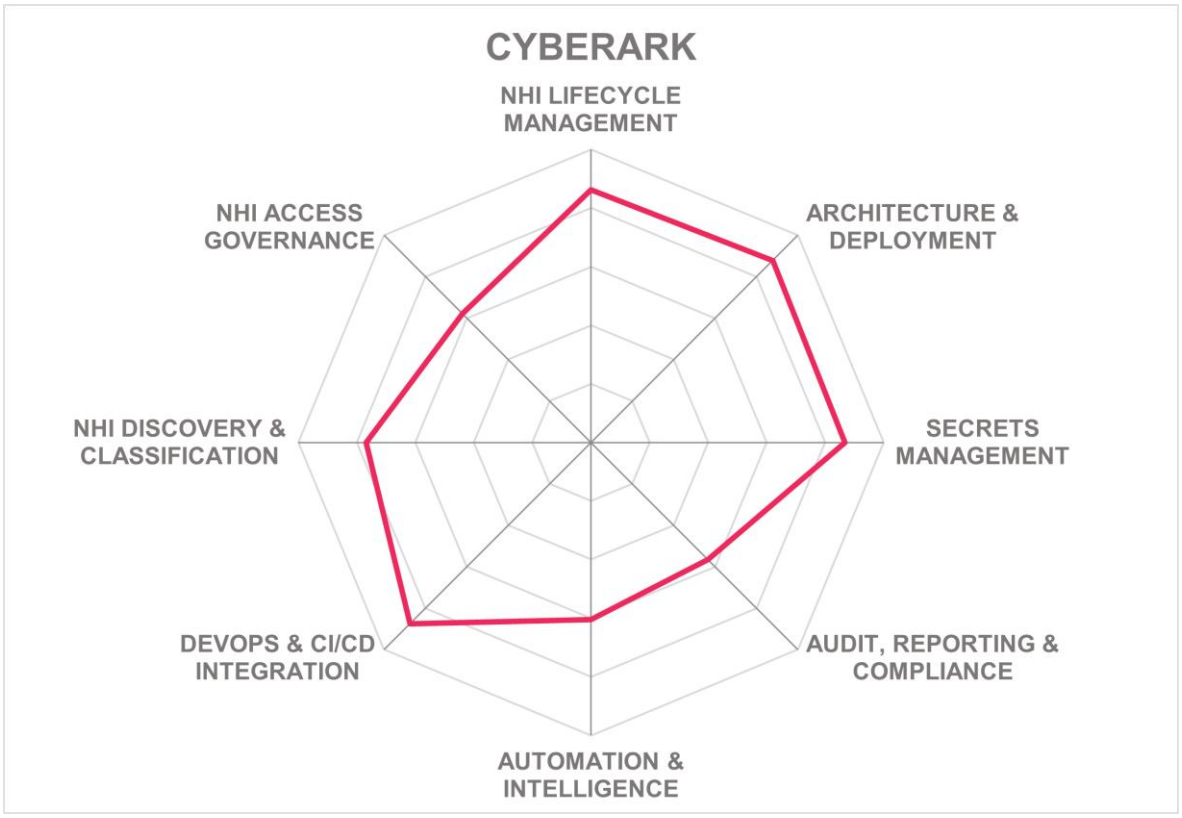
Strengths

- Unique Identity Lineage technology offers deep insights into NHI relationships and ownership.
- Wide range of supported NHI types with excellent lifecycle management capabilities.
- Scalable microservices-based Zero Knowledge architecture with API-first integration.
- Advanced ML-powered behavioral analytics for real-time anomaly detection and adaptive security measures.
- Good support for audit and monitoring.
- Integration with major cloud providers and CI/CD tools enhancing universal platform coverage.

Challenges

- Relies on third-party integrations for secrets management.
- Support for SDKs is missing but planned in roadmap.
- Limited market presence.

CyberArk – CyberArk Identity Security Platform



Leader in

CyberArk, founded back in 1999 with U.S. headquarters in Newton, Mass., is one of the leaders in the NHI market, consistently holding leadership positions in product, market, innovation, and overall leadership. CyberArk focuses on identity security, offering a wide range of products through the CyberArk Identity Security Platform, which encompasses solutions for privilege access management, endpoint security, and NHI management. The deployment options for these solutions include software installed on customer premises, SaaS, and containerized environments, supporting various public and private cloud ecosystems. The deployment options for these solutions include software installed on customer premises, SaaS, and containerized environments, supporting various public and private cloud ecosystems. Among its offerings, the company employs diverse licensing models, such as subscriptions and modular licenses. Palo Alto Networks, a leading cybersecurity stack vendor, agreed to acquire CyberArk in July 2025.

This platform provides identity security controls for human, machine, workload, and other NHIs, which was facilitated through its strategic acquisition of Venafi in late 2024, a certificate management and machine identity specialist. CyberArk's NHI security capabilities include securing all secret types, certificates, and workload access, to enable customers to centrally manage NHIs across their lifecycles and entire enterprise infrastructure.

CyberArk supports sidecar injection and management of serverless architectures in addition to automated secrets rotation. API authentication mechanisms include JWT, OAuth, OIDC, and key exchange. SDKs extend compatibility across diverse programming environments such as Python, Java, .NET, Android, iOS, JavaScript, Ruby and Go. The solution integrates with DevOps and CI/CD pipelines, and has tools to inject secrets, support automation, and synchronize identity management across these workflows.

The secrets vault supports policy-based access. Moreover, secrets vaulting includes fine-grained policy controls. They have also integrated zero trust authentication for secrets management, which constantly verifies identities based on cryptographic proof and workload identity attributes instead of just tokens.

CyberArk logs all NHI lifecycle events and integrates with SIEM systems. Its platform provides auditing and forensic capabilities for effective incident response and compliance tracking.

CyberArk CORA AI is an advanced component of the CyberArk Identity Security Platform that leverages generative AI for detection and response capabilities. It supports natural language processing to simplify user interaction and supports dynamic adjustments to security controls based on behavioural analysis. It supports session analysis and anomaly detection for machine identities.

CyberArk's strategic roadmap includes integrations with additional secret management solutions such as HashiCorp Vault. Although the HashiCorp vault integration was recently released, with the recent acquisition, there could be delays with addressing roadmap. Their certifications include US FedRAMP, SOC 2 Type II, and compliance with standards like FIPS 140-2 and ISO/IEC 27001. Multi-language support includes English, Spanish, and Japanese, further strengthens customer engagement. CyberArk's strengths lie in its approach to identity security, covering both human and machine identities, making it a suitable choice for organizations requiring robust security solutions across complex IT environments.

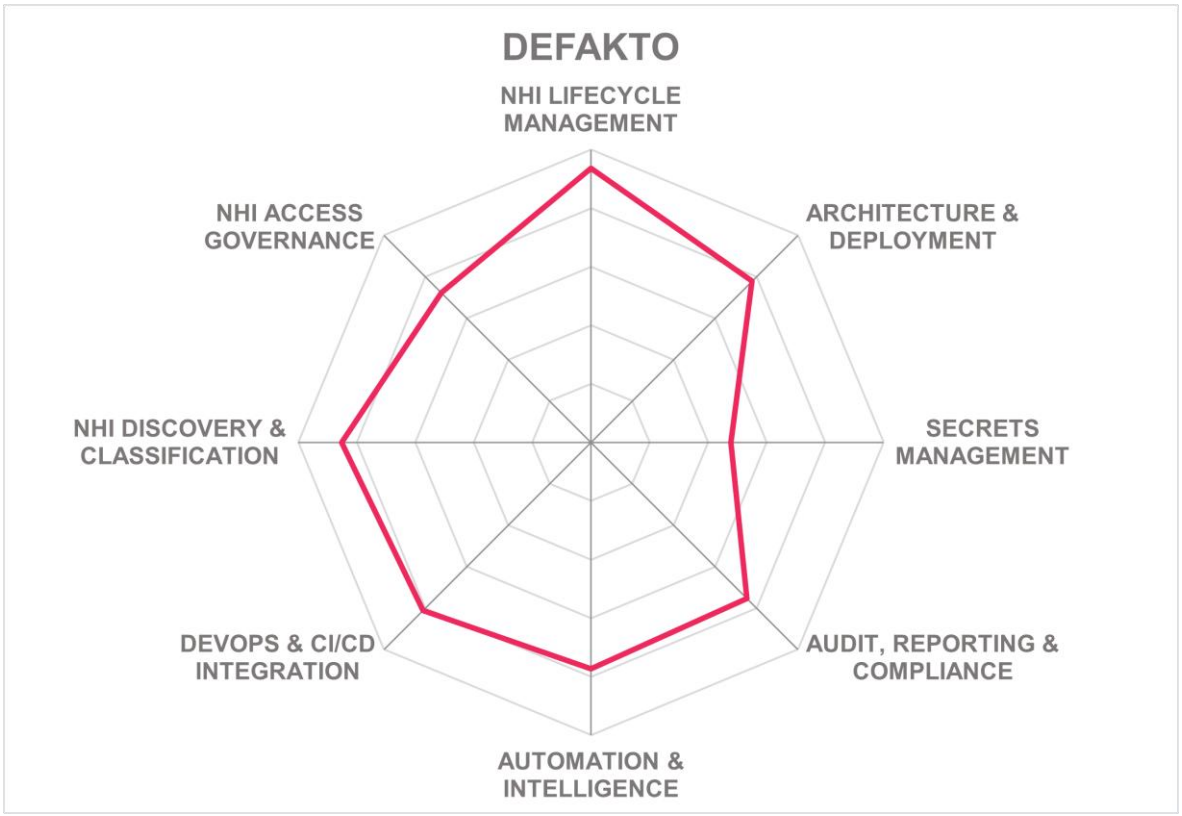
Strengths

- Strong coverage of NHIs across cloud and on-premises.
- Advanced AI capabilities with CORA AI for enhanced identity threat detection and response.
- Zero-trust security model for workload access and secrets management.
- Extensive partner ecosystem with over 1,000 integrations and 350+ C3 Alliance partners.
- Automated lifecycle management for secrets and certificates.
- Strong market presence with significant customer base.
- Strong DevOps and CI/CD integration capabilities

Challenges

- Does not provide reporting on NHI lifecycle status
- Does not detect privilege overlap among NHIs
- Real time monitoring of NHI behavior not yet available but included in 2026 roadmap.
- Some advanced tracking and automation capabilities are missing

Defakto – Non-Human IAM Platform



Leader in

Defakto, founded in 2022 and based in California, USA, operates as a privately held company with venture capital backing. The company is engaged across North America and the EMEA regions however, it has a very low number of active customers. Originating from the creators of the SPIFFE standards, Defakto‘s solution addresses dynamic and ephemeral credentials for machine identities. Licensing is available per node or workload, supporting both on-premises and SaaS deployments.

Defakto is a hybrid SaaS-delivered but is containerized and can run on-premises as well. The solution is a microservices-based architecture and is infrastructure agnostic, supporting Docker, Red Hat, and Rancher Labs. This enables customers to eliminate the requirement for standing access credentials.

Defakto's solution manages all types of NHIs, including machine identities, such as VMs, containers, AI agents, and CI/CD pipelines. It addresses key lifecycle activities such as discovery, classification, posture management, and rotation. Defakto features customizable workflows, detection of inactivity, and automated de-provisioning. The platform supports JIT creation and IaC and integrates with cloud-native identity systems in AWS, Azure, and GCP. Dashboards include status reporting.

The Defakto platform supports sidecars and serverless environments to enable no code/low-code deployments, along with SDKs for application integration. All features are available through API access, including REST and gRPC. SDKs are available for the Go, Java, Python, C/C++, C#, and Rust languages. Defakto integrates with Jenkins and GitLab CI/CD, allowing dynamic injection of secrets and automatic provisioning of NHIs. These functions enhance pipeline security without writing secrets to disk.

Defakto does not operate a traditional secrets management system or vault but instead focuses on creating short-lived, ephemeral identities. The platform integrates with third-party secrets vaults such as AWS Secrets Manager, Azure Key Vault, and HashiCorp Vault. Defakto can inject temporary identities into applications and workloads such as containers, virtual machines, AI agents, and CI/CD pipelines at runtime.

Defakto supports secure logging, tracks lifecycle events, and provides detailed session-level monitoring. The solution integrates with SIEM platforms like Splunk. Defakto offers behaviour tracking and risk scoring for NHIs by monitoring activity patterns. Dynamic risk assessments are supported to inform access permissions. Additionally, Defakto supports automated approvals and uses organizational-specific behaviour patterns to enforce policies at runtime based on context.

Enhancements in detection and remediation of secrets in cloud environments are planned. Defakto has not been certified for ISO 27001, however they are SOC Type 1 certified and SOC 2 Type 2 is planned. The solution has analysis and remediation services for incident response. Defakto serves industries primarily within the retail and finance sectors. There are also a few functional gaps. Secrets management capability is missing but included in the product roadmap. These factors should be considered when assessing the suitability of Defakto for specific security-sensitive or compliance-driven environments.

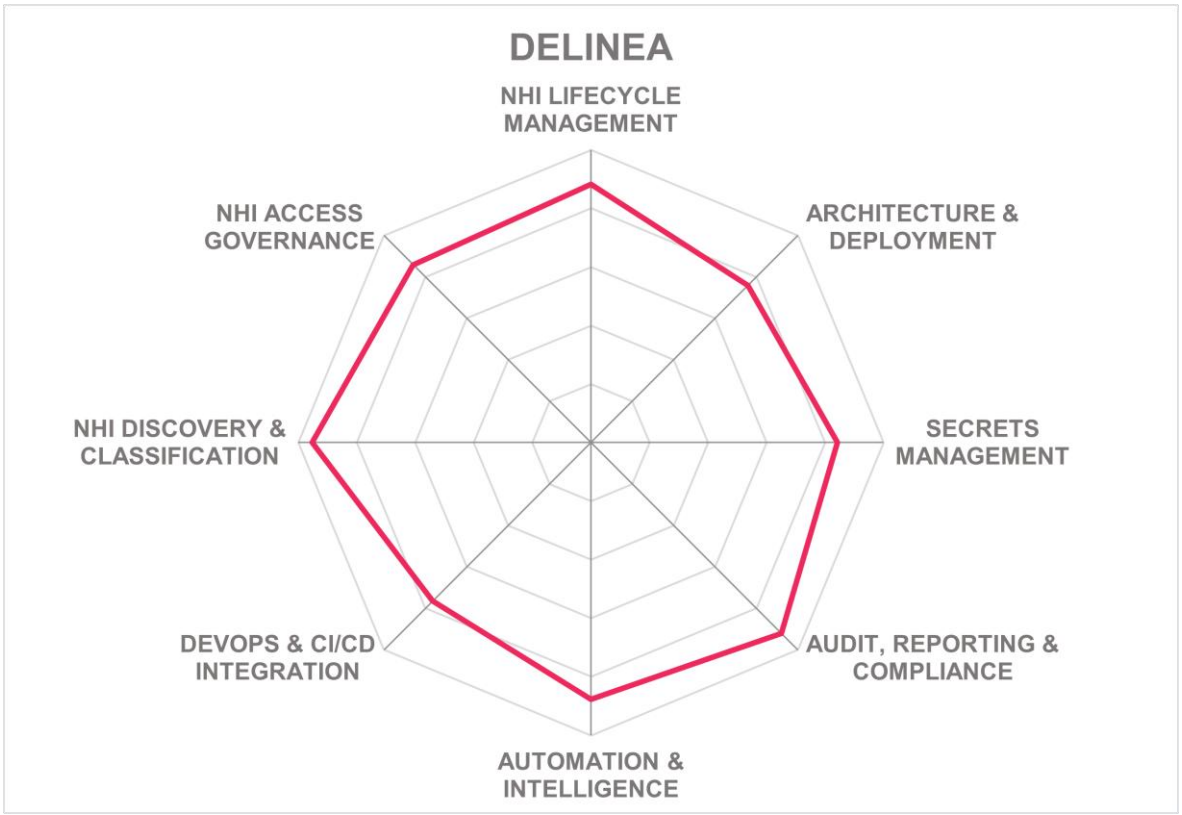
Strengths

- SPIFFE-based architecture enables zero trust and helps eliminate long-lived credentials for containers, virtual machines, AI agents and CI/CD pipelines, eliminating the need for secrets managers.
- Interoperates with a wide range of SIEM platforms and other security operations solutions out of the box.
- Excellent management of various NHIs, supporting cloud, on-prem, and hybrid environments.
- Good integration with major cloud providers and interoperability with existing vault solutions.
- Microservices-based hybrid SaaS model offers scalability and enterprise resilience.
- Detailed audit capabilities ensuring full traceability and security compliance.
- Efficient, dynamic automation in identity provisioning reduces manual intervention.

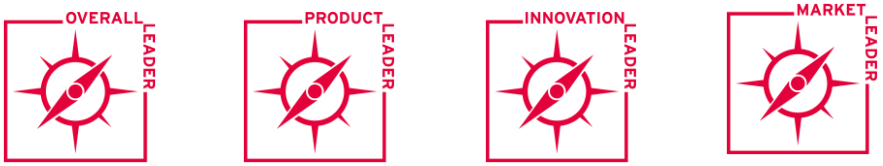
Challenges

- Expanding real-time alerting capabilities and enhancing automated detection for deeper security intelligence.
- Requires integration with secrets managers for legacy secret injection use cases.
- Limited market presence.
- Support for out-of-the-box reports for major compliance frameworks is not provided.

Delinea – Delinea Platform



Leader in



Delinea, founded in 2004 and headquartered in San Francisco, U.S., has evolved from a leading PAM vendor toward being one of the leaders in the broader NHI management landscape. Delinea's product offerings include the Delinea Platform, Secret Server, DevOps Secret Vault, Identity Threat Protection (ITP), and Privilege Control for Cloud Entitlements (PCCE). Delinea can be deployed on-premises, in public and private cloud environments, and is available as a managed services through partners. Licensing models are based on per user subscriptions and numbers of transaction.

Delinea addresses the full range of NHIs, including full support for discovery, inventory, classification, posture management, and continuous monitoring. The solution covers all aspects of machine identity management, including identity federation and ephemeral secret provisioning policies. It supports JIT creation and IaC for NHIs. It integrates with AWS, Microsoft Azure, and Google Cloud identity systems. It offers customizable onboarding

workflows and templates. Additionally, delegated lifecycle management, inactivity detection, and automated deprovisioning features with contextual information about each NHI and dependency mapping are also supported.

Delinea's platform facilitates the secure management of secrets within DevOps pipelines, offering SDK and CLI tools to support integration into containerized and serverless architectures. The solution integrates with popular CI/CD tools such as Jenkins, GitHub Actions, and GitLab CI/CD. RESTful API is supported and is it supplemented by SDK support for Java, .NET, Python, and Go languages. Delinea's platform supports a range of API authentication methods including OAuth 2.0, SAML, OpenID Connect, and JWT.

Secrets are encrypted at rest and in transit. Delinea offers capabilities for automatic secrets rotation, expiration notifications, and versioning. The hardened secrets vault supports a broad range of secret types, including API keys and TLS/SSL certificates, and includes role-based access control and policy-based access control over the storage, retrieval, and management of secrets.

Compliance capabilities include detailed user and secret audit trails, monitoring of access attempts, and support for automated remediation of security alerts. Behavioural analytics is used to enhance risk detection and facilitate adaptive access control mechanisms. The platform's reporting capabilities includes support for all major standard reports however customization is required to conform to specific compliance frameworks.

Delinea plans to enhance NHI credentials in code management for inventory and monitoring, extended discovery in SaaS applications and mapping of OAuth tokens to map the relation between them and remediation capabilities to take down NHIs under threats. Delinea maintains certifications for FIPS 140-2 and US FedRAMP. English, German, Spanish, Chinese, and Japanese languages are supported. Delinea's strengths lie in its unified platform approach, flexible deployment options, and wide-ranging identity management capabilities for NHIs, making it well-suited for enterprises seeking full-featured NHI management.

Strengths

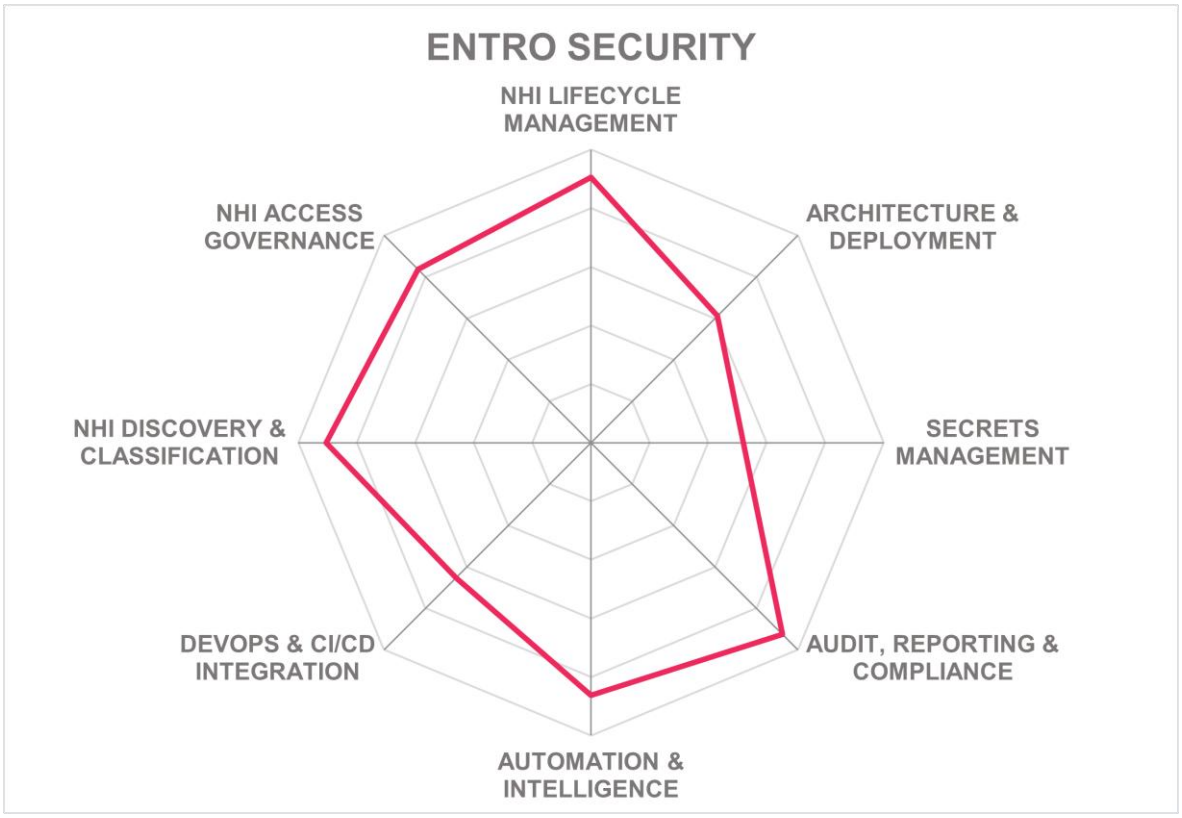
- Excellent management of NHIs in hybrid and multi-cloud environments.
- Extensive AI capabilities for dynamic identity threat detection and response.
- Strong market presence through extensive partner ecosystem with over 500 integrations.
- Automated lifecycle management and credential security.
- Very good secrets discovery capabilities.
- Extensive distributed vaulting features.
- Support for short-lived secrets.

Challenges

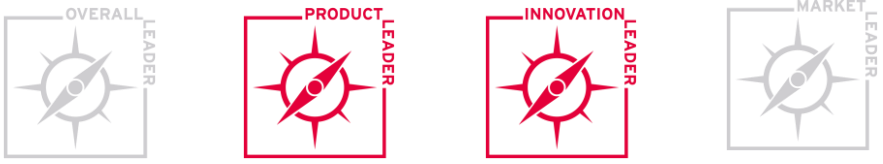
- Complexity in integrating with legacy systems that may not support modern identity management protocols.

- Difficulty ensuring consistent governance across disparate systems and environments, leading to potential gaps in security policies.
- Some DevOps and CI/CD integration capabilities are missing.

Entro Security – Entro Security NHI and Secrets Platform



Leader in



Entro Security, founded in 2022 and headquartered in Boston, U.S., focuses on NHIs such as service accounts and application tokens. The company's main solution is its Non-Human Identity & Secrets Security Platform. This fully integrated suite supports cloud service deployment while supporting both software installations on customer premises and virtual appliances containerized in Kubernetes. Entro Security utilizes flexible pricing models, primarily determined by the number of integrations, accommodating various stages of organizational security needs.

Entro Security's platform manages all types of NHIs, covering the entire lifecycle from discovery to deprovisioning. Additionally, Entro Security ensures real-time inventory management and visibility across diverse setups. The platform supports JIT creation and IaC and is compatible with major cloud identity systems like AWS, Azure, and GCP. Customizable workflows, templates for repeatable deployments, and identification of unused NHIs add to its lifecycle governance capabilities. Additional features include automatic

metadata enrichment and comprehensive identity mapping functionalities, allowing organizations to easily track changes and manage dependencies.

Entro Security supports DevOps and CI/CD environments by providing tools like a CLI for DevOps, automated secret policy APIs, and hardcoded secret detection. It lacks support for sidecars and serverless secret injections. The solution’s API support is limited to REST and lacks SDK support Entro Security covers CI/CD pipelines via Jenkins and GitHub Actions integration.

Entro Security does not operate its own vault but integrates with leading vault solutions for enhanced security measures. This approach allows organizations to maintain distributed or centralized vaults while benefiting from Entro Security's advanced lifecycle management, which includes automated rotation and expiry notifications.

Entro Security's platform provides audit and compliance capabilities, ensuring integrity through tamper-evident cryptographically signed logs. A variety of reports are present, addressing lifecycle management and policy enforcement. The platform offers forensic capabilities for security incident analysis, along with session-level detail for secrets access and usage.

Entro Security's Non-Human Identity Detection & Response (NHIDR) module contains a behavioural analytics engine which dynamically assigns risk scores to NHIs. It uses ML models to detect anomalies and classify them which allows for the optimization of responses. Secrets rotation and remediation workflows are automated for privilege escalation, sudden geolocation changes, API reconnaissance, or secret misuse in real time.

and driven by risk analysis. Policies dynamically attach to identities based on contextual tags, thereby augmenting access controls. Entro Security supports real-time behaviour tracking and privilege adjustments based on risk evaluation.

Looking ahead, Entro Security plans to expand its focus on agentic AI and rectify identified challenges around AI agent lifecycle management. Entro Security has ISO/IEC 27001 certification. The service supports multiple languages. While continually innovating, Entro Security has a strong and innovative product that is likely to gain market share. Organizations that have existing secrets vaults that need additional NHI governance features should consider Entro Security.

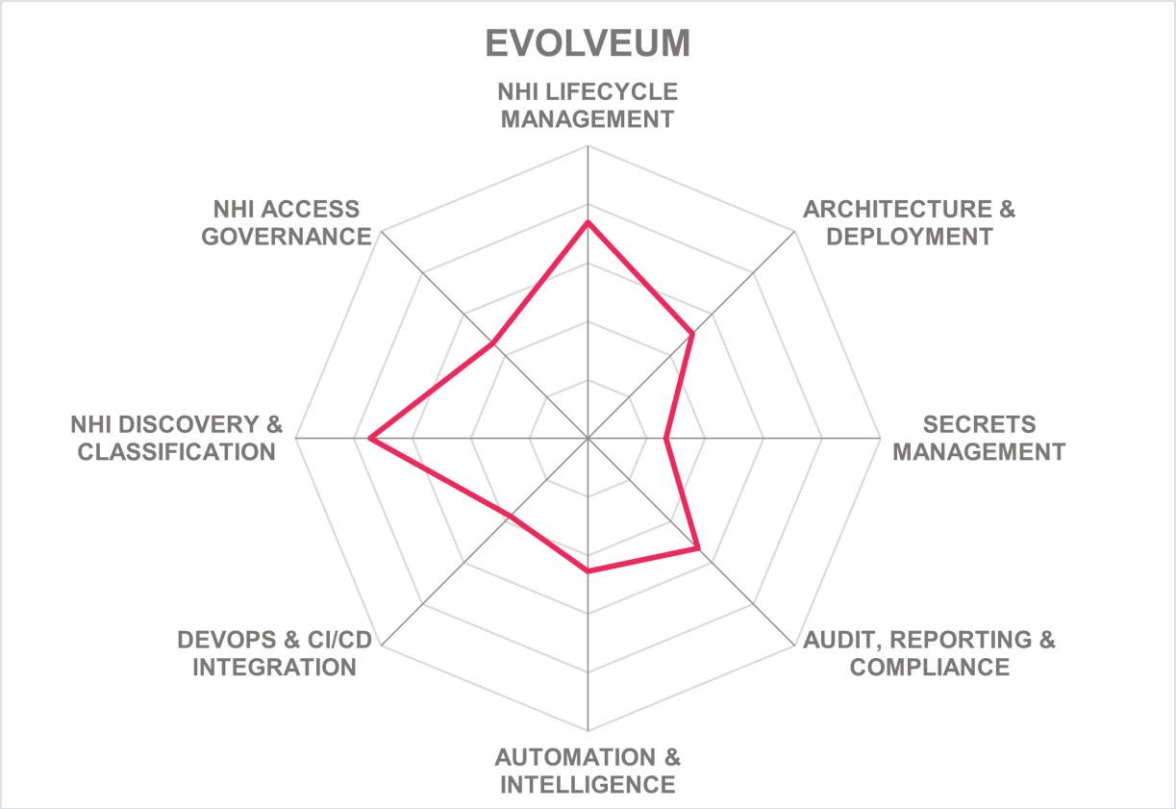
Strengths

- Strong discovery and classification capabilities.
- Advanced risk assessment tools.
- Support for semi-automated and automated remediation workflows
- Advanced AI/ML-powered detection models for anomaly detection and adaptive access.
- Dynamic risk scoring and automated policy adjustments.
- Good audit and reporting capabilities address lifecycle and policy enforcement actions.

Challenges

- Small but growing vendor with a good partner ecosystem.
- Lacks out-of-the-box compliance reports for major frameworks like GDPR and HIPAA.
- Some advanced secrets management capabilities are missing.
- Lack of service-to-service onboarding automation capabilities via templates or APIs.

Evolveum – midPoint



Evolveum is an IGA vendor based in Slovakia. Founded in 2011, Evolveum's midPoint product is open source, and they support subscriptions and professional services. Deployment options include on-premises, container-based, and SaaS provided by partners. There is no licensing cost for the product.

Evolveum's midPoint supports management for a wide range of non-human identities such as virtual machines, CI/CD tools, containers, microservices, web and backend applications, service-mesh components, mobile applications, cloud-native service accounts, integration bots, AI/ML pipelines, IoT devices, connected edge systems, custom automation scripts, API clients, and various device types. The solution addresses full lifecycle processes such as discovery, inventory, and decommissioning. Machine Identities are not directly supported in terms of workload protection. Evolveum supports JIT creation through APIs and has integrations with AWS, Microsoft Azure, and Google Cloud. Customizable workflows and assignment templates are included, with lifecycle management features allowing for delegated actions, inactivity detection, and automated de-provisioning. Metadata and dependency mappings can also be managed. Dynamic access evaluation and automated credential rotation are omitted. It integrates with third-party solutions such as AWS, Microsoft Azure and GCP for lifecycle and access management.

MidPoint does not support sidecar injections or serverless function management. REST and SCIM API types are supported. The platform offers SDKs for Java development. For

DevOps and CI/CD, dynamic secret injection and integration with tools like Docker are available, though direct support for specific CI/CD platforms such as Jenkins or GitHub Actions is not provided. MidPoint provides good on-premises DevOps options and hopes to move towards a hybrid or a full cloud environment in the future.

While Evolveum offers secrets management capabilities, it does not provide a hardened secrets vault or support extensive credential lifecycle management features. Only basic encryption of secrets is supported. Additionally, the platform supports integration with external secrets vaults with limited compatibility extending to Docker secret files.

Audit trails capture identity lifecycle events, and SIEM integration is supported via syslog. The tool supports risk scoring and policy enforcement. Through its "Time Machine" feature, Evolveum provides retrospective insights into identity states.

The project enhances efficiency through automation of correlation processes using similarity-based search, when needed, and currently developing GenAI features to provide intelligent recommendations and ML techniques for identity mapping. midPoint analytics capabilities include ML-powered outlier detection and classification, although real-time behaviour tracking and adaptive authentication for NHIs are not currently supported.

Evolveum's customer deployments include medium-sized to enterprise companies, critical infrastructures, government, healthcare, and universities. The roadmap outlines capabilities in line with user requests for UI/UX improvements and AI-based feature enhancements including AI application onboarding assistant. Evolveum holds ISO/IEC 27001 certification. Evolveum's strengths lie in its open-source model, ability to be deployed both on-premises and cloud, and flexible integration capabilities, though challenges remain in advanced secrets management and workload protection. The solution is suitable for organizations seeking an extensible, open-source platform.

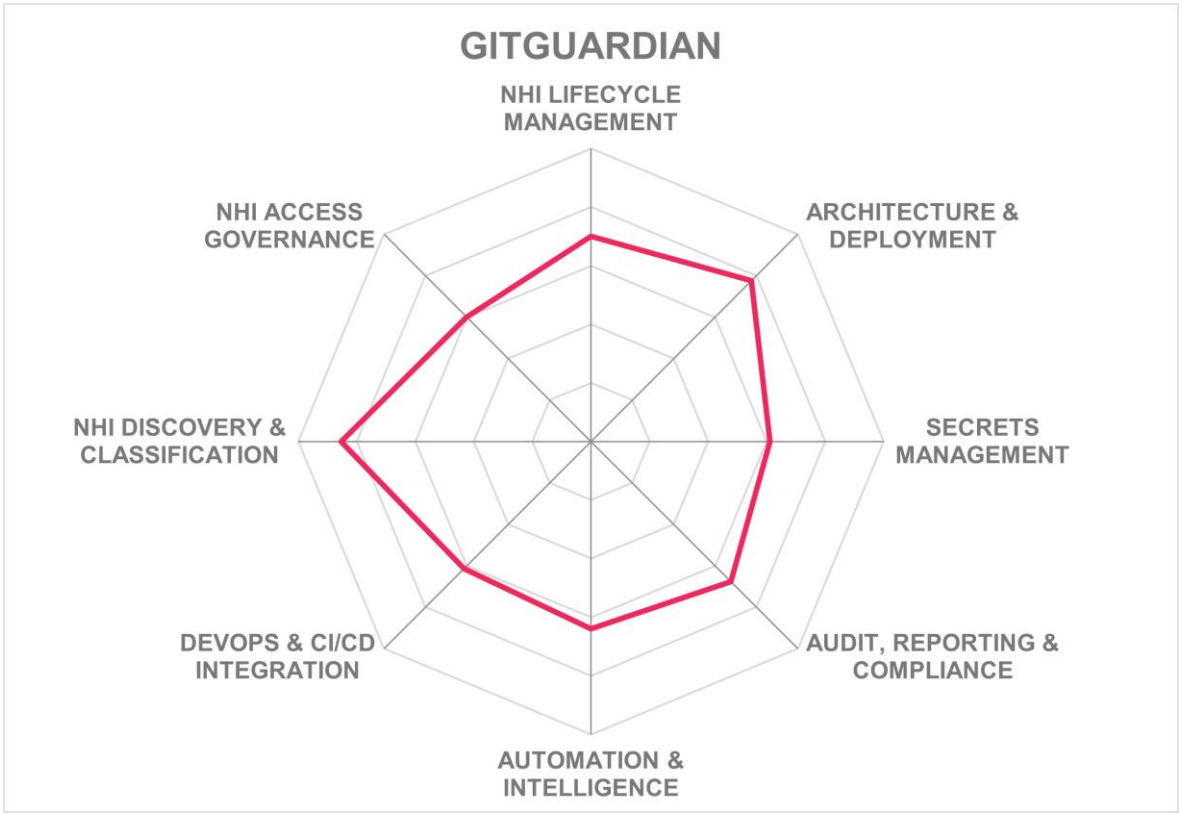
Strengths

- Supports a wide range of NHIs.
- Open-source platform.
- Solution is highly customizable and integrates well with existing systems.
- The platform provides full lifecycle management features for NHIs.
- Interoperability with SIEM systems for compliance management.
- 100% of solutions’ capabilities exposed via APIs.
- Good NHI governance capabilities for expired or unused NHIs.
- Flexible deployment options.
- Owned and based in EU.

Challenges

- Does not provide dynamic credentials rotation capabilities.
- Real-time access evaluation is not directly supported by MidPoint.
- Partner-dependent SaaS delivery might lead to inconsistent service levels.
- Does not support credential lifecycle management and overall secrets management capabilities are limited
- Support for IaC tools is limited.

GitGuardian – GitGuardian Platform



GitGuardian, founded in 2017 and headquartered in Paris, France, is an enterprise-ready provider in the NHI Management sector. The company predominantly operates in North America, EMEA, and APAC. The solution performs secrets discovery, security, and management for heterogeneous environments. Their flagship service is the GitGuardian Platform, targeting secrets detection and NHI management. Deployable on-premises, in public, private, and air-gapped environments, GitGuardian supports flexible deployment through SaaS, and virtual appliances, offering licensing per active developer.

GitGuardian's platform supports all major NHIs, addressing their discovery, inventory, classification, posture management, detection, response, vaulting and decommissioning. The platform supports cloud-native identity systems such as AWS, Azure, and GCP, though it does not support JIT NHI creation through infrastructure-as-code. Workflow customization and replication capabilities complement features for detecting inactivity, bulk imports, and lifecycle status reporting, with metadata enrichment and dependency mapping to enhance inventory accuracy.

For integration, GitGuardian facilitates secret delivery through sidecar injection and supports APIs to expose core functionalities. Developers benefit from Python SDK support, enabling

compatibility in DevOps pipelines. The platform’s CLI tools, like ggshield and ggscout, further facilitate DevOps integration by offering features for secret scanning and NHI management across various CI/CD tools.

Despite not offering a built-in secrets management system, GitGuardian integrates with existing secrets vaults such as AWS Secrets Manager and HashiCorp Vault. GitGuardian's solution focuses on identifying where secrets are located and how they are used or exposed within systems. The solution then provides insights and recommendations on how to manage these secrets securely and integrate with established secrets management systems such as AWS Secrets Manager, HashiCorp Vault, Google Secret Manager, Azure Key Vault, CyberArk Conjur, and Akeyless Vault.

Audit and compliance features address NHI activities, organizational change tracking, and policy enforcement. The platform lacks specific policy reports tied to major compliance frameworks, but supports automated incident management analytics, and insightful threat landscape visualization. Dynamic risk scoring based on policy violation severity and integration with SIEM platforms offers further compliance opportunities. GitGuardian NHI access governance capabilities include a unified multi-vault governance with duplication detection, rotation hygiene, and environment-specific policy enforcement. It maps identities to owners, performs continuous presence and validity checks, and verifies deletion. Additionally, it deploys honeytokens as decoys for active misuse detection, strengthening identity threat detection and response for secrets and NHIs.

Recently, GitGuardian has added one-click secret revocation across clouds, AI-powered contextual code fixes, broader integrations, and enhanced identity mapping to link secrets, NHIs, and accessed resources for better offboarding and governance. Their roadmap includes plans to expand features such as behavioural anomaly detection and automated remediation workflows, AWS Container Registry support, and advanced compliance reporting. Although GitGuardian lacks certain incident response capabilities, its integration with third-party monitoring technologies can help customers achieve adherence to fundamental security practices. With flexible workflows and extensive integration capabilities, GitGuardian's platform is suited to large enterprises with complex cloud infrastructures, such as those in technology, finance, and healthcare sectors, which require thorough NHI management.

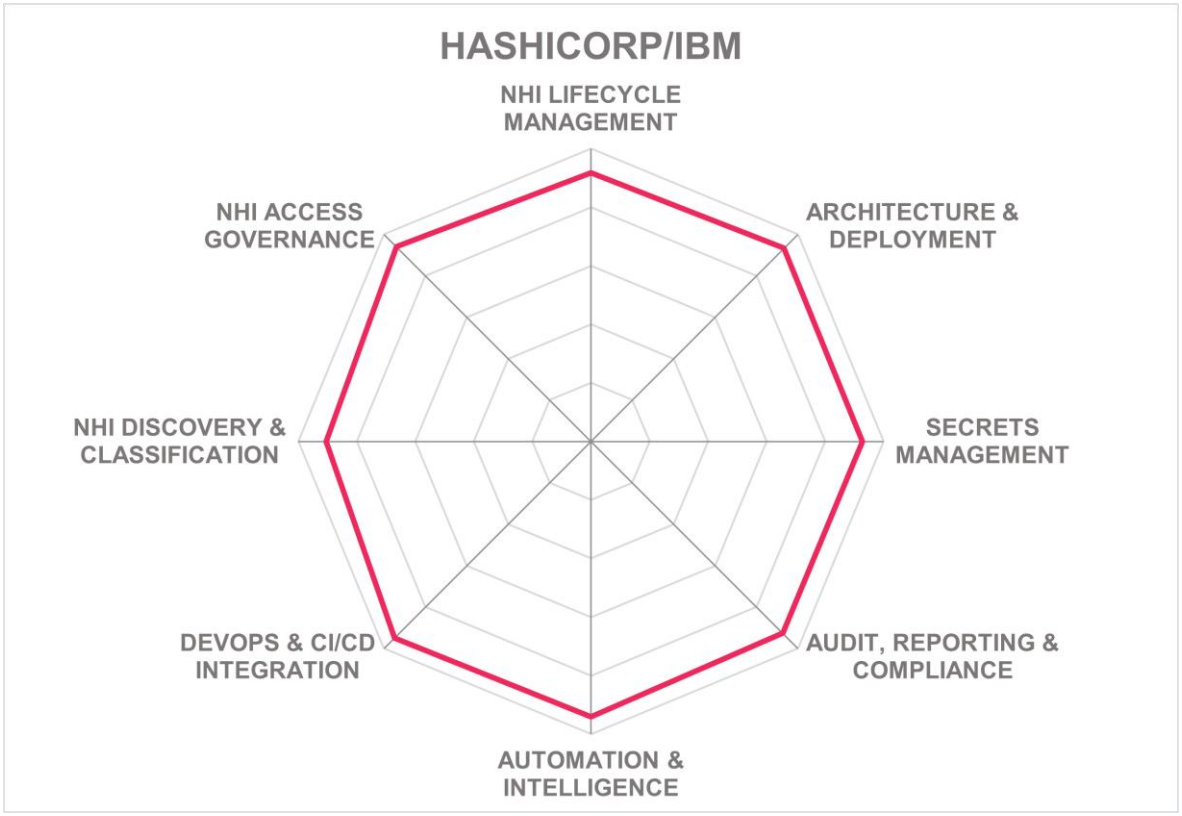
Strengths

- Supports a broad range of NHIs.
- Supports templated NHIs for repeatable deployments.
- Automated policy updates as NHIs transition between environments,
- Continuous discovery ensures up-to-date tracking of NHIs and their statuses.
- Extensive integration capabilities with third-party secrets vaults like AWS Secrets Manager and HashiCorp Vault.
- Microservice architecture for flexible deployment across various environments.
- Supports maintaining detailed audit logs and tracks lifecycle events for NHIs.
- Provides dashboards for lifecycle management and security metrics tracking.

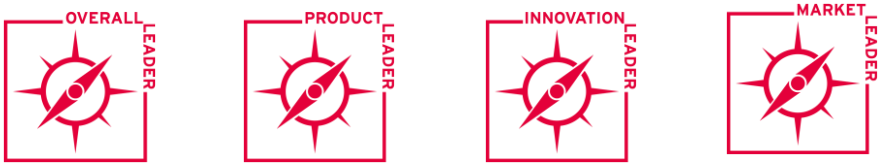
Challenges

- Needs expansion in secrets lifecycle management.
- Just-in-time NHI creation and API provisioning are not supported.
- Automated deprovisioning of unused or expired NHIs is unavailable, relying on manual processes.
- Limited automation for anomaly detection and adaptive access adjustments.

HashiCorp, an IBM company – HashiCorp Vault



Leader in



HashiCorp, founded 2012,headquartered in San Francisco, U.S. and with its recent acquisition by IBM, plays a significant role within the broader NHI Management space, particularly with its Vault product, which is central to its cybersecurity solutions. HashiCorp places a strong emphasis on securing dynamic, low-trust environments often found in cloud-native applications, focusing its efforts primarily on workload identities. It offers both software and services, with other adjacent products including HashiCorp Boundary, IBM Verify, and IBM Guardium. It can be deployed on-premises, as cloud services, and managed services are available for SaaS. Licenses can be obtained via subscriptions or consumption-based pricing models.

HashiCorp supports a wide range of NHIs. It supports all lifecycle elements, such as discovery, inventory, classification, and decommissioning. The solution's capabilities extend to JIT creation of NHIs and IaC support. It is integrated with major cloud-native identity

systems like AWS, Microsoft Azure, and Google Cloud Platform. HashiCorp has customizable onboarding workflows, and it provides templated NHIs for consistent deployments. Moreover, it supports delegated lifecycle management, inactivity detection, bulk import, and detailed lifecycle reporting. Metadata enrichment and identity mapping are also integral components of its offering.

HashiCorp Vault supports the use of sidecar and serverless functions. Its functions are API accessible, and it is complemented by SDKs in multiple programming languages. DevOps and CI/CD integrations focus on dynamic secrets management, supporting tools like Terraform and Ansible, with integrations available for popular CI tools such as Jenkins and GitHub.

Secrets management functions within HashiCorp Vault offers secure storage and encryption, role-based access, TTL for secrets, and third-party vault integrations. HashiCorp's Vault includes support for both static and dynamic secret types and logging, policy-based access control, FIPS compliance, and the ability to scope secrets per application or environment

In terms of audit and compliance, HashiCorp Vault ensures thorough trails of NHIs access and lifecycle events, aligned with various regulatory compliance standards. The platform also offers extensive analytics and support for automated responses based on Verify's analytics engine used to identify anomalous behaviour for both human and non-human identities, enabling enhanced identity risk management, real-time behavioural monitoring, and dynamic policy adjustment for NHIs.

HashiCorp's roadmap includes native support for SPIFFE standards and SVID minting for machine identity authentication and expanded governance capabilities within its solutions. Security certifications such as FIPS 197, FIPS 140-2, FIPS 140-3, ISO/IEC, NIST 800-57, ISO/IEC 15408.In addition, their services support ISO/IEC 27001, PCI-DSS v 3.2, ISAE 18 SOC Type 2, and HIPAA/HITRUST are maintained. It offers broad incident support and multi-language customer service. The strength of HashiCorp lies in its approach to handling machine identities and NHIs, providing scalable, reliable security and identity solutions for diverse enterprise needs.

Strengths

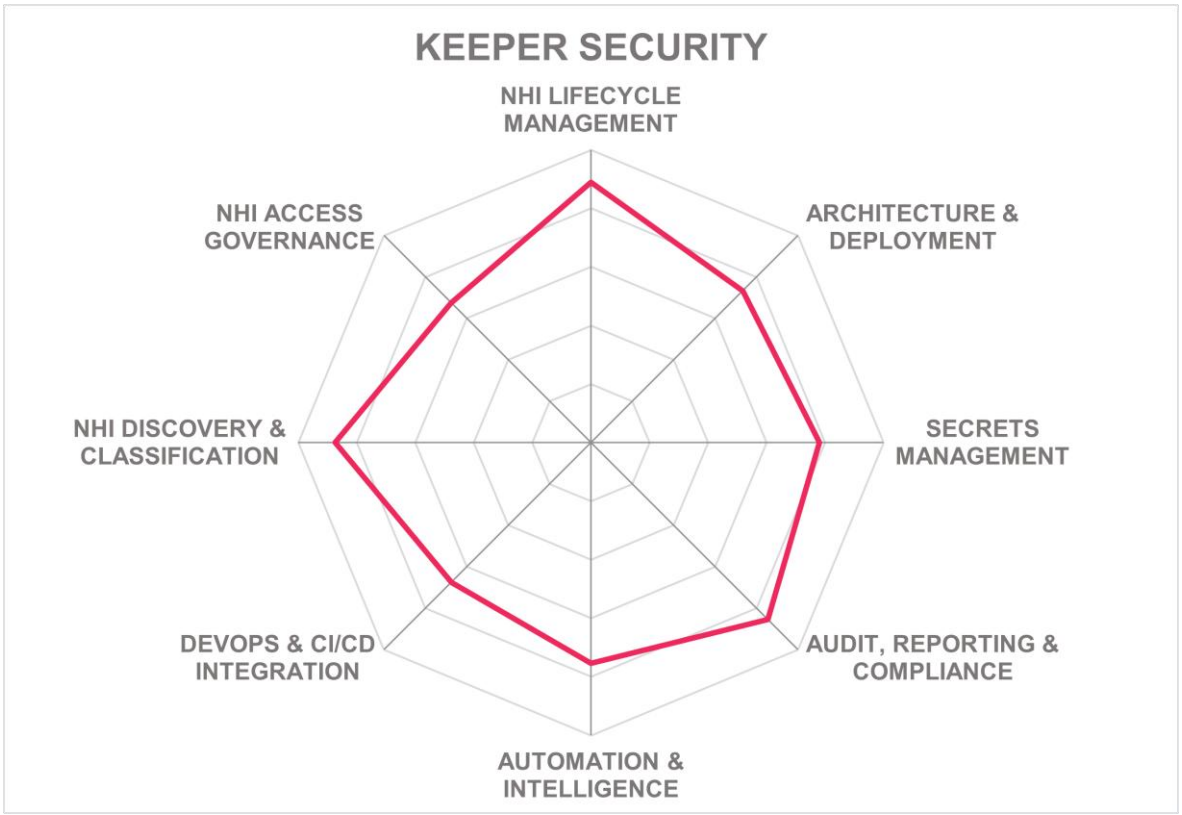
- Supports secrets management across diverse environments.
- Supports a wide range of NHI types, including CI/CD tools and containers.
- Extensive policy enforcement features for access and management.
- Provides just-in-time creation and automation for NHIs.
- Supports lifecycle management including discovery, vaulting, and decommissioning.
- Logging and auditing features for security and compliance.
- Good solution for workload identities.
- Many integrations with DevOps tools.
- Flexible deployment options.

Challenges

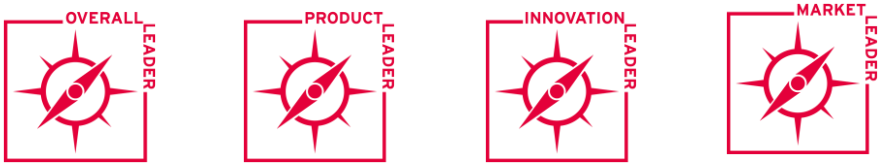
- Needs improvement in secrets lifecycle management automation.
- Some remediation workflows are not supported.
- Automated reassignment of ownership for orphaned NHIs is missing.

- Out-of-the-box support for reports for some major compliance frameworks such as FERPA and FISMA is missing.

Keeper Security – Keeper Secrets Manager



Leader in



Keeper Security, founded in 2011 and headquartered in Chicago, U.S., is a is a privately held company. Keeper Security's solutions include Keeper Secrets Manager and KeeperPAM. They are active across North America, EMEA, APAC, and Latin America. Keeper Security SaaS solutions are hosted in a Tier 1 IaaS provider. The core infrastructure is cloud-based with several optional components to support on-premises including a stand-alone Keeper Connection Manager application to support on-premise installation requirements for connection management. Licensing is available per user and through fixed cost per API bundle for Keeper Secrets Manager.

Keeper Security supports a wide range of NHIs such as virtual machines, CI/CD tools and pipeline agents, containers, microservices, web and backend applications, cloud-native service accounts, integration bots, AI/ML pipelines, IoT devices, connected edge systems, custom automation scripts, API clients, and devices. Support for mobile applications and service-mesh components is not available. It supports full lifecycle management. Keeper

provides in-depth machine identity management through various mechanisms such as workload federation and service account scoping. It provides JIT creation and IaC provisioning. It supports integrations with cloud-native identity systems like AWS, Azure, and Google Cloud Platform, as well as other third-party platforms. It allows delegated lifecycle management and automatic deprovisioning for inactive NHIs, with lifecycle status reporting and metadata mapping capabilities.

Keeper Security does not support sidecar injection but allows management of secrets in serverless functions. API types supported include REST, SCIM, and OAuth. They offer SDKs for multiple languages, such as Java, .NET, Python, and JavaScript. The company extends its DevOps and CI/CD capabilities with integration into tools like Jenkins, GitHub Actions, GitLab CI/CD, CircleCI, Bitbucket Pipelines and Azure DevOps.

Keeper Security's secrets management capabilities are centred around a zero-knowledge architecture with a hardened secrets vault that supports a wide variety of secret types, including API keys, OAuth tokens, SSH keys, database credentials, TLS/SSL certifications, JWTs, service tokens, cloud IAM credentials, CI/CD tokens, and structured secrets. Keeper ensures all secrets are encrypted both at rest and in transit by employing client-side AES-256 encryption This vault is designed to be compliant with the latest FIPS 140-3 standard. The system provides granular access control, offers automatic rotation, and supports API-based secret retrieval ensuring details never persist on disk.

Keeper Security's audit and compliance tools provide the ability to track NHIs across the entire lifecycle within customer environments. The Keeper Security admin interface features context-aware risk dashboards and supports compliance with regulatory standards such as GDPR, HIPAA, and PCI DSS. Every action is logged for audit purposes supporting certifications like ISO/IEC 27001, PCI-DSS, and SOC 2 Type 2.Events can be streamed to SIEM systems and analyzed by SOAR solutions. Their ML-powered analytics provide in-depth behavioural insights and anomaly detection capabilities. These systems enable risk-based analysis and can flag stale NHIs.

Keeper Security's roadmap includes enhancements to its products like KeeperAI for advanced threat detection, as well as expanding partner integrations. Keeper Security offers a robust solution for organizations seeking robust secrets management capabilities with detailed audit and compliance tracking.

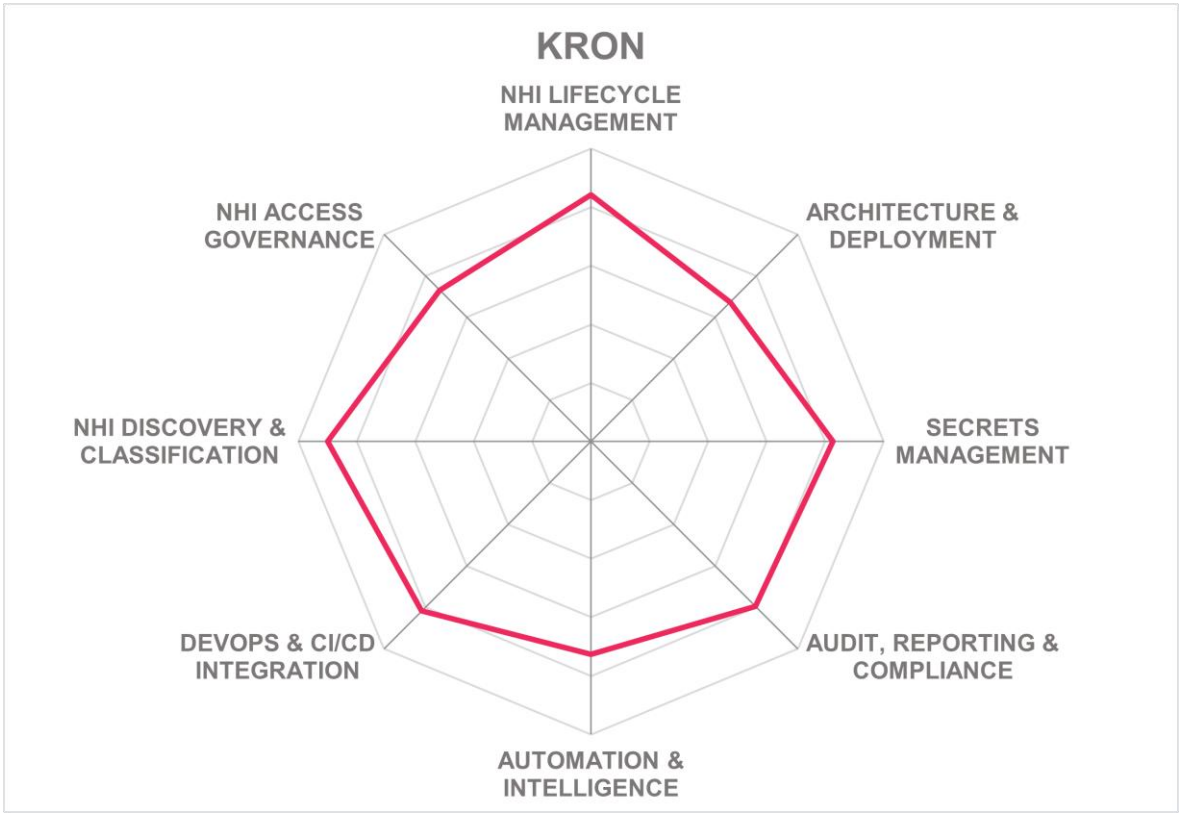
Strengths

- Vault are encrypted using a zero-knowledge encryption model.
- Manages an extensive scope of NHIs, including virtual machines, containers, and CI/CD agents.
- Full Lifecycle management with support for discovery, classification, and decommissioning.
- Rich integration with major cloud platforms and CI/CD tools enhances deployment flexibility.
- Detailed audit logs and event tracking support compliance and security monitoring.
- Scalable infrastructure with FIPS 140-3 approved encryption.
- Securely injects secrets into runtime environments without persistent storage.

Challenges

- Just-in-time NHI creation for workload applications is currently limited and planned for future development.
- Manual intervention is required for orphaned identity management and reconciling stale NHIs.
- In-depth policy enforcement based on context-aware attributes is missing but planned for release 2025 EoY.

KRON – KRON PAM



Leader in

Founded in 2007 and headquartered in Istanbul, Turkey, Kron Technologies has established itself as a notable player in the data security and access management space. With a core presence in the EMEA region, Kron has expanded its global reach through a partner network across North America, APAC, and Latin America. The company's US office is located in Jersey City, New Jersey. Kron PAM is their flagship product, supporting diverse deployment platforms including on-premises, private and public cloud environments. The product is available through flexible licensing models encompassing user-based and per node options that cater to bespoke needs.

The Kron PAM solution addresses all major NHIs, facilitating extensive lifecycle management activities such as discovery, classification, and decommissioning. Machine Identity management supports virtual machines, containers, CI/CD pipelines, API clients and standalone applications. Kron offers JIT creation and IaC support, including integration with major IaaS providers. The platform's customization capacity allows tailored workflows and

template-based provisioning, along with status reporting, delegated lifecycle management, inactivity detection and automatic de-provisioning of orphan identities.

Kron PAM supports modern infrastructure with capabilities like sidecar injection for containerized environments. The solution provides REST APIs for integration and supports authentication through Active Directory/LDAP, SAML, PKI, and Windows Authentication (Kerberos).The solution provides SDKs support for a range of programming platforms and languages, including Android, iOS, Java, C/C++, .NET, Python, along with additional support for PHP, Bash (CLI scripts), and PowerShell The solution strengthens CI/CD processes through secure secrets handling by supporting major platforms like Jenkins and GitLab CI/CD.

Kron's capabilities in secrets management are notable, with mechanisms for secure secrets storage and retrieval, automated rotation, and encrypted transmission. The secrets vault is constructed with zero-trust architectural principles that require robust identity verifications prior to access.

Audit and compliance are core strengths, with logging of all NHI interactions and lifecycle events, privilege escalation detection, and compliance checks against frameworks such as GDPR, HIPAA, FIPS 200, NERC CIP, NIST SP 800-53, PCI DSS, SOX, and ISO 27001.

Kron Technologies' roadmap includes incorporating AI-based behaviour analytics, enhancements such as zero-trust orchestration and support for federated identities across multi-cloud environments. The company is ISO/IEC 27001 certified. Kron's products are well-suited for organizations with complex infrastructures, especially those operating in multi-cloud and hybrid environments. Enterprises in sectors such as technology, finance, healthcare, and manufacturing, where secure management of a diverse range of NHIs is imperative, will find significant value in Kron PAM.

Strengths

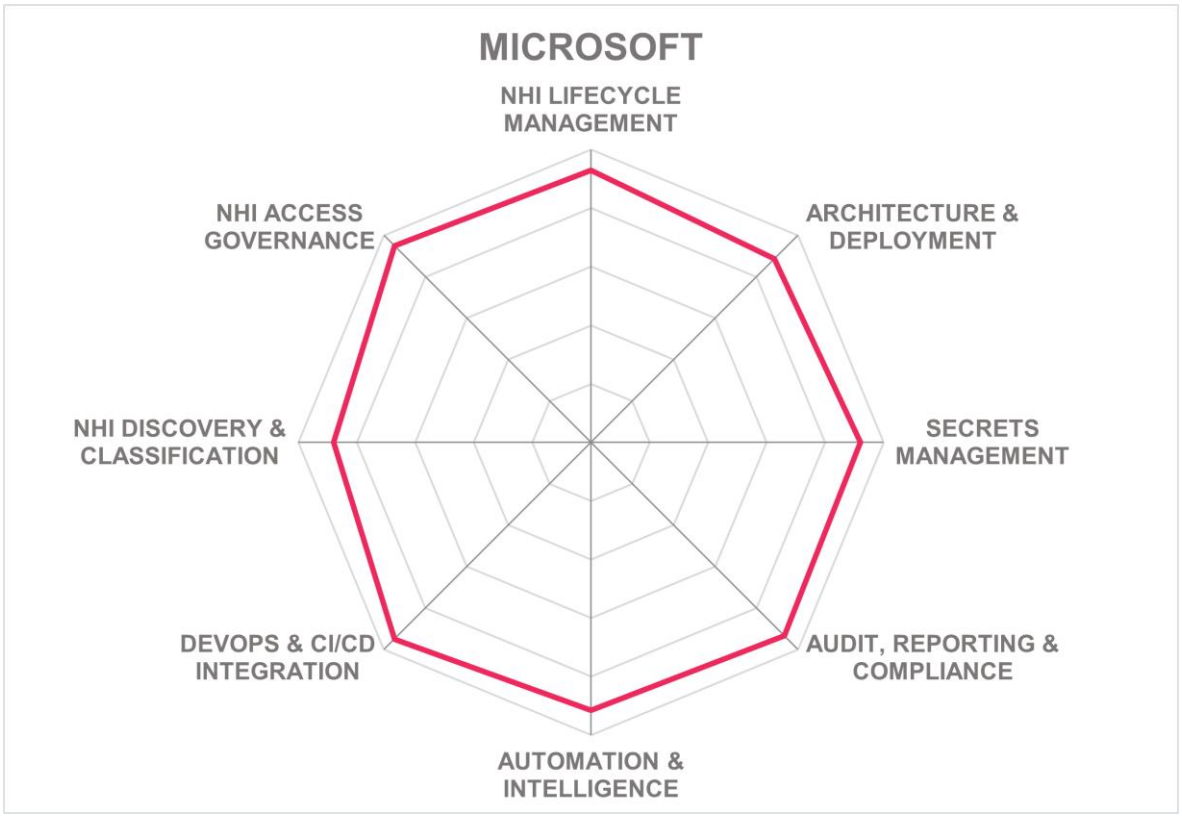
- Strong lifecycle management for NHIs across varied environments.
- Supports secret management with automated rotation and secure storage capabilities.
- Integrates effectively with major cloud-native platforms like AWS IAM, Azure AD, and Google Cloud IAM.
- Facilitates JIT provisioning for ephemeral workloads.
- Offers RESTful APIs for integration with CI/CD and IaC workflows.
- Includes a password vault and identity orchestration services for secure operations.
- Provides extensive SDKs support.

Challenges

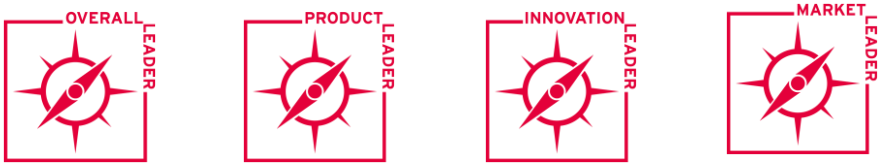
- Lacks AI-driven insights for anomaly detection and risk evaluation but planned for release 2025 EoY.
- Integration with third-party secrets vaults is on the roadmap but not yet available.
- Limited capabilities in detecting privilege overlaps and misconfigurations automatically.
- Does not provide detailed AI/ML analytics for role modification or entitlement assessments.

- Needs some advancement in real-time behavioral analytics and context-aware policy enforcement to enhance its proactive threat response capabilities.

Microsoft – Entra ID



Leader in



Microsoft, established in 1975 and headquartered in Redmond, WA, USA, is a publicly traded company with customers around the globe. Microsoft Entra ID, a part of the Microsoft Identity Suite, plays a pivotal role in NHI Management by providing extensive capabilities across the lifecycle of machine and workload identities. Microsoft's product suite relevant to NHIs includes Microsoft Entra ID, Microsoft Sentinel, and Azure Key Vault. Microsoft Entra is offered as a fully managed SaaS solution, with regional deployment support in sovereign and government cloud environments. The company supports per-user and per-time period licensing models.

Microsoft Entra ID facilitates granular control over NHIs through features such as Managed Identities, Service Principals, and Workload Identity Federation. These tools enable workloads to authenticate and interact securely across various platforms including Azure, AWS, and GCP, without the need for long-lived credentials. This fosters a secure environment for dynamic, ephemeral workloads in DevOps settings by leveraging JIT identity creation and federated identity models. Additionally, Entra ID provides delegated lifecycle

management, inactivity detection, and automated cleanup for unused machine identities. Reporting functions document lifecycle status, inactivity alerts, and transitions, accompanied by metadata and ownership mapping enhancements.

Sidecar support aligns with Azure Key Vault and CSI Driver for secrets management in serverless functions, while extensive API support is available via REST, SCIM, OAuth, OIDC, SAML, WS-Federation and WS-Trust. CSI driver connects Kubernetes clusters to external storage systems for dynamic storage management. SDKs for multiple languages such as .NET, Python, and Java facilitate integration into DevOps and CI/CD environments, empowering tools like GitHub Actions and Azure DevOps with automated identity and secrets management capabilities.

Microsoft emphasizes integrated secrets management through Azure Key Vault including support for storage of API key storage, automated rotation and encrypted transmission, certificate management, and OAuth token lifecycle management. Secrets access in Azure Key Vault is supported by encryption standards such as AES-256, policy-based governance, and automation features, while federated and managed identities eliminate the need for long-lived credentials.

Microsoft Entra ID offers extensive audit and automation capabilities, providing logging and event tracking for NHIs. The Entra ID platform captures logs and telemetry, supporting nearly 30 compliance frameworks through audit trails, anomaly detection, and risk assessments. Analytics in Microsoft Entra ID leverage AI and ML to dynamically adjust access controls, provide anomaly detection and risk evaluation, monitor potential misconfigurations, and facilitate risk scoring for NHIs. It supports automated remediation through Azure Logic Apps. Integration with Microsoft Sentinel enables centralized alerting and compliance reporting.

Microsoft’s roadmap includes improved AI agent governance capabilities. Microsoft has obtained a wide range of security certifications, such as FIPS 140-2, FIPS 140-3, ISO/IEC 27001, and SOC 2 Type 2. Microsoft's excellent feature set and strong global presence make it suitable for nearly any organization. Microsoft Entra ID is poised to further its reach as a leading solution in the NHI landscape.

Strengths

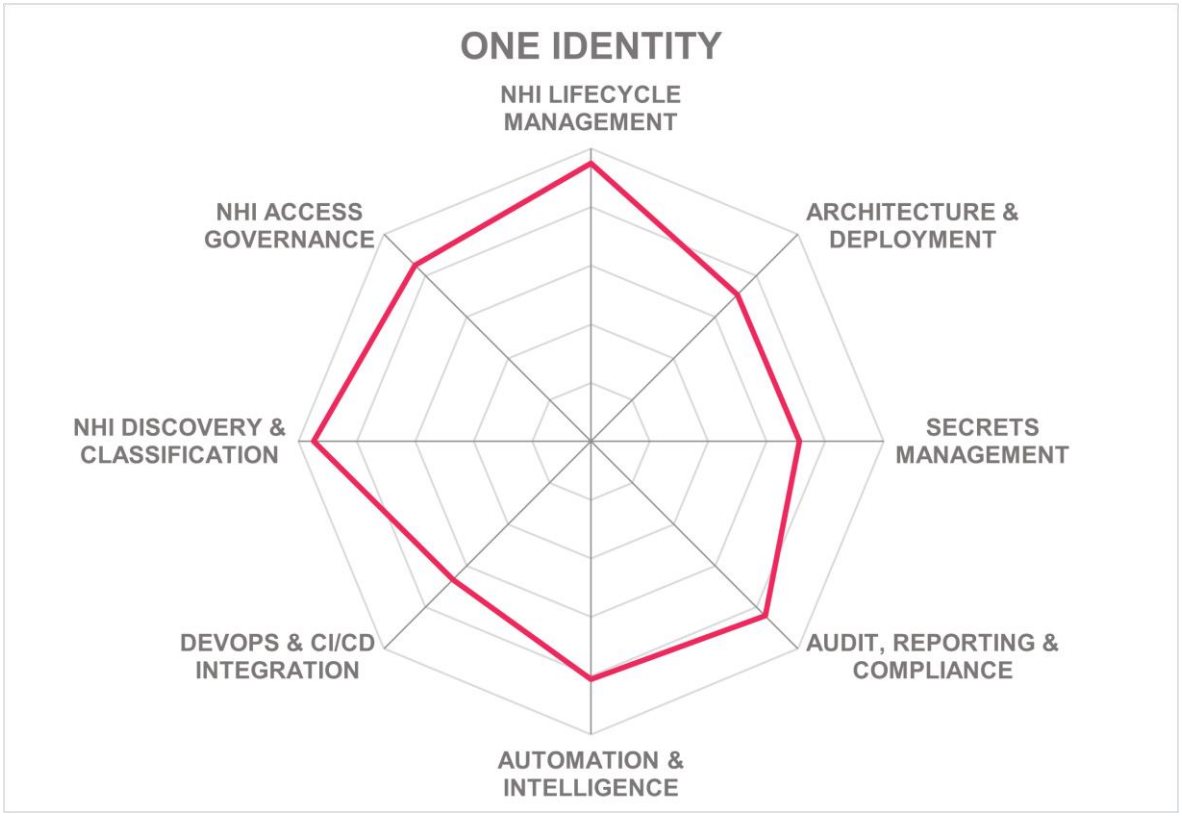
- Supports JIT identity creation for temporary workloads.
- Integrates with a wide range of cloud-native identity systems including using Federated Identity Credentials (FIC) for secretless authentication.
- Offers extensive API support enabling strong automation and integration into DevOps workflows.
- Ensures tight governance through Conditional Access and Identity Protection policies.
- Includes risk-based policy enforcement, sign-in monitoring.
- Integrates AI and ML for anomaly detection and adaptive access controls, offering intelligent governance and threat detection.
- Global leader with a strong market presence.

Challenges

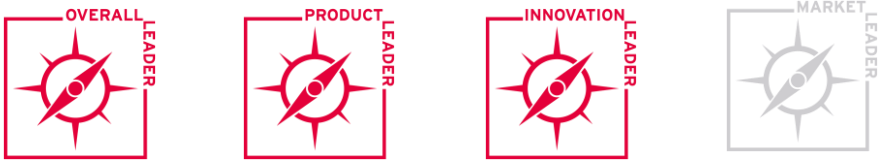
- Does not currently leverage AI/ML to detect dormant or unused credentials.

- Automated ownership reassignment for orphaned NHIs is not yet available.
- Does not support proactive, agent-based continuous discovery across unmanaged or third-party environments.
- Further development is needed in advanced analytics for role modification and privilege management.

One Identity – One Identity Manager



Leader in



Founded in 1987, One Identity is a strong player in the IAM space. The organization operates across multiple regions, including North America, EMEA, APAC, and Latin America. One Identity Manager ensures governance with flexible deployment. Syslog-NG offers logging, available on-premises, or AWS. One Identity's deployment options are extensive, covering on-premises installations, cloud services, SaaS, hardware appliances, virtual appliances, and container orchestration systems such as Kubernetes. Licensing models include per user, per appliance, and managed service structures.

The One Identity solutions address all major NHIs. The full lifecycle of NHIs is supported. Their solutions provide for secure management of machine identities, ensuring federation, workload isolation, and service account scoping. One Identity's platform supports customizable onboarding workflows, templated NHIs for repeatable deployments, lifecycle policy assignments, and automated policy updates across environments. The platform supports conditional policy binding based on various contexts, delegated lifecycle management, and automatic deprovisioning of unused NHIs.

The platform includes sidecar injection for secrets management and supports serverless functions. API support includes REST and. SDK support includes Python, .NET, Ruby, and others. This allows for advanced management of secrets in CI/CD pipelines with plugins for Jenkins, GitHub Actions, CircleCI, Google, AWS, Azure and HashiCorp, promoting automated workflow efficiency and secure practices within DevOps environments.

One Identity has a strong secrets management framework and a secure vaulting system with key management and automated rotation. The secrets vault complies with FIPS 140-3 standards and supports secure storage of a wide variety of secret types, such as API keys, OAuth tokens, and database credentials. Interoperability capabilities extend to third-party vaults like AWS Secrets Manager and Google Secret Manager.

Audit trails and compliance features track all lifecycle events and providing extensive forensic capabilities. Real-time monitoring and AI-driven analytics support behavioural risk assessment and anomaly detection. The platform facilitates policy enforcement, automated remediation, and provides strong reporting options via their web portal where reports can be customized to consume any attribute associated with the identity. Dashboards show dynamic risk scoring and user behavioural analytics.

One Identity's roadmap includes adding AI-driven enhancements such as AI-assisted policy and elevation management, AI-driven bundle deployment for simplified onboarding, ML-based anomaly detection for sessions and user risk and leveraging AI scripting for automated platform support and non-human identity scalability. One Identity is compliant with major certifications such as ISO 27001 and several standards such as SOC 2 Type 1 2, ISO/IEC 27001, PCI-DSS v3.2, HIPAA/HITRUST, US FedRAMP, UK Cyber Essentials, France SecNumCloud, FIPS 197 Advanced Encryption Standard, FIPS 140-2 Cryptographic Module Standards, NIST 800-57 Key Management, and ISO/IEC 15408 Common Criteria. Overall, One Identity offers strong NHI lifecycle management solutions, advanced analytics, and flexible deployment options, but there are areas for development such as extending its capabilities in posture management and developing more native integrations with CI tools critical for DevOps environments.

Strengths

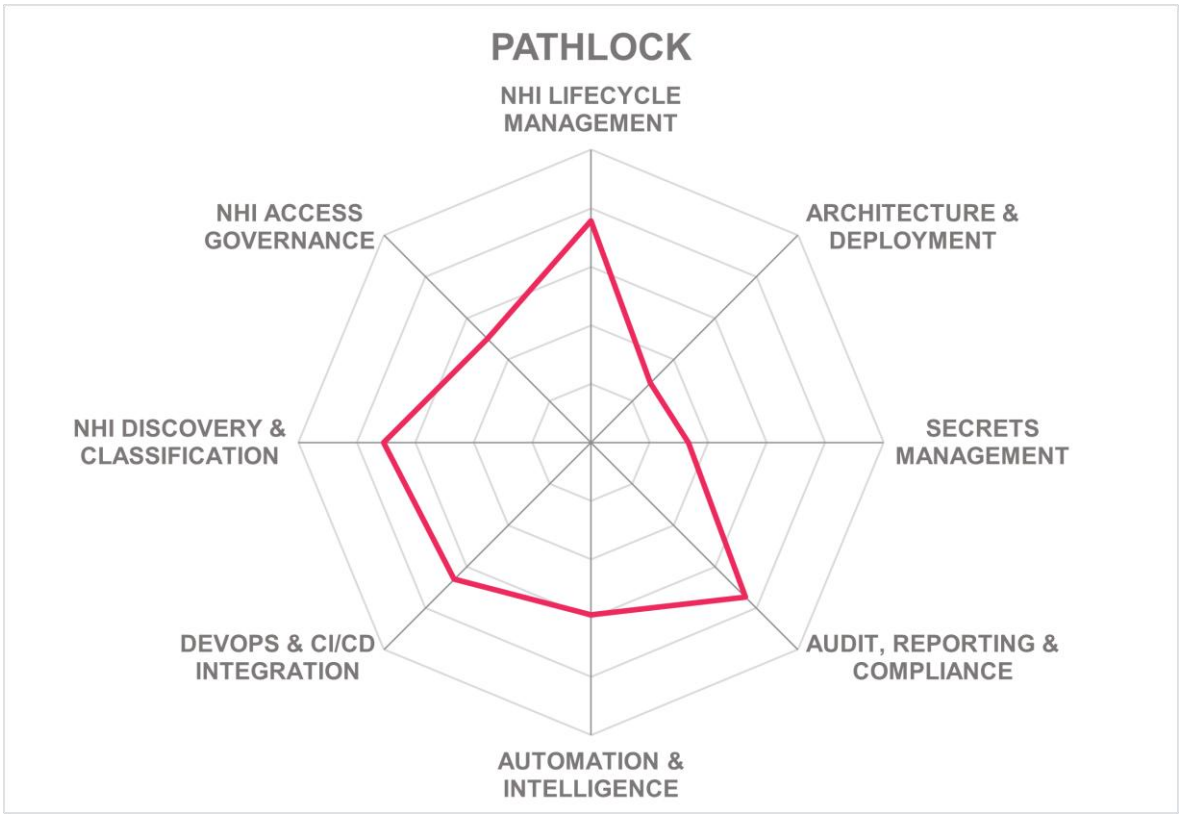
- Strong support for lifecycle activities such as discovery, classification, and decommissioning.
- Extensive integration support with major cloud-native identity systems.
- Policy-driven management with conditional and automated policy updates.
- Secrets management, with support for a variety of secret types and integration with third-party vaults.
- Strong support for audit, compliance, and monitoring capabilities.
- FIPS 140-3 encryption

Challenges

- Lacks support for JIT creation of NHIs for temporary workloads.
- Limited native integrations with CI/CD tools.
- Needs posture management functions.
- Potential improvements needed for real-time anomaly detection and behavioral analytics.

- Enhancing support for ephemeral secrets and short-lived credentials could align better with modern agile methodologies.
- Adding scalability in roadmap means there could be some limitations for managing high-volume NHIs right now

Pathlock – Pathlock Cloud



Founded in 2004, Pathlock is an identity security and application access governance platform and an emerging player in the NHIM domain. It has a significant presence across North America, EMEA, and APAC. The company offers solutions such as Pathlock Cloud and Pathlock Native, designed for deployment in public cloud environments and on-premises, respectively. Their licensing model is diverse, featuring per-user charges and modular options tailored to specific customer requirements, allowing integration with enterprise applications such as SAP and Oracle.

Pathlock manages all types of NHIs focusing on essential lifecycle elements like discovery, posture management, and responses. JIT creation is available however IaC provisioning is not yet supported. It provides identity management options for Microsoft Azure. Pathlock's workflows are customizable. The platform supports bulk import, lifecycle status reporting, metadata enrichment, and mapping of NHIs.

While Pathlock does not currently support sidecars or serverless functions directly, it offers REST APIs that enable integration within DevOps and CI/CD processes. Although direct SDK support is absent, the platform facilitates DevOps functionalities, including key CI/CD integrations and context-aware access. Automation of policy adherence within CI/CD

workflows is supported, accommodating tools like GitHub Actions and Terraform for secure secrets management.

Pathlock's current offerings do not include native secrets management or vaulting. However, future integration with Azure Key Vault is planned. This is aimed at bridging the gap between ERP identity risk management and enterprise secrets security. As such, reliance on third-party tools remains necessary for managing secrets encryption, rotation, and lifecycle, presenting a target area for future enhancements.

Pathlock offers audit trails, real-time identity behaviour monitoring, and integration with SIEM platforms like Splunk and Microsoft Sentinel. Detailed reports policy enforcement, and access violations align closely with compliance requirements. Anomalies and privilege escalations are detected, and role-based policy updates are facilitated. However, the platform's AI-driven capabilities remain underdeveloped, with opportunities for enhancements in real-time anomaly detection and automated risk evaluation.

Pathlock's strategic roadmap includes integrating secrets management and AI-driven insights to enhance ERP governance. Pathlock has achieved SOC Type 2 certification. Incident support is robust, with expert assistance available for remediation. While excelling in ERP-centric identity management, Pathlock faces challenges in native secrets management. Overall, Pathlock's solution is well-suited for organizations aiming for strong NHI lifecycle management however, it faces challenges in native secrets management.

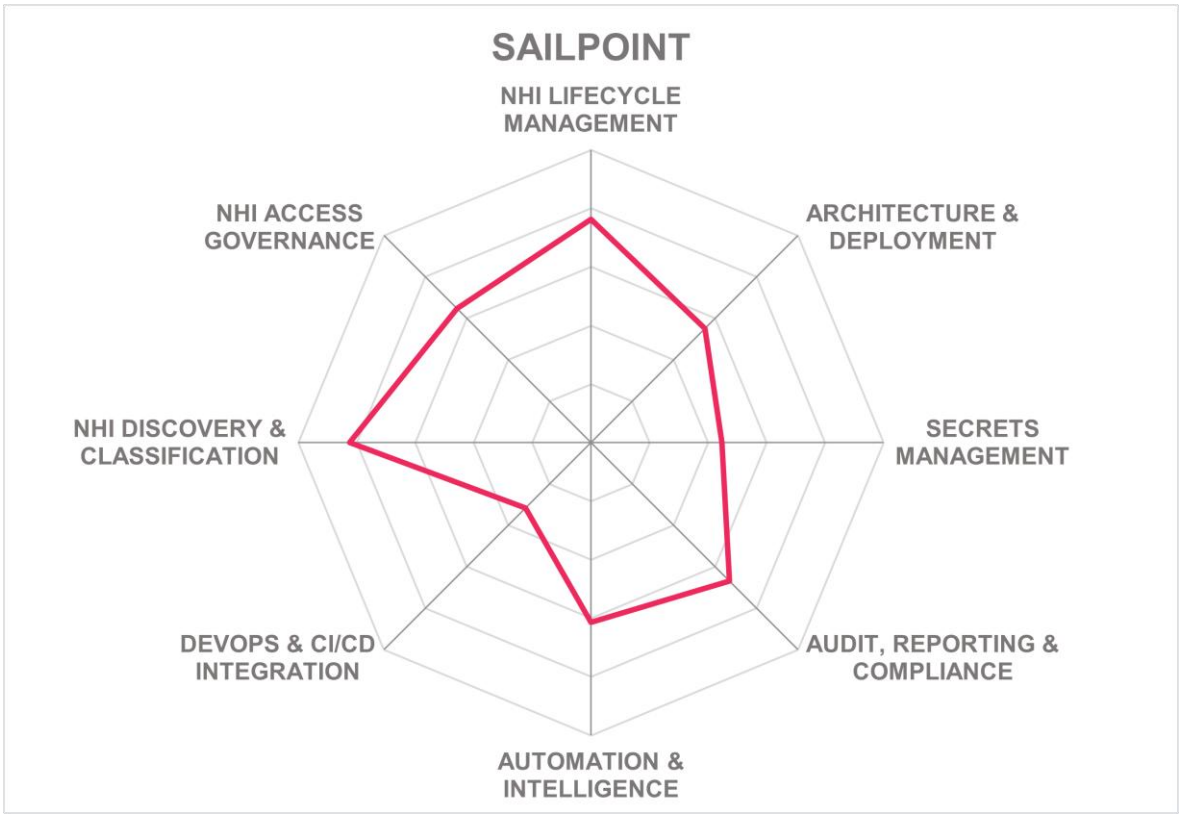
Strengths

- Supports backend applications and integration bots, with strong identity lifecycle features.
- JIT creation of NHIs for temporary workloads.
- Integration with Microsoft Azure cloud-native identity systems.
- Secure deployment models supporting cloud, on-premises, and hybrid configurations.
- Audit, monitoring, and SIEM integration capabilities.

Challenges

- Lacks broader support for identities such as virtual machines, CI/CD tools, and microservices.
- Absence of a built-in secrets management system and third-party vault integrations.
- Missing real-time AI/ML analytics for advanced anomaly detection and risk evaluation.

SailPoint – Identity IQ, Identity Security Cloud



Leader in

Founded in 2005 and headquartered in Austin, Texas, SailPoint Technologies has established itself as a leader in identity governance. SailPoint has a global market presence. SailPoint's product portfolio includes SailPoint Identity Security Cloud and SailPoint IdentityIQ. The solution is primarily delivered as SaaS, although on-premises options are available. Licensing models include per user and subscription-based formats.

SailPoint support for NHIs is limited. It currently supports web applications, backend applications, mobile applications, cloud-native service accounts, integration bots, IoT devices, and devices however support for virtual machines, CI/CD tools and pipeline agents, containers, microservices, service-mesh components, AI/ML pipelines, connected edge systems, custom automation scripts, and API clients is missing The solution supports all major lifecycle management events such as discovery, inventory, classification, posture management, and decommissioning. Their machine identity coverage focuses on security posture management, automated mapping, and application ownership association. Though JIT creation is not supported, provisioning through IaC and cloud-native identity systems is

available. The solution supports customizable onboarding workflows, delegated lifecycle management, and capabilities to flag inactivity. Bulk import and lifecycle status reporting are also supported.

The solution does not offer integrated serverless functions for sidecar injections, yet it supports various API protocols such as REST, SCIM, and OAuth. SDKs are available primarily for Python and Go, while CLI tools are available for DevOps capabilities. While the platform does not replace DevOps secrets management tools, it does support integrations and toolkits for CI/CD enhancements, particularly with GitHub Actions and GitLab CI/CD.

SailPoint's secrets management is facilitated through a native secrets vault that encrypts at rest and in transit. The vault integrates with third-party systems such as AWS Secrets Manager and Azure Key Vault. Though some advanced features like automatic secret expiry notification are lacking, the platform supports encryption and metadata tagging for secure secret handling and management.

Audit and compliance within the SailPoint solution are supported through lifecycle logging, behavioural anomaly detection integrated with SIEM platforms, and a wide range of compliance reporting templates such as FERPA, FISMA, FIPS 200, GDPR, HIPAA, CCPA, NERC CIP, NIST SP 800-53, PCS DSS, SOX, PSD2, and CIS. Analytics are powered by machine learning capabilities that offer insights into identity and entitlement anomalies. SailPoint’s AI-driven insights capabilities include support for automatic discovery of enterprise applications, provides tailored recommendations for configuring sources, and optimizing the onboarding experience. Additionally, AI-driven tools support enhanced access modelling and adaptive security measures while aligning with privacy standards.

SailPoint's platform is well-suited for organizations with extensive digital and cloud-based infrastructures, particularly in industries such as finance, healthcare, and manufacturing. SailPoint’s roadmap includes advancing non-human identity provisioning, deepening integration with AI agents, and expanding lifecycle management capabilities. SailPoint is certified to key standards like ISO/IEC 27001, SOC Type 2 and FedRAMP. SailPoint's core strengths lie in its identity governance capabilities, yet opportunities remain to expand serverless and secrets management functionalities.

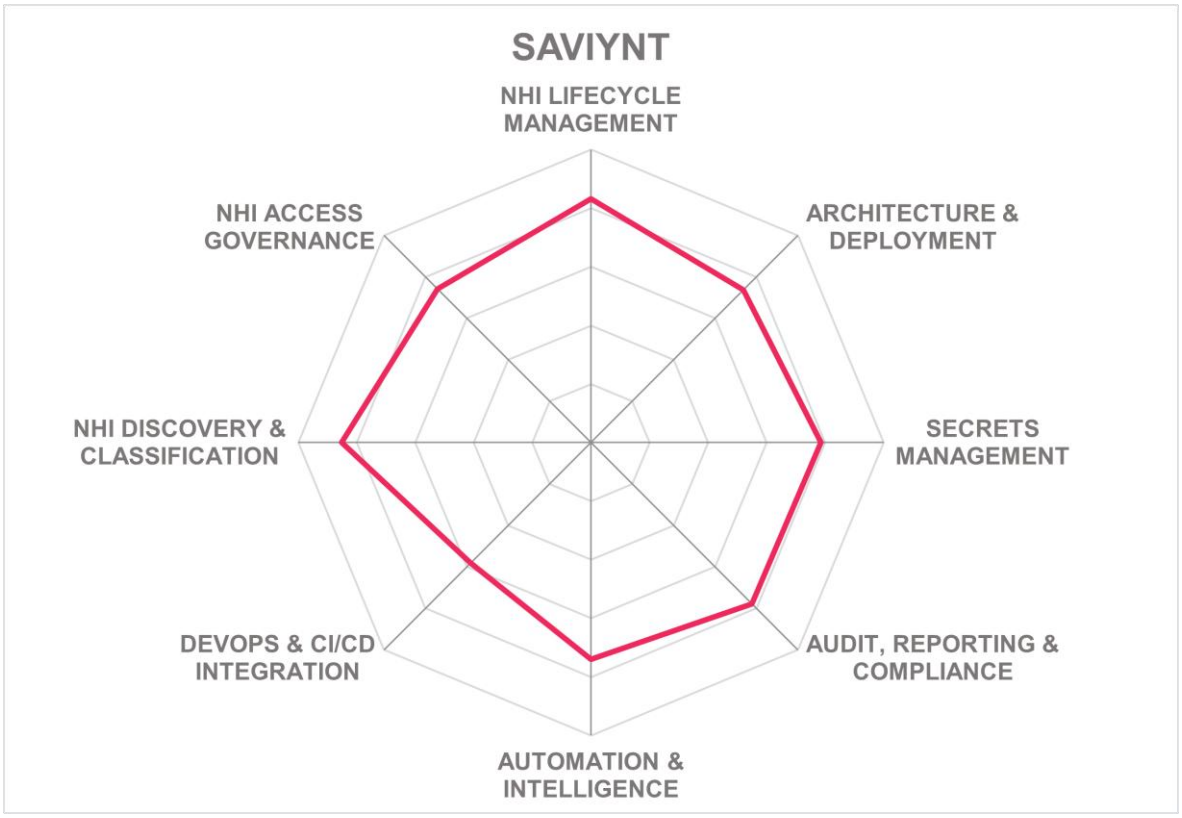
Strengths

- Strong automated discovery and classification features.
- Multi-tenant SaaS unified platform with robust microservices architecture ensures scalability and high availability.
- Compliance support with audit trails and reports supporting major compliance frameworks.
- Strong Agentic AI security capabilities.
- Strong market presence with global partner network.

Challenges

- Limited functionality in certain advanced DevOps and CI/CD integrations, particularly around policy automation.
- Real-time risk scoring and behavior monitoring for NHIs are on the roadmap and not fully developed.
- Overall several missing features for NHIM such as breadth of NHIs supported.

Saviynt – Saviynt Identity Cloud



Leader in

Founded in 2010 and headquartered in U.S., Saviynt is a key player in the IAM domain with its primary solution, Saviynt Identity Cloud. The company operates in North America, EMEA, and APAC. Saviynt provides a range of deployment options including on-premises, public cloud, and private cloud configurations. Licensing models include per user pricing, with variations for different product tiers. Their identity platform supports integration with containers such as Docker and Kubernetes, and interfaces with widely used cloud services including AWS, Azure, and Google Cloud.

Saviynt supports managing virtual machines, CI/CD tools and pipeline agents, containers, microservices, web applications, backend applications, service-mesh components, cloud-native service accounts, integration bots, AI/ML pipelines, custom automation scripts, and API clients, but it does not support mobile applications, IoT devices, connected edge systems, or non-specified types. They support all major lifecycle events for NHIs. Additional support extends to JIT creation and IaC deployments, as well as integrations with cloud-

native identity systems for AWS, Azure, and Google Cloud. A key differentiation is their expansions to support Oracle Cloud Infrastructure and AI-specific identities. Saviynt provides capabilities around workflow customization, templates, and advanced mapping. This framework also supports the automated management, reporting, and metadata enrichment of NHIs.

Saviynt's solution includes integration support for development processes, though it lacks sidecar support for secrets delivery. It does not have a DevOps tailored CLI, but it does support thorough REST API support . SDK offerings are limited to JavaScript. Dynamic secrets injection is possible. However, more native integration with popular CI/CD tools could enhance its capabilities.

Saviynt has built-in secrets management capable of secure API key and token storage. It supports both static and dynamic secrets. Their secrets vaulting process leverages policy-based access and encryption at rest and in transit. Automatic flagging of idle identities and enabling automated secrets rotation is supported. The system includes strong identity verification and supports integration with third-party vaults like AWS Secrets Manager and HashiCorp Vault.

Saviynt supports audit and compliance through logging and monitoring capabilities by providing detailed lifecycle and access activity reports. Saviynt's tools support recording of NHI activities and align with major compliance frameworks such as FISMA, FIPS 200, GDPR, HIPAA, CCPA, NERC CIP, NIST SP 800-53, PCI DSS, PSD2, CIS, and additional standards like FedRAMP and BASEL III. The solution supports automated alerts and risk management policies, but it has limited functions for real-time adaptive analytics and AI-driven insights. The analytics features focus more on anomaly detection and identification.

Saviynt targets enterprises in various sectors, including manufacturing, finance, and technology. The roadmap includes leveraging AI to enhance governance capabilities and behaviour analytics. Saviynt supports multiple standards and certifications including FIPS 140-2, NIST 800-57 Key Management, ISO/IEC 15408, PCI-DSS v3.2, ISAE 18 SOC 2 Types 1 and 2 as well as France SecNumCloud and Germany C5 standards. Saviynt remains a strong contender for organizations seeking identity management solutions with extensive deployment and lifecycle management capabilities.

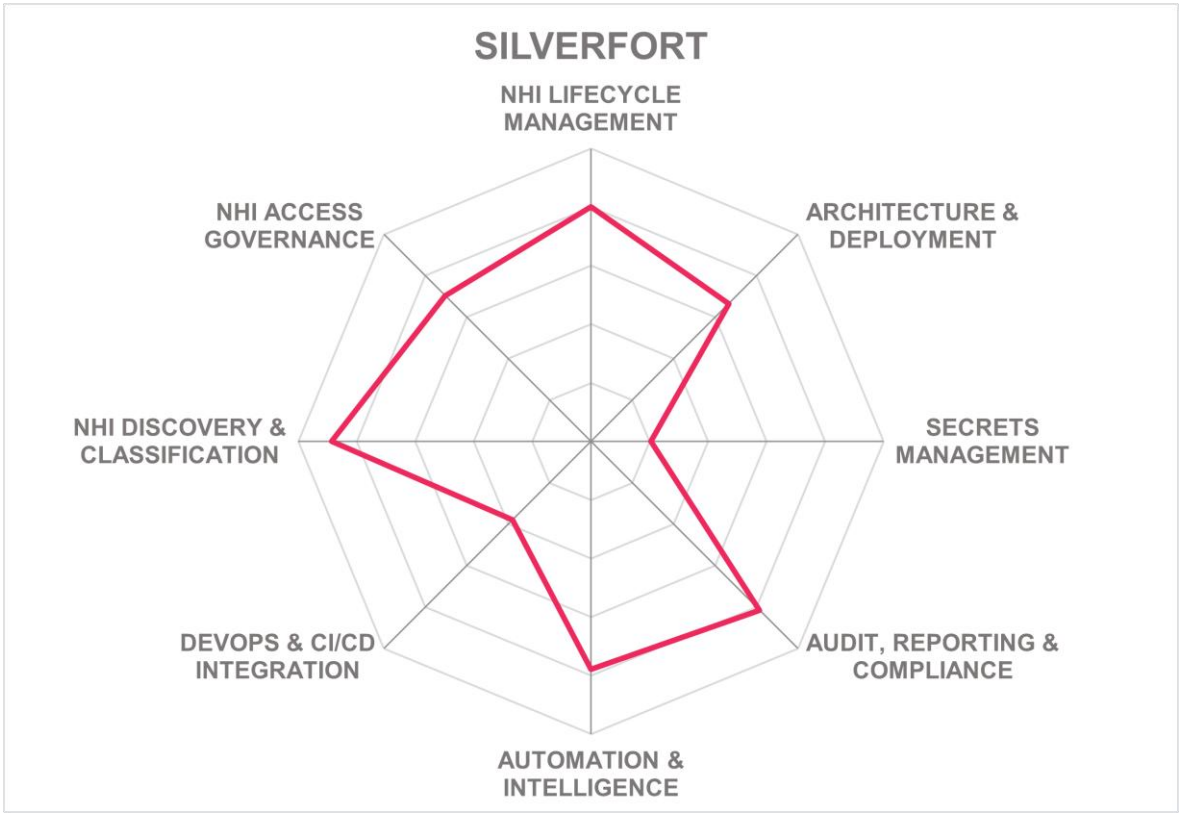
Strengths

- Unified identity control platform integrating human, machine, and privileged identities for consistent governance.
- Access certification for NHIs is strong
- Good feature set for secrets management, including encryption, rotation, and integration with external vaults.
- Excellent coverage of major compliance frameworks.
- Support for AI specific identities

Challenges

- Needs to advance real-time monitoring and AI-driven administration capabilities.
- Lacks behavioral analytics engine.
- Needs to expand integration for deeper DevOps and more CI/CD tools.
- Support for some NHI types is missing but extending support from next year

Silverfort – NHI Security



Founded in 2016 and based in US, Silverfort offers a solution for service account protection, and more recently added cloud-NHI security after its acquisition of Rezonate in late 2024. Its related products focus on areas such as Privileged Access Management, AI agent security, identity segmentation, MFA, ITDR and ISPM. Silverfort offers multiple deployment models including on-premises, public cloud, private cloud, and container-based systems through Kubernetes and Docker. It is licensed per-user and offers cost variations based on company size and usage needs.

Silverfort offers a unified identity security platform. Their platform is powered by patented Runtime Access Protection (RAP). This provides native integration with existing IAM infrastructures without requiring proxies or agents. It sees every authentication request going through Active Directory, enforcing security controls like MFA, JIT, and Virtual Fencing. It works parallelly with AD's native protocols by letting AD continue doing the authentication while Silverfort enforces security controls like MFA, JIT, and Virtual Fencing which avoids breaking applications, changing credentials, or altering workflows

Silverfort secures a wide range of NHIs including service accounts, virtual machines, CI/CD tools, containers, microservices, web applications, backend applications, service-mesh components, mobile applications, cloud-native service accounts, integration bots, AI/ML pipelines, IoT devices, connected edge systems, custom automation scripts, API clients, and devices. The solution addresses most lifecycle elements such as inline protection, discovery,

inventory, classification, posture management, detection and response; however, support for decommissioning, vaulting and rotation is not available. The platform supports virtual fencing of service accounts, JIT creation, and integration with IaC for provisioning. It extends support for multiple cloud identity systems and offers templates for managing identity workflows. The solution includes capabilities for bulk or batch import, automatic discovery, and lifecycle status reporting. It also offers a “Smart Policy” feature, where it uses behaviour analytics to group service accounts automatically and applying policy templates with real time enforcement.

Though Silverfort does not support sidecar injection, it does manage secrets in serverless environments. The platform provides extensive API support with RESTful interfaces but does not currently offer SDKs. In terms of DevOps integration, Silverfort collaborates with CI/CD tools such as GitLab CI/CD and CircleCI, although it does not handle dynamic secret injection or direct CLI usage. Silverfort takes a different approach to DevOps and CI/CD integration. Inline enforcement and virtual fencing ensure that NHIs created through CI/CD remain secure.

Silverfort supports third-party secrets vaults such as AWS Secrets Manager, Google Secret Manager, and Azure Key Vault. It does not have its own vault at present.

Silverfort provides real-time monitoring and audit trails for identity lifecycle events. It can generate alerts for anomalies, performs behavioural analytics, and generates compliance reports aligned with major frameworks such as GDPR, NERC CIP, NIST SP 800-53, PCI DSS, SOX, HIPAA and industry standards like OWASP NHI Top 10 risks. Silverfort’s platform offers advanced functionalities such as privileged access security and AI Agent security. Their innovative "Virtual Fencing" capability restricts service accounts to predetermined touchpoints. Their solutions provide actionable insights and recommendations.

Silverfort's NHI solution is well-suited for a diverse range of industries with hybrid environments including finance, insurance, manufacturing, healthcare, government, and utilities, with its customer base predominantly composed of medium to large enterprises. Silverfort plans to introduce features like secrets rotation and to expand integrations with third-party products. The platform is certified for ISO/IEC 27001 and SOC 2. While Silverfort exhibits strong capabilities, it also has areas for development, such as enhancing native integrations with CI/CD tools.

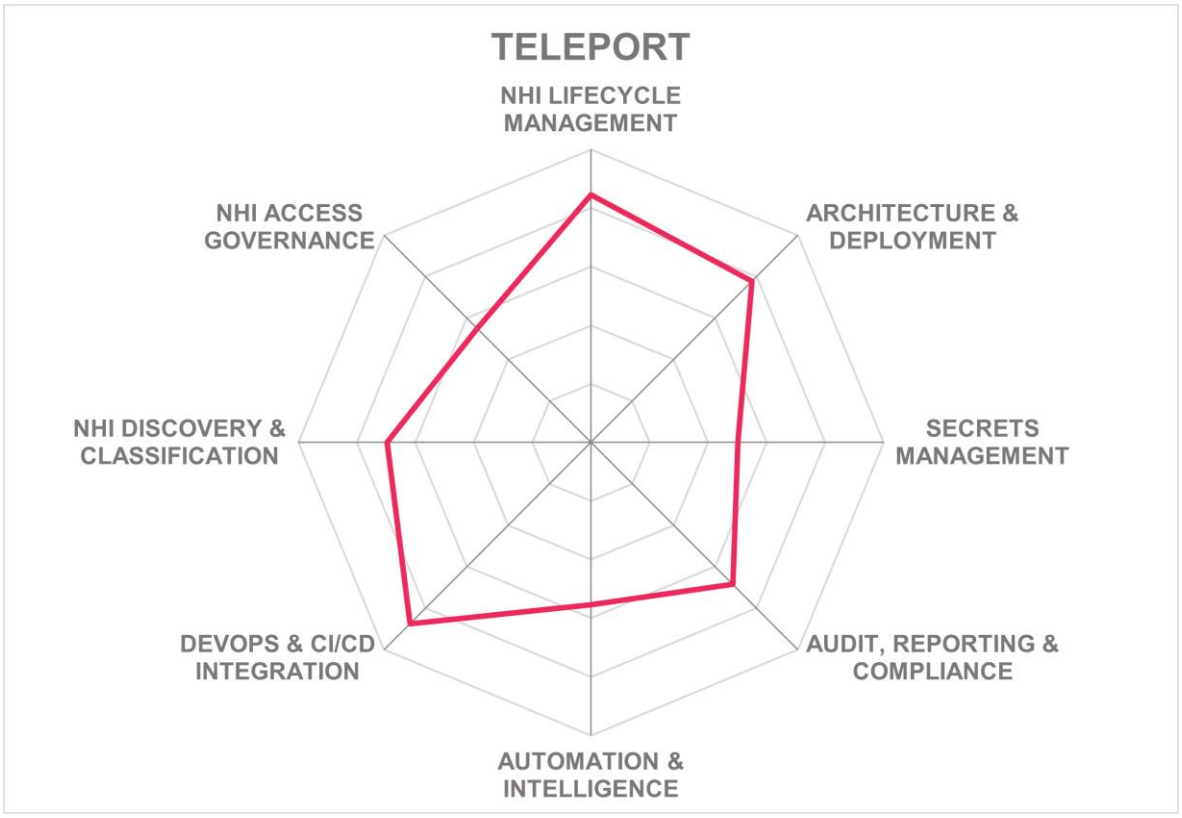
Strengths

- Unified platform for human, non-human, and agentic AI identities.
- Patented Runtime Access Protection.
- ‘Virtual Fencing’ capability restricts service accounts to predetermined touchpoints.
- Automated discovery and protection of service accounts.
- Integration with CMDB and other lifecycle management systems.
- Emphasis on inline, preemptive protection and automated remediation.
- Strong global market presence.

Challenges

- Rotation, vaulting, and decommissioning not supported but planned in roadmap.
- Expansion and better integration with third-party secrets vaults can further optimize secrets management.
- Support for SDKs is missing.

Teleport – Teleport Infrastructure Identity Platform



Founded in 2015 and headquartered in Oakland, California, Teleport is focused on providing support for managing NHIs through their Teleport Infrastructure Identity Platform. The platform is delivered as a SaaS and virtual appliances or containers such as Kubernetes enable on-premises and private cloud deployment options. Licensing models are based on usage-based metrics such as monthly active users.

Teleport supports virtual machines, CI/CD tools and pipeline agents, containers, microservices, web applications, backend applications, service-mesh components, cloud-native service accounts, integration bots, AI/ML pipelines, IoT devices, connected edge systems, custom automation scripts, API clients, and devices. It does not support mobile applications directly but offers support for mobile through Device Trust when coupled with human access. While it supports several lifecycle stages such as inventory management, security posture management, detection and response, identity rotation, and automatic decommissioning. Although it does not do traditional discovery and classification processes, it supports time-limited machine identities. Machine identities are managed effectively with workload identity federation and security posture management to continuously assess and ensure that security controls are implemented and maintained across various environments such as AWS, Azure, and Google Cloud. The platform supports JIT creation, IaC, customizable workflows and templates. It also offers delegated lifecycle management,

automatic decommissioning, and bulk import capabilities along with metadata and mapping features.

Teleport supports sidecar injection for secrets delivery, offers API access via gRPC, and provides an SDK for Go. Support for other APIs is currently missing. Its DevOps and CI/CD integrations support dynamic secret injections with native integration for tools like Jenkins and GitHub Actions. Automation extends to secrets policies and machine identities.

In terms of secrets management, Teleport uses a built-in certificate authority for identity issuance, but it can also support external certificate authorities. Teleport leverages TPM for authentication, cloud-native joining methods to make secrets and vaulting obsolete. Teleport provides SPIFFE support, as well as JWT and X.509.

Audit and compliance capabilities includes logging of all lifecycle events and interoperability with SIEM, SOAR, and ITSM systems. Although it does not natively generate reports for compliance frameworks, it purports to adhere to GDPR and HIPAA. Analytics are supported by AI/ML for anomaly and privilege misconfiguration detection.

Teleport's strengths lie in its ability to manage machine identities at scale, simplify identity governance through templated and automated workflows, and support built-in failover for high availability. However, the platform faces challenges in areas such as continuous and real-time behavioural analytics and adaptive risk-based policy adjustments, which remain on its roadmap. Teleport claims certifications for FIPS 197 Advanced Encryption Standard, FIPS 140-2 Cryptographic Module Standards, NIST 800-57 Key Management, ISO/IEC 27001, PCI DSS v3.2, ISAE 18 SOC 2 Type 2, and HIPAA/HITRUST. Teleport's offerings are particularly suited for enterprises operating within multi-cloud and hybrid environments.

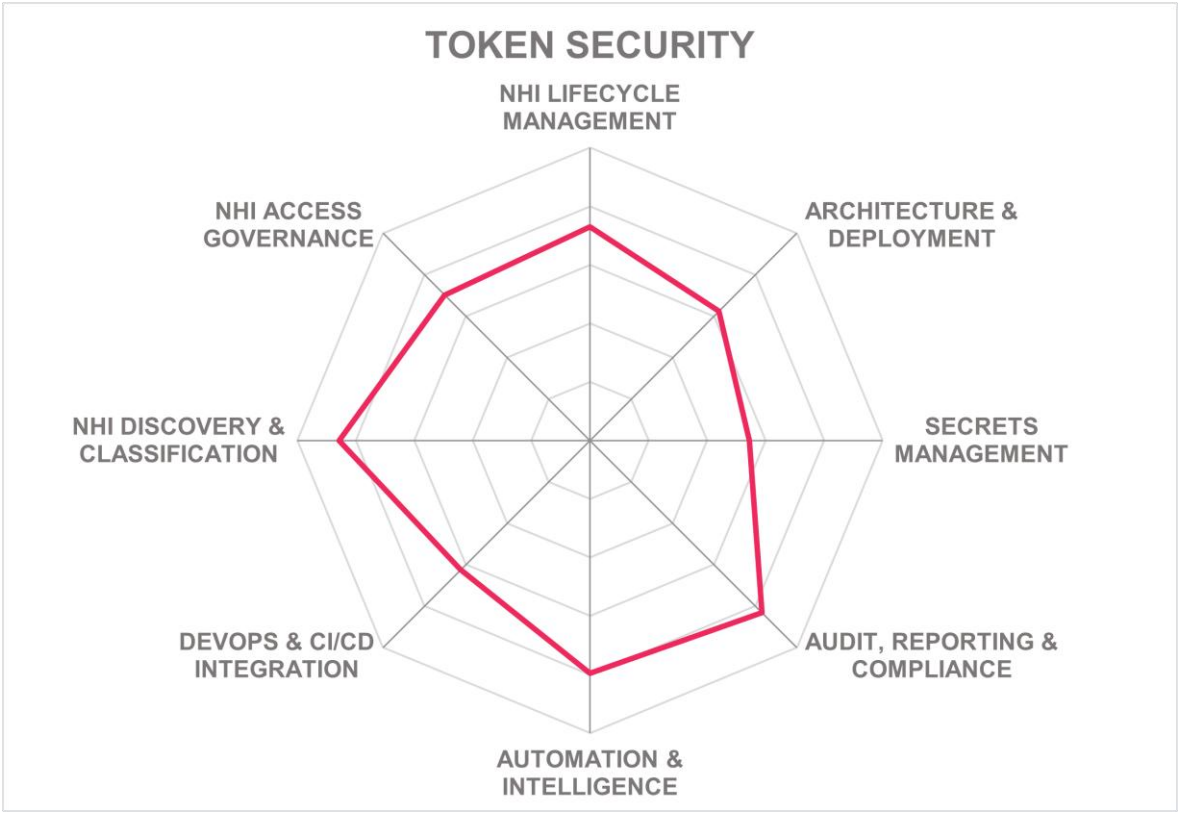
Strengths

- Strong DevOps and CI/CD integration capabilities.
- Diverse NHIs, including virtual machines, containers, microservices, and AI/ML pipelines.
- Supports JIT identity provisioning and infrastructure-as-code.
- Built-in failover and multi-region options enhance operational resilience and availability.
- The solution governs access and identity lifecycles through automated and templated workflows.

Challenges

- Real-time behavioral analytics for NHIs are not fully developed.
- Lacks adaptive, risk-based policy adjustments, relying on static configurations.
- Enhanced AI/ML-driven insights and anomaly detection capabilities need further development.

Token Security – NHI Security Platform



Founded in 2023, Token Security is an emerging vendor specializing in NHI solutions. Their customer base is mostly concentrated in North America and to a lesser extent the Middle East. Its principal offering is the fully integrated NHI Security Platform, deployed as SaaS, supporting Docker and Kubernetes for containerized environments. The product utilizes a lightweight, agentless architecture that integrates with existing identity systems, cloud services, SaaS applications, CI/CD, and AI platforms. The solution's licensing model is centred around charging per NHI.

Token Security supports a broad range of NHIs such as virtual machines, CI/CD tools, containers, microservices, web and backend applications, service-mesh components, mobile applications, cloud-native service accounts, integration bots, AI/ML pipelines, connected edge systems, custom automation scripts, API clients, and devices It does not support IoT devices. Lifecycle events supported include discovery, inventory, classification, posture management, detection and response, rotation, vaulting, decommissioning, continuous discovery, and reporting; however, the platform does not support just-in-time creation, customizable onboarding workflows, or lifecycle templates for repeatable deployments. It interoperates with cloud-native identity systems such as AWS, Microsoft Azure, Google

Cloud Platform, Okta, Entra ID, and HashiCorp Onboarding workflows cannot be customized. The solution allows bulk importation and offers full lifecycle status reporting.

Serverless functions and sidecar injections are not supported. Token Security provides extensive API integration covering SOAP, REST, SCIM, and LDAP protocols, but it does not provide SDKs. For DevOps and CI/CD, the platform supports Jenkins, GitHub Actions, GitLab CI/CD, CircleCI, Azure DevOps, and Bitbucket. It lacks dynamic secret injection and GitOps support. Token Security places a high emphasis on API-operated provisioning. Moreover, Token Security supports policy enforcement and governance for NHIs.

Token Security does not have its own vault but interoperates with third-party vaults such as AWS Secrets Manager, Akeyless Vault, CyberArk Conjur, Google Secrets Manager, Azure Key Vault, and HashiCorp Vault. It discovers and secures both static and dynamic secrets, supports automated secret rotation, tagging, and metadata enrichment. Its NHI Risk Graph feature graphically displays NHIs, what they connect to, who the owner is, and what secrets are deployed.

Auditing and compliance features include logging, reporting on lifecycle events, privileged access monitoring, and SIEM integration via Splunk. Token Security's platform utilizes AI/ML for dynamic risk analysis, anomaly detection, and remediation. It supports automated secrets rotation and privilege adjustments for real-time decision-making and managing NHIs across cloud-native environments.

Token Security's offerings are particularly applicable for enterprises situated in dynamic, hybrid, or multi-cloud environments. Token Security’s roadmap includes enhancing AI/ML-driven features, including real-time identity behavioural tracking and machine identity graphs. Token Security's platform is certified for ISO/IEC 27001 and SOC Type 2. Token Security is well-suited for organizations seeking robust NHI management across multi-cloud environments.

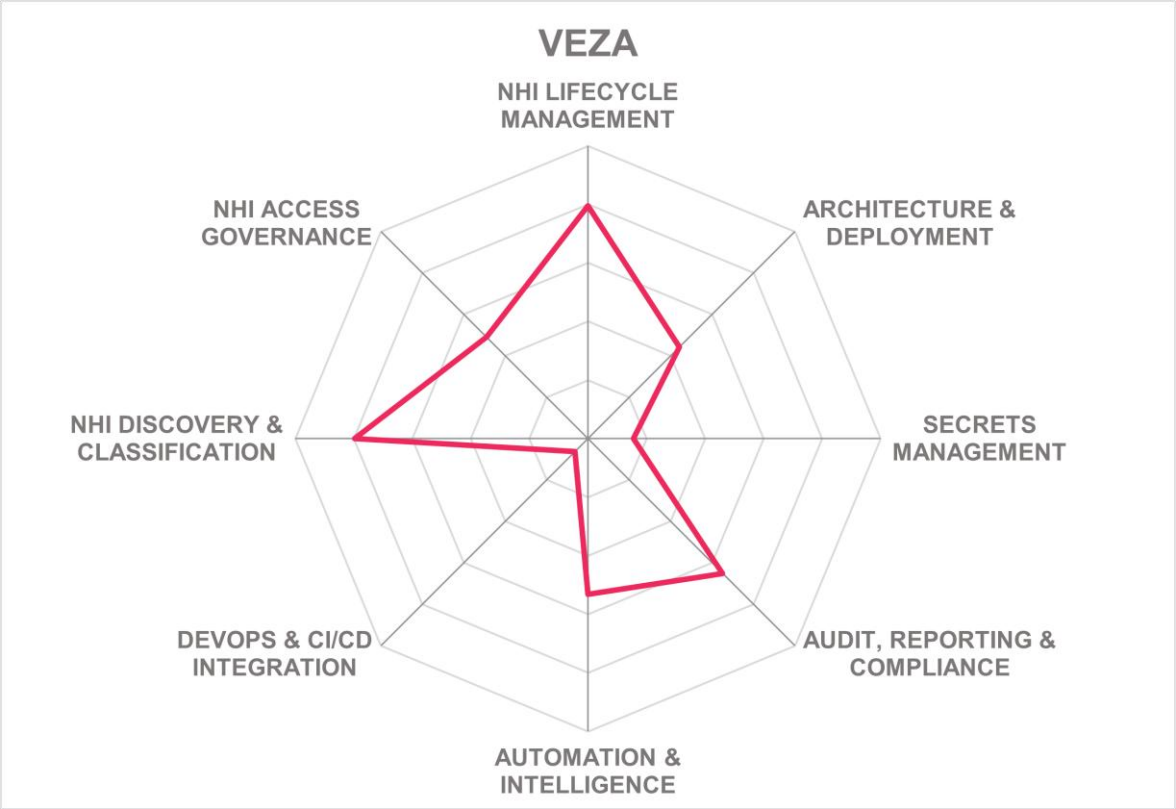
Strengths

- Excellent discovery and classification capabilities.
- Works with a wide range of NHI types.
- Good role-based access controls and policy management capabilities.
- Management of a wide range of NHIs across their lifecycles.
- Auditing and monitoring dashboard captures lifecycle and compliance metrics.
- ISO27001 and SOC Type 2 certified.
- AI/ML models for real time decision-making, dynamic risk scoring, and privilege escalation.

Challenges

- Lacks built-in secrets management system, Relies on third-party vaults.
- Absence of JIT identity provisioning for temporary workloads, limiting usefulness for specific cloud-native scenarios.
- Lacks support for risk-adaptive policy adjustments.
- Onboarding workflows cannot be customized.
- Limited market presence.

Veza – Veza Access Platform



Founded in 2020 and headquartered in Redwood City, California, Veza delivers identity security and governance across human and non-human identities in SaaS, cloud, and on-prem environments. The platform is primarily deployed as a cloud service, with the option for private cloud deployment in customer-managed environments. Subscriptions are priced per active identity, product, and integration. Veza has monthly subscription-based pricing per active Identity, per product, and per integration

Veza supports virtual machines, CI/CD tools, containers, microservices, web applications, backend applications, service-mesh components, cloud-native service accounts, integration bots, custom automation scripts, and API clients. It does not support mobile applications, AI/ML pipelines, IoT devices, connected edge systems, or other devices. Veza supports lifecycle elements like discovery, inventory, classification, posture management, and continuous discovery. The platform supports machine identities, enabling service account scoping and security posture management. Although JIT creation is not currently available, support for IaC provisioning is provided. Veza facilitates NHI onboarding workflows and provides templates. It provides for delegated lifecycle management, inactivity detection, de-provisioning, and bulk import. Furthermore, it has lifecycle status reporting, metadata enrichment, and identity mapping functions.

Veza does not support sidecar injection for secrets or serverless functions. REST APIs and OAuth protocols are supported. Veza connects via APIs and integrations rather than SDKs. This is designed for agentless operation. The platform does not provide native CI/CD integrations or plugin support for popular DevOps tools Despite the lack of CLI offerings and automated secrets management within DevOps workflows, Veza does have governance functionalities to complement existing CI/CD systems. In terms of secrets management, Veza has a limited built-in system which secures internally generated secrets rather than functioning as a vaulting service. It interoperates with third-party vaults such as AWS Secrets Manager, Google Secrets Manager, Azure Key Vault, and HashiCorp Vault for classification and tagging ownership of secrets.

Veza maintains audit trails for NHI lifecycle events and generates standardized compliance reports for GDPR and HIPAA. Veza's access graph is a visualization of identity relationships, and it maps permissions and resources across connected systems. Analytics and automation capabilities include dynamic risk scoring and customizable workflows. The platform does not use ML for anomaly detection or real-time behavioural insights. The absence of adaptive, risk-based policy adjustments is also noted. Veza’s Access AI introduces natural-language analytics and role/permission recommendations. Anomaly detection and behavioural insight generation are in development.

Veza’s roadmap includes addressing new NHI types, expanding auto-detection capabilities, and real-time identity behavioural tracking and management of AI agent identities. Veza is certified for ISO 27001, PCI-DSS, and SOC 2. Veza does have some limitations in secrets management and DevOps integration, but their strength is in their identity governance approach. It is a good fit for enterprises seeking centralized visibility and risk management across complex identity landscapes.

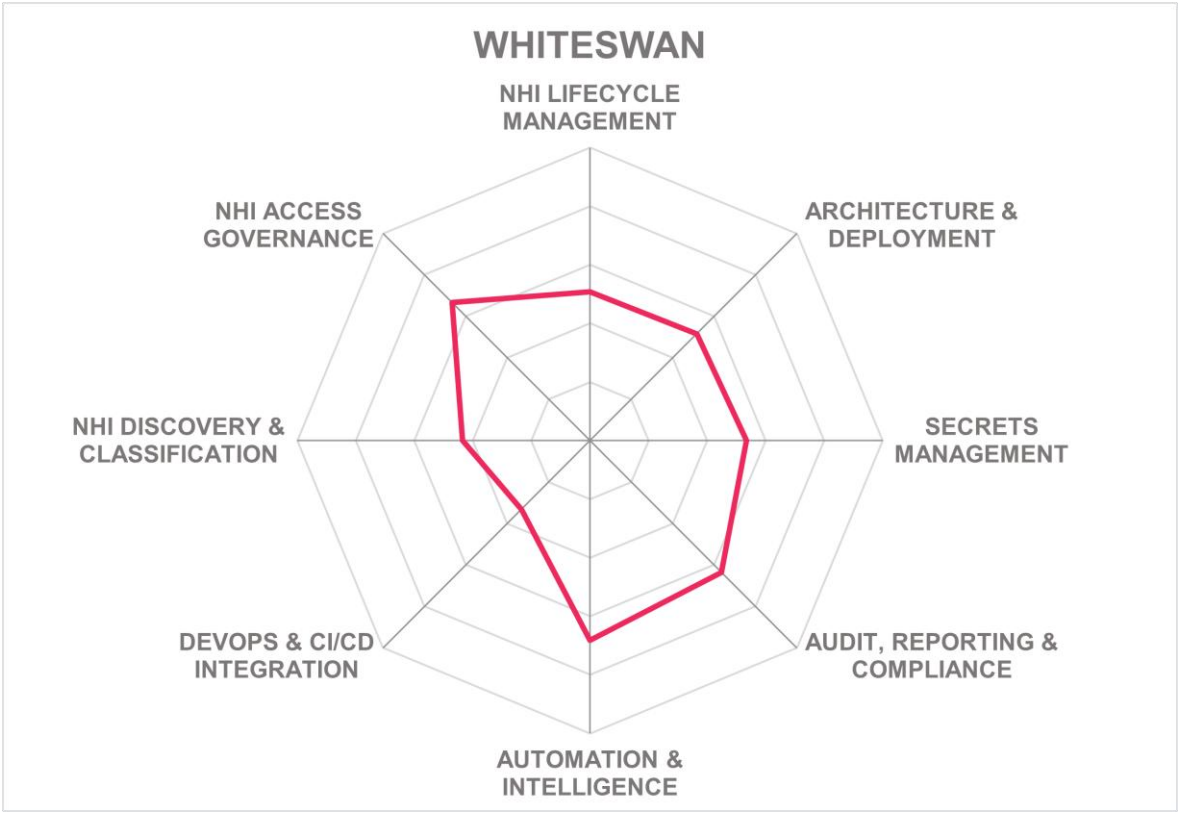
Strengths

- Access Graph delivers unified, real-time visibility of every identity-to-permission-to-data relationship.
- Unified governance for both human and non-human identities across multi-cloud environments.
- Strong discovery and classification for NHIs, with posture scoring and ownership mapping.
- Advanced auditing and compliance dashboards for rapid least-privilege enforcement and continuous authorization.
- Orphaned NHIs can be auto tagged for ownership reassignment.
- Supports a wide range of analytics and intelligence use cases.

Challenges

- Absence of JIT identity provisioning.
- Real-time behavioral analytics and dynamic policy adjustments are planned under Access AI roadmap.
- Cannot adjust policies based on real-time risk analysis.
- SDK, Sidecar injection and serverless support are currently not prioritized in favour of agentless architectures.
- Support for some NHI types is missing but will be addressed in roadmap.

Whiteswan – Whiteswan ITDR



Founded in 2023 and based in California, USA, Whiteswan Security is a newcomer in the NHIM space. Whiteswan Security's customer base is spread across APAC, EMEA, and North America. It can be deployed on-premises, in public clouds or private clouds, and hybrid environments. It supports SaaS deployment along with support for containerized deployment. Key products include Whiteswan ITDR, a suite focused on identity threat detection and response. Increase functionality and innovation rating for just in time feature.

Whiteswan Security supports a wide range of NHIs including virtual machines, containers, web applications, backend applications, cloud-native service accounts, integration bots, AI/ML pipelines, custom automation scripts, and devices, but not CI/CD tools, microservices, service-mesh components, mobile applications, and IoT devices. Whiteswan's solution addresses essential lifecycle elements including discovery, posture management, detection, response, and automated deprovisioning. The solution supports JIT creation and IaC provisioning, and integrates with major cloud identity systems such as AWS, Azure, and GCP. Customizable workflows, bulk identity import, and metadata and dependency mapping are supported.

Whiteswan Security supports REST APIs for provisioning and managing NHIs and, although SDK availability for various programming environments is not indicated. DevOps and CI/CD processes are supported by enabling dynamic interaction with secrets and facilitating the automation of identity and secret management tasks. However, it currently does not provide native support for specific CI/CD tools, sidecar injection, or serverless functions

Whiteswan encrypts and automatically rotates both static and dynamic secrets. It interoperates with third-party secrets vaults such as AWS Secrets Manager and Azure Key Vault. Its vaulting solution is compliant with FIPS 140-3 standards. It enables policy-based access controls. The secrets management capabilities extend to API keys, tokens, SSH keys, and various credentials such as database credentials, and TLS/SSL certifications

Whiteswan Security's AI/ML capabilities include providing support for adaptive access controls, and dynamic privilege adjustments. Real-time behaviour tracking and anomaly detection are included.

Detailed audits and monitoring dashboards are available, despite some strong foundational functionalities, Whiteswan currently lacks in some areas, such as the absence of built-in support for CI/CD integration . Whiteswan Security's platform supports FIPS 140-3 compliance. Whiteswan is actively addressing these limitations, including improvements in workload identity security and Snowflake NHI, as indicated in its roadmap for future deployments. Whiteswan is suitable for sectors like technology, finance, or any industry prioritizing automated identity management, adaptive security measures, and seamless integration with cloud-native systems

Strengths

- FIPS 140-3 compliance
- Integrated secrets management system with capability for third-party vault integration.
- Strong lifecycle management features including posture management and vaulting.
- Versatile deployment options suitable for modern and traditional IT environments.
- Strong alignment with cloud-native identity systems and infrastructure-as-code.
- AI/ML-driven analytics and automation support adaptive access control and intelligent risk-based policy enforcement

Challenges

- Lacks native CI/CD integration capabilities limiting DevOps alignment.
- Limited capability in customization of onboarding workflows and automatic policy updates.
- Support for some NHIs is missing.

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.

Astrix

Astrix, founded in 2021 and headquartered in Tel Aviv, Israel, focuses on securing NHIs connected through third-party integrations and APIs. Its platform detects and manages service accounts, tokens, and OAuth connections across SaaS, IaaS, and PaaS environments. Astrix provides continuous visibility into the relationships between applications and cloud services to uncover hidden access risks. The solution offers automated remediation workflows to reduce exposure from unused or overprivileged connections.

Why worth watching: Astrix offers an innovative approach to controlling non-human access by managing API and integration-based identities that often remain outside traditional IAM visibility.

AWS

Amazon Web Services (AWS) provides a wide range of identity and access management capabilities designed to secure human and NHIs across its cloud ecosystem. Through AWS IAM, Secrets Manager, and IAM Roles Anywhere, organizations can manage workloads, service identities, and secrets within and beyond AWS environments. The platform's integration with native and third-party security tools supports automation and fine-grained policy enforcement at scale.

Why worth watching: AWS continues to evolve its non-human identity controls, embedding stronger governance and lifecycle management into the broader AWS security framework.

Axiad

Axiad, founded in 2010 and based in Santa Clara, California, delivers an identity-centric platform that unifies credential and access management for both human and machine identities. Its cloud service integrates PKI, FIDO2, and certificate lifecycle management into a cohesive environment. Axiad's centralized approach enables organizations to automate certificate issuance and renewal, reducing operational overhead and minimizing the risk of credential-related outages.

Why worth watching: Axiad's integrated platform offers consistent management of digital certificates and credentials across users, devices, and workloads, supporting stronger machine identity governance.

Axis Now

Axis Now, headquartered in Austin, Texas, offers a platform that simplifies access control across distributed infrastructure by securing machine-to-machine communication and service authentication. Its solution provides centralized credential management, secret rotation, and visibility into service account usage. Axis Now's emphasis on simplicity and automation helps organizations reduce manual operations while enforcing consistent identity governance policies.

Why worth watching: Axis Now brings a practical approach to managing NHIs by integrating automation and visibility into credential management workflows.

Clarity Security

Clarity Security, founded in 2020 and based in Atlanta, Georgia, focuses on improving identity governance across human and non-human entities. The platform groups identity data from multiple systems to provide context, policy enforcement, and actionable insights. Clarity enables organizations to better understand entitlements and access paths, reducing complexity and improving compliance posture.

Why worth watching: Clarity Security's unified governance model brings much-needed visibility and policy control to non-human identity management within complex environments.

Corsha

Corsha, founded in 2018 and headquartered in Washington, D.C., delivers an API identity and access management platform purpose-built for securing machine-to-machine communication. It issues dynamic identities for APIs, providing continuous authentication and fine-grained access control. Corsha's solution enhances visibility into API traffic and helps enforce Zero Trust principles for non-human entities.

Why worth watching: Corsha's approach to dynamic API identity management strengthens the security of non-human communications across distributed systems.

Cycode

Cycode, founded in 2019 and based in Tel Aviv, Israel, focuses on securing software supply chains by protecting source code, build systems, and machine identities. The platform provides visibility into development pipelines, detecting risks related to service accounts, credentials, and automation tools. Cycode's policy-based approach helps align security and DevOps teams around enforcing consistent identity and access practices.

Why worth watching: Cycode integrates non-human identity management into software supply chain security, addressing a growing blind spot in DevOps environments.

Google

Google offers a comprehensive set of services for managing human identities and NHIs through its Cloud IAM, Workload Identity Federation, and Secret Manager offerings. These tools enable organizations to securely manage service accounts, credentials, and workload permissions across Google Cloud and connected environments. Google's automation and policy enforcement capabilities reduce credential sprawl while maintaining fine-grained control.

Why worth watching: Google continues to advance NHIM by embedding workload security and governance deeply within its cloud ecosystem.

P0 Security

P0 Security, based in San Francisco, California, provides a platform that discovers, monitors, and governs NHIs across cloud and development environments. Its solution maps relationships between workloads, APIs, and automation tools to identify unused or overprivileged identities. P0 Security integrates with CI/CD pipelines to prevent misconfigurations and enforce least privilege access.

Why worth watching: P0 Security delivers actionable visibility into non-human identity sprawl, helping organizations better secure automated and cloud-native workloads.

SlashID

SlashID, founded in 2022 and headquartered in New York, provides a unified identity platform that extends beyond user management to include NHIs such as APIs and workloads. Its architecture simplifies authentication and authorization across distributed applications using token-based access and centralized policies. The platform's developer-centric design facilitates secure integration within diverse environments.

Why worth watching: SlashID's unified approach to human and non-human identity management supports consistent access governance across varied application architectures.

Thales

Thales offers a broad portfolio of identity, access, and data protection solutions, including machine identity management capabilities through its CipherTrust and SafeNet platforms. The company supports certificate lifecycle automation, key management, and secure credential storage for both on-premises and cloud-based workloads. Thales integrates with existing IAM ecosystems to help organizations extend trust to non-human entities.

Why worth watching: Thales brings mature cryptographic expertise and lifecycle automation capabilities to managing NHIs across regulated environments.

TrustFour

TrustFour, based in Boston, Massachusetts, focuses on securing software infrastructure by managing credentials, secrets, and certificates used by applications and services. The platform detects unmanaged secrets and enables automated rotation and revocation. Its policy-driven framework provides consistent oversight of NHIs across development and production environments.

Why worth watching: TrustFour provides effective control and automation for managing service identities and secrets that underpin application security.

Unosecur

Unosecur, headquartered in Austin, Texas, delivers a cloud-native platform for managing secrets, certificates, and API keys across distributed environments. Its system unifies discovery, lifecycle management, and access control for NHIs. Unosecur integrates with CI/CD tools and runtime environments, allowing teams to secure machine credentials without disrupting workflows.

Why worth watching: Unosecur's focus on automation and visibility across the credential lifecycle supports scalable governance for NHIs.

Widas

Widas, founded in 1997 and based in Germany, provides identity and access management solutions through its cidaas platform. While known for customer and workforce identity, Widas has extended capabilities to include API and device identity management. The platform integrates with enterprise systems to deliver centralized authentication, authorization, and credential lifecycle functions.

Why worth watching: Widas expands its mature identity management framework to address non-human identity needs across connected systems.

WSO2

WSO2, established in 2005 and headquartered in Santa Clara, California, provides an open-source identity platform supporting both human and NHIs. Its Identity Server delivers advanced access management, API security, and federated identity capabilities. WSO2's extensible design enables organizations to integrate policy-based controls and automate non-human identity workflows across complex infrastructures.

Why worth watching: WSO2's open and extensible platform provides organizations with a flexible foundation for managing NHIs alongside existing IAM strategies.

Related Research

Advisory Note: Maturity Level Matrices for NHI Management

Advisory Note: Security for the agile IT: Bridging DevSecOps, NHI Management, PAM, CIEM, and more
Advisory Note: From Machine Identity to Agentic AI – Charting the NHI Continuum
Advisory Note: NHI and CIEM: Beyond Point Solutions towards Strategy
Blog: Mastering Non-Human Identity Governance for Enhanced Security and Efficiency
Blog: Non-Human Identity Management: Mature or Just Getting Started?
Blog: Rage Against the Machines: ITDR and the Rise of Non-Human Identities
Leadership Compass: Cloud Infrastructure & Entitlement Management (CIEM)
Leadership Compass: Cloud Security Posture Management
Leadership Compass: Container Security
Leadership Compass: Enterprise Secrets Management
Leadership Compass: SASE Integration Suites
Leadership Compass: Privileged Access Management
Leadership Compass: Identity Threat Detection and Response (ITDR)

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..