kuppingercole ANALYSTS

Identity Threat Detection and Response (ITDR)

Alejandro Leal

November 25

LEADERSHIP COMPASS 2025

This Leadership Compass explores the Identity Threat Detection and Response (ITDR) market. As digital identities have become the primary attack vector in modern cybersecurity incidents, ITDR has grown in importance as a complementary capability to traditional IAM. Effective ITDR solutions help organizations detect malicious activity involving identity systems and provide continuous discovery and visibility of identity assets. They also offer robust threat detection and accelerate investigations while supporting response and recovery efforts. This report analyzes the key players in the ITDR market in 2025, their technical capabilities and strategic direction, and provides practical guidance for organizations seeking to strengthen their identity defenses in the face of evolving threats.

Contents

Executive Summary

Identity is no longer just an IT issue. It is now a critical component of cybersecurity and business operations. There is growing consensus that identity misuse has overtaken other methods as the preferred mode of intrusion. For example, according to the 2025 Data Breach Investigations report, more than 80 percent of data breaches involve compromised identities, as adversaries exploit techniques such as Kerberoasting, brute force attacks, password spraying, and the abuse of misconfigured identity systems.

In addition to identity-based threats, the increasing reliance on Non-Human Identities (NHIs) introduces significant security and compliance risks. This is especially true when these identities are not properly managed. KuppingerCole's research suggests that the majority of identity-related breaches stem from compromised NHIs, particularly service accounts and API keys. While identity threat detection and response (ITDR) is often discussed in the context of human users, its application to NHIs is increasingly crucial. And as AI agents begin to act on behalf of humans, organizations face a critical governance challenge: how to establish trust in these systems, monitor their behavior, and enforce guardrails when automated actions deviate from expected norms.

To make matters more complicated, organizations typically operate a combination of different systems and applications, including those dedicated to privileged access

management (PAM), Identity Governance and Administration (IGA), and those serving as identity providers, such as single sign-on (SSO) platforms. They also use cloud-based services, on-premises servers, and integrations into Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools. This creates a dispersed "identity fabric" in which many components are managed separately. As a result, organizations face challenges in maintaining visibility and control across the entire landscape.

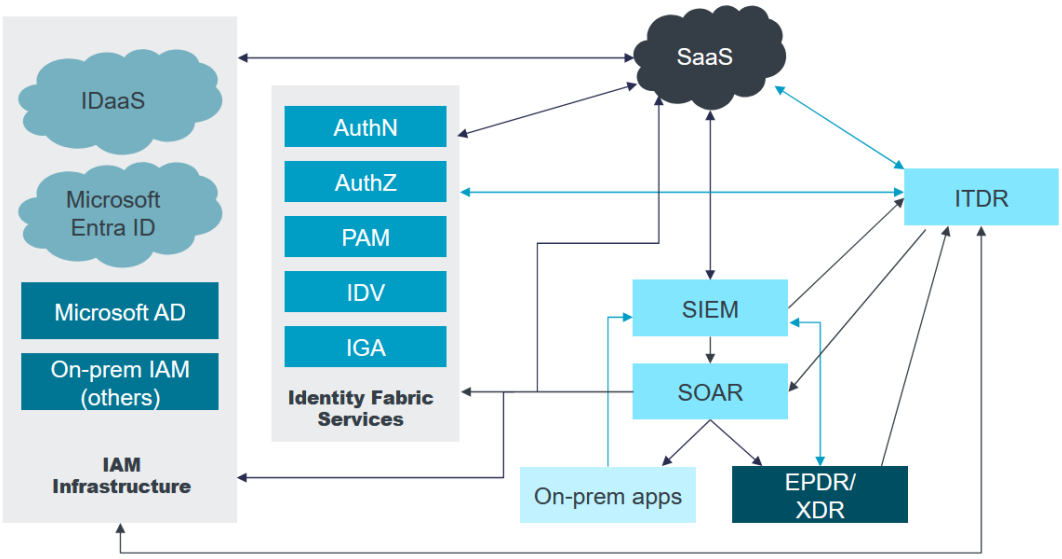


Figure 1: ITDR adds the identity analytics capabilities and insights to SIEM, SOAR, and XDR

Point solutions may cover individual segments of the identity stack, but they often fail to provide a holistic view or real-time awareness. To properly secure the identity environment, organizations must adopt an integrated approach that can monitor all components collectively. This highlights the need for continuous ITDR that spans the full identity fabric. Such capabilities must unify fragmented tools, bridge siloed data, correlate activity across systems to assess risk dynamically, detect threats as they emerge, and support proactive remediation strategies. Visibility and compliance alone are not enough; a resilient defense against identity-based attacks demands integrated detection, response, and recovery capabilities.

ITDR solutions should both protect and defend. However, identity-related threats now span multiple domains, creating a problem that no longer fits neatly within the scope of a single team. IT administrators may have visibility into identity systems but often lack the threat context. On the other hand, SOC analysts are trained to hunt threats across the network and endpoint layers, yet they usually have limited familiarity with IAM systems and governance structures. In response, ITDR vendors are positioning their tools as the connective tissue between these teams, introducing real-time monitoring, contextual analytics, and adaptive controls to identify abnormal activity, assess risk, and support automated or guided response actions.

The vendors included in this Leadership Compass hail from various backgrounds and offer diverse approaches. This is not a sign of market immaturity, but rather a reflection of how cross-functional and strategic identity has become. Some are pure-play ITDR vendors, having built their platforms specifically to address identity-based threats through detection, correlation, and response. Others are more established identity or security players that have added ITDR capabilities to existing platforms not originally designed for this purpose. As a result, some vendors excel at real-time detection and signal correlation, while others stand out for their strengths in visibility, recovery, or posture management.

The smart bet is on vendors that can help organizations converge around identity as both a control plane and a detection surface. When evaluating identity threat detection capabilities, organizations should avoid limiting their questions to whether a solution can detect specific techniques like credential stuffing or Golden Ticket attacks. Instead, the right questions center on whether the platform can establish and adapt behavioral baselines over time, correlate weak signals across identity silos, and automate the investigation process. Buyers should assess how well a solution can surface identity anomalies and suspicious behaviors, not just match known techniques. Nevertheless, the business value is clear: reduce false positives in the SOC, enable real-time enforcement actions, and build a defensible security posture around identity. What unites all of the vendors in this report is the assumption that prevention is no longer enough. Organizations must assume compromise and invest in detection and response mechanisms. This includes integration with as many relevant systems as possible, including identity providers, directories, SaaS applications, ticketing systems, EDR platforms, SOAR, and other security tools.

This Leadership Compass covers the dynamics of this emerging market, provides a framework for evaluating ITDR solutions, and offers guidance on how enterprises can select the appropriate technologies for their organizations. To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

Key Findings

- The ITDR market spans the space between identity IT administration and security operations center (SOC) threat detection and response. This dynamic is creating a new type of solution, because protecting identity requires both departments to cooperate in converged products.
- Not all vendors offer the same level of operational readiness. Buyers should consider the maturity of the platform, customization of dashboards and playbooks, availability of APIs, and the vendor's track record in supporting enterprise-scale deployments.
- While not universally available, deception technologies, such as honeytokens and identity decoys, can provide early warning signals and help slow down or divert attackers. Consider whether these techniques align with your SOC capabilities and threat model.
- ITDR platforms should integrate natively with IAM tools (IGA, PAM, Access Management), security tools (SIEM, SOAR, XDR), and ITSM systems. Gaps in integrations can lead to fragmented investigations or require custom workarounds, limiting response effectiveness and increasing operational overhead.

- All vendors we cover in this report have experienced strong product-market fit, but they are also fairly diverse in their architecture and approaches. As such, selecting a vendor relies primarily on enterprise organizations understanding internal requirements for ITDR.

Market Analysis

The ITDR market is experiencing substantial growth. Several key drivers underpin this growth. Most notably, identity-based attacks account for a substantial and growing share of breach activity. Meanwhile, rising regulatory and compliance demands, such as GDPR, CCPA, and other data protection standards, are compelling organizations to adopt proactive identity threat detection as part of their security frameworks. Additionally, the Zero Trust paradigm, with its core principle that breaches are inevitable, further emphasizes the need for continuous authentication, identity validation, and responsive mitigation, areas where ITDR excels.

As described above, the market landscape includes specialist vendors born in the ITDR space, who offer focused capabilities in threat detection, identity behavior analytics, and contextual correlation. At the same time, larger identity and security platforms are evolving by incorporating ITDR capabilities into their existing IAM, IGA, or XDR stacks. This is sometimes achieved through native development and other times via acquisition. This has resulted in solutions that vary significantly in scope, architecture, and depth of capabilities. Nevertheless, adoption still faces setbacks. For many organizations, aligning ITDR with existing workflows and governance is a significant challenge. High implementation costs, talent shortages, and organizational inertia further impede adoption.

The total market size for ITDR is difficult to establish compared to other tech industry markets for several reasons. First, as mentioned above, few products are currently sold purely as ITDR solutions, so determining the amount of economic activity generated by ITDR requires some triangulation of the money spent on the various products used to create ITDR solutions. However, based on our analysis, we project compound annual growth rates (CAGR) between 19% and 23% over the next five years, reflecting strong and sustained demand for ITDR solutions as identity continues to solidify its role at the core of enterprise security strategies.

Large enterprises, particularly those in the financial services, healthcare, government, and critical infrastructure sectors, currently dominate ITDR adoption due to strict compliance mandates and valuable assets at risk. Yet Small and Medium-sized Enterprises (SMEs) are projected to exhibit strong growth, especially when cloud platforms and managed services lower adoption barriers. Regionally, North America and the EMEA hold the largest share, supported by mature cybersecurity infrastructure and regulatory frameworks. Meanwhile, Asia-Pacific is seen as a high-growth frontier due to rapid digital transformation across emerging economies.

Delivery Models

ITDR solutions are delivered through a variety of models to meet different organizational needs and integration preferences:

- **Cloud-Native/SaaS:** Many modern ITDR offerings are cloud-native, delivered as Software-as-a-Service (SaaS). This model supports rapid deployment, continuous updates, and integration with cloud IAM providers and SaaS applications.
- **Hybrid Deployment:** Some vendors offer hybrid approaches, combining cloud-based analytics with on-premises connectors or sensors to monitor legacy infrastructure such as Active Directory (AD) or on-prem identity stores. This model is common in enterprises with mixed IT environments.
- **On-Premises:** Though less common, certain ITDR capabilities are available in fully on-prem deployments, typically required by highly regulated industries or organizations with strict data residency requirements.
- **Modular/Embedded:** ITDR capabilities may also be embedded into broader identity platforms (e.g., IAM, IGA, PAM) or XDR/SIEM tools, delivered as feature modules rather than standalone products. This model suits organizations seeking tighter integration with existing security operations.

Additionally, some ITDR solutions are delivered through managed service partners. This enables organizations to offload deployment and operations while gaining access to specialized expertise and continuous monitoring. Although all delivery models are looked at in this Leadership Compass, it is worth considering each delivery model's pros and cons against the use cases for ITDR solutions.

Required Capabilities

Although ITDR solutions come in many forms, key aspects of any solution include:

- **Discovery and Visibility:** Discovery refers to the automated identification and classification of identities, credentials, service accounts, roles, and entitlements across systems and applications. Visibility, in turn, enables organizations to understand how those identities interact, what access they have, and how they are being used in real time.

- **Monitoring:** This refers to the continuous observation of identity-related signals, sessions, and events across an organization’s IT environment. It includes collecting telemetry from identity providers, directories, endpoints, cloud services, and applications to detect anomalies, suspicious behaviors, and indicators of compromise.

- **Prevention and Posture Management:** Posture management also involves evaluating an organization’s identity hygiene, setting baselines for normal behavior, and ensuring identity systems follow policy and compliance standards. Some ITDR solutions also deploy decoy accounts or honeytokens to detect unauthorized activity early. The goal is to expose misconfigurations before attackers do.

- **Detection:** The ability to identify abnormal behavior or suspicious activities that could indicate a threat to an identity, such as unauthorized access attempts, anomalous login patterns, or exploitation of vulnerabilities related to identity services and protocols. This enables teams to distinguish between legitimate and malicious use of credentials across hybrid environments.

- **Correlation:** Linking identity events with entitlements, user context, and signals from security tools like SIEM, SOAR, or XDR, thereby distinguishing between legitimate usage and credential abuse. Rather than analyzing events in isolation, correlation engines identify patterns across multiple domains.

- **Investigation:** The goal is to give SOC analysts and identity teams the tools to quickly validate incidents, understand their scope and impact, and determine the appropriate response. This involves correlating data from various sources to gain insights into the nature of the threat and identifying the affected systems or data.

- **Response:** Appropriate actions to mitigate attacks include executing predefined or dynamic playbooks, adjusting security policies, implementing stronger authentication measures, revoking compromised credentials, and deploying patches to address vulnerabilities. These actions are often automated or orchestrated through integrations with SIEM and SOAR platforms.

- **Recovery:** This capability is critical for organizations recovering from ransomware, Golden Ticket attacks, or deep compromise of the identity infrastructure. It includes directory integrity validation, automated rollback of malicious changes, and forest-level restoration of Active Directory environments.

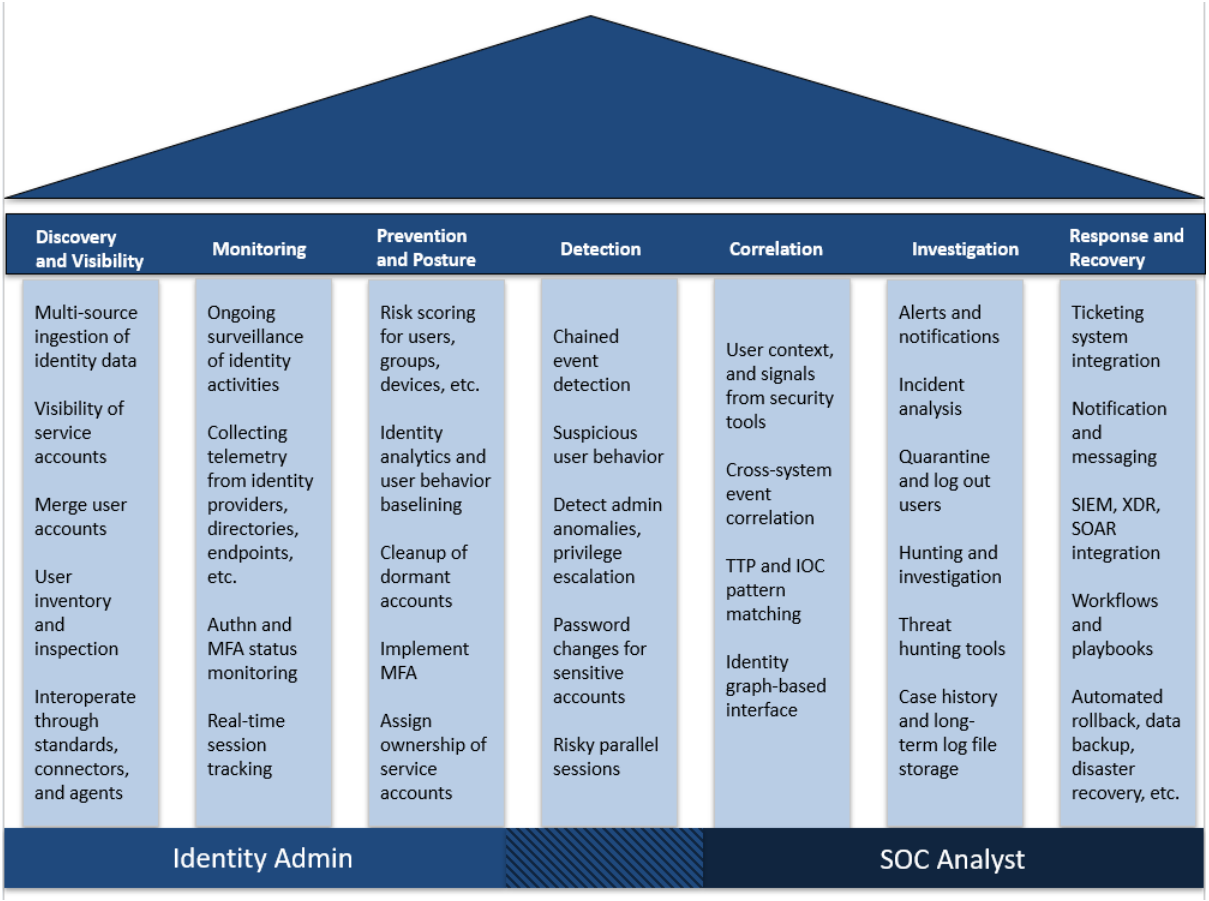


Figure 2: The Seven Pillars of ITDR

These pillars support activities that range from administration of identity systems (on the left) to SOC-related responsibilities (on the right). However, several functions depicted sit at the intersection of both domains. These overlapping areas underscore the necessity of shared responsibility between identity administrators and SOC teams. Tools that offer integrated visibility and shared workflows significantly enhance the effectiveness of ITDR initiatives, helping teams respond faster and with greater confidence to identity-based threats.

Other capabilities include, amongst others:

- Standards support
- Data Access Governance
- Developer support
- Connectors to target systems
- Toolkits for customizing connectors
- Integration and/or synchronization to directory services
- Compromised credential intelligence
- Identity and access analytics
- Service account and NHI protection
- Auditing, reporting, and dashboarding
- Comprehensive set of APIs

- Flexible, modern software architecture & deployment
- Configurable and explainable AI capabilities
- Fraud Reduction Intelligence Platform Integration
- ITSM integration (i.e., ServiceNow)
- NDR and EPDR integration
- SIEM, SOAR, and XDR integration
- Integration into Incident Management / Response Systems
- Applied AI/ML for identity and access analytics
- Applied AI/ML for adaptive authentication and authorization
- Support for strong risk- and context-based authentication to the ITDR system
- Ability to create and manage deceptive assets like accounts, token, certificates, etc.

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

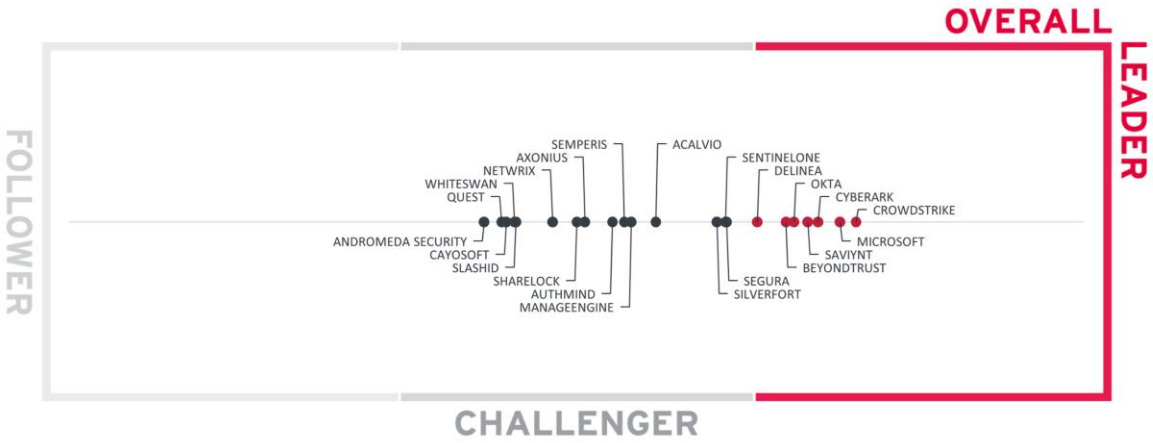


Figure 3: Overall Leadership in the ITDR market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security. However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Among the Overall Leaders we find CrowdStrike, recognized for its strong integration of identity detections within its Falcon platform; Microsoft, with ITDR deeply embedded across Defender, Sentinel, and Entra ID; CyberArk, which combines credential protection with visibility and risk-based remediation; Saviynt, leveraging its governance engine to drive identity-centric detection and posture management; BeyondTrust, extending privilege and session control into identity risk insights; Okta, which uses identity context and API-driven

architecture to detect and respond to suspicious behavior across apps and services; and Delinea, delivering continuous discovery of assets, entitlements, and misconfigurations.

In the Challengers section, SentinelOne brings detection strengths but lacks built-in identity lifecycle and response capabilities, while Segura, Silverfort, and Acalvio offer specialized detection or deception but fall short on orchestration, posture management, remediation, or broader coverage; and ManageEngine which provides a modular suite but lacks deeper integrations or coverage across ITDR functions. Finally, vendors such as Semperis, AuthMind, Axonius, Sharelock, Whiteswan, Netwrix, SlashID, Quest, Cayosoft, and Andromeda Security are positioned as Challengers due to narrower focus, lower market visibility, fewer response capabilities, limited integrations with identity tools, or dependency on specific platforms such as Microsoft.

Overall Leaders are (in alphabetical order):

- BeyondTrust
- CrowdStrike
- CyberArk
- Delinea
- Microsoft
- Okta
- Saviynt

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 4: Product Leadership in the ITDR market

Microsoft, CrowdStrike, Saviynt, Okta, Segura, BeyondTrust, Silverfort, and CyberArk are the Product Leaders. The leaders in ITDR are those delivering broad coverage across key

detection and response use cases, while also enabling advanced coordination with external systems when required. The remaining vendors are positioned in the Challengers section. While many demonstrate strength in specific areas, they may fall short in delivering a complete ITDR solution. Common limitations include a lack of integrations with key systems such as IGA, Access Management, PAM, SIEM, SOAR, and ITSM, or an overly narrow focus on Microsoft-centric environments that may not support more diverse infrastructures. That said, organizations with targeted requirements should closely evaluate the unique strengths and trade-offs of each vendor in this group.

Product Leaders (in alphabetical order):

- BeyondTrust
- CrowdStrike
- CyberArk
- Microsoft
- Okta
- Saviynt
- Segura
- Silverfort

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.

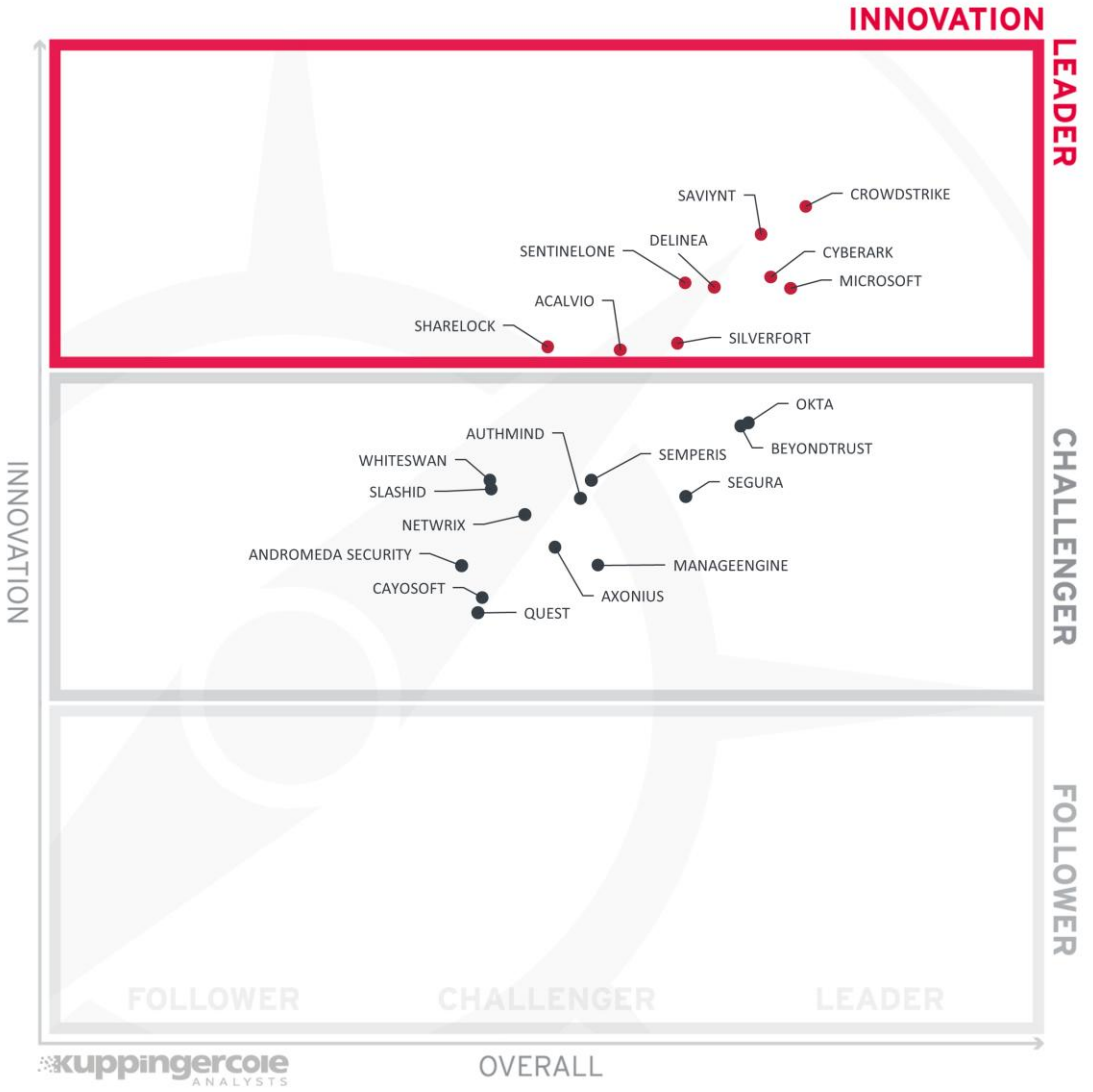


Figure 5: Innovation Leadership in the ITDR market

CrowdStrike, Saviynt, CyberArk, SentinelOne, Delinea, Microsoft, Silverfort, Sharelock, and Acalvio are Innovation Leaders. Innovation Leaders are those vendors that are delivering 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.

Vendors in the Innovation Leadership category stand out through differentiated capabilities that go beyond foundational ITDR. These include, among others, advanced decoy and deception techniques that enrich detection fidelity, along with the use of AI and ML to analyze behavioral baselines and correlate subtle identity signals across silos. What distinguishes this group further is their support for automated identity-centric responses such as disabling accounts, revoking access tokens, or terminating active sessions based on risk. Some also offer playbook-driven response orchestration and real-time enrichment of alerts using contextual insights from identity systems.

Innovation Leaders (in alphabetical order):

- Acalvio
- CrowdStrike
- CyberArk
- Delinea
- Microsoft
- Saviynt
- SentinelOne
- Sharelock
- Silverfort

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, the number of developers, 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.

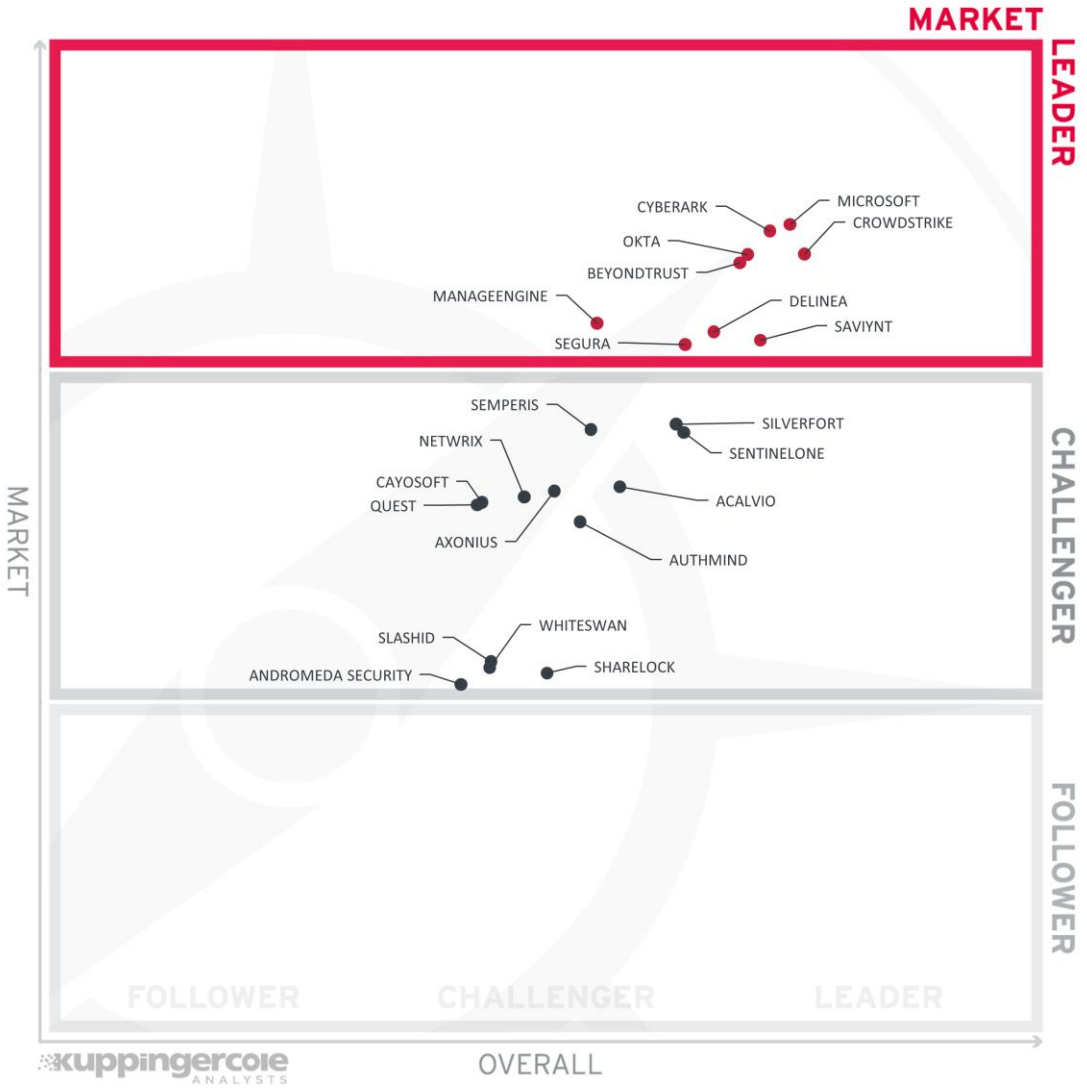


Figure 6: Market Leaders in the ITDR Market

Microsoft, CyberArk, Okta, CrowdStrike, BeyondTrust, ManageEngine, Saviynt, Segura, and Delinea are Market Leaders. These vendors benefit from extensive partner networks, global operational reach, flexible licensing models, and broad support for diverse deployment and integration scenarios. The rest of the vendors are rated as Challengers. These are smaller vendors with mostly small partner ecosystems and limited market presence on a global scale.

Market Leaders (in alphabetical order):

- BeyondTrust
- CrowdStrike
- CyberArk
- Delinea
- ManageEngine
- Microsoft
- Okta
- Saviynt
- Segura

Product/Vendor evaluation

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

Spider graphs

In addition to the ratings for our standard categories, we provide a spider graph for every product we rate. These graphs provide a review of specific use cases for the ITDR market and are not meant to be considered a comprehensive evaluation of a product; rather, they are intended to aid organizations in evaluating the product's fit to their specific requirements. In this way, they do not always align with the rankings for Overall Leader or our other standard ratings, which take many other factors into account.

For the ITDR market, we evaluate products at the following eight capabilities:

Discovery: The solution's ability to identify all identities across cloud, on-premises, and hybrid environments. This includes locating unmanaged, orphaned, or shadow accounts as well as service accounts and credentials embedded in code or infrastructure.

Visibility: Provides detailed inspection tools to understand ownership, privileges, usage patterns, and entitlements across identity assets. Enables mapping of identity-to-resource relationships for both individual users and organizational units.

Risk Assessment: Applies contextual and automated risk scoring based on behavioral analytics, posture evaluation (for example, MFA status and credential hygiene), and peer comparison to highlight misconfigurations, over-privileged identities, or toxic combinations.

Detection: Continuously monitors for identity-related threats, flagging anomalies or indicators of compromise. Triggers alerts based on changes in risk posture, abnormal behavior, or deviations from policy and baselines.

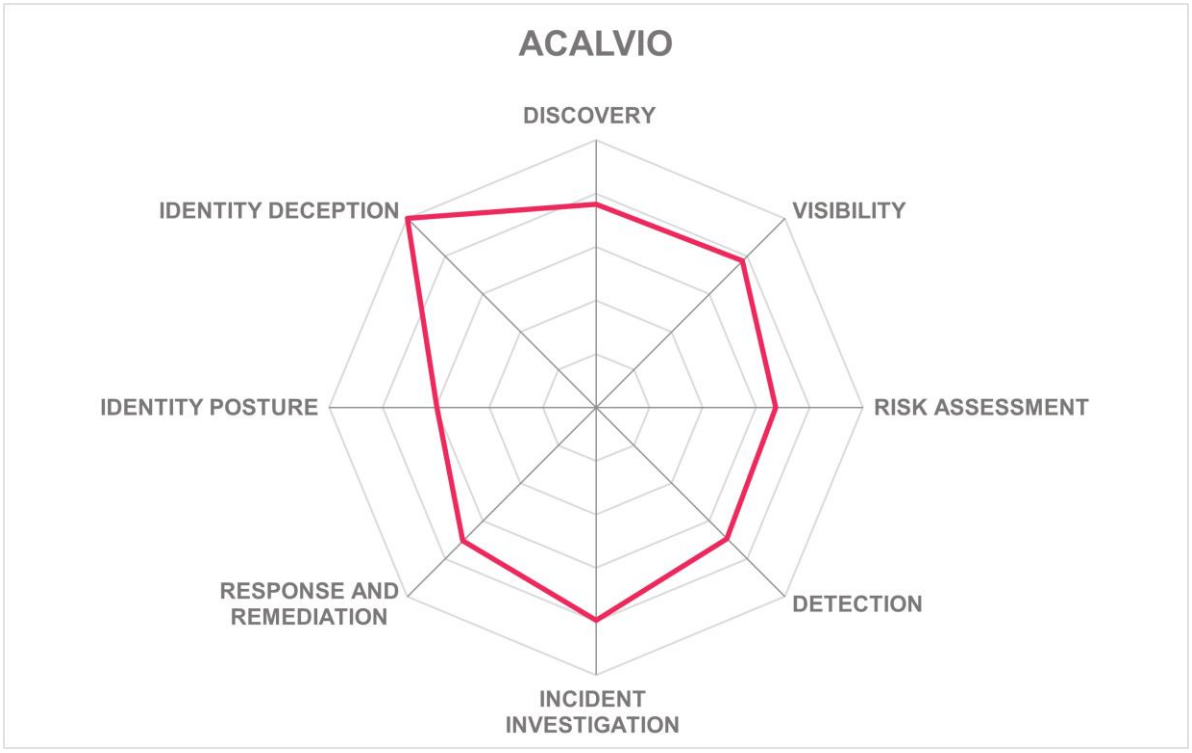
Incident Investigation: Equips analysts with correlated identity activity trails, cross-platform attack mapping, and evidence needed to reconstruct incidents. Supports prioritization and triage based on threat severity and asset criticality.

Response and Remediation: Supports both automated and manual responses, including containment, access revocation, and privilege reduction. Integrates with ITSM and SOAR tools for workflow orchestration and root cause documentation.

Identity Posture: Enables continuous assessment and hardening of identity environments by surfacing weak configurations, stale entitlements, and policy violations to reduce the blast radius of identity compromise.

Deception: The ability to deploy and monitor decoy accounts and assets in identity systems.

Acalvio – Acalvio ShadowPlex



Leader in

Founded in 2015 and headquartered in Santa Clara, California, Acalvio is known for its patented cyber deception technology that underpins its ITDR solutions. The company's ShadowPlex Identity Protection and ShadowPlex Cloud Security products form the core of its offering in this segment. These solutions are delivered via multiple models, including SaaS, appliance, container-based, private, and public cloud, and are also offered through MSSPs. Acalvio supports integration with common protocols such as REST and Webhooks, with authentication via JWT, OAuth2, and SAML. Its licensing model is per user. The platform is certified under standards including FIPS 140-2, NIST 800-57, ISO/IEC 27001, and FedRAMP. Targeting large enterprises globally, Acalvio serves industries including finance, healthcare, manufacturing, oil and gas, government, and insurance.

Acalvio ShadowPlex delivers ITDR through distributed deception and honeytoken technology designed to confuse attackers and surface identity threats. The platform deploys deceptive artifacts in identity systems, cloud workloads, endpoints, and externally exposed APIs to proactively detect compromise. ShadowPlex supports Microsoft, Okta, Ping Identity,

Delinea and CyberArk for PAM, and cloud platforms such as AWS, Azure, GCP, and Oracle. It places honey users, policies, and credentials into locations attackers typically scan, including storage buckets, secrets stores, and Kubernetes clusters. Detection is triggered when these decoys are accessed, offering strong signal capabilities to reduce false positives. In addition, ShadowPlex captures credential related attack activity and surfaces related intelligence. This includes visibility for credential attacks, such as credential brute force, password spraying, credential stuffing attacks. For visibility, the dashboard surfaces alerts enriched through external threat intelligence and mapped to the MITRE ATT&CK framework. Correlation is performed through telemetry collection across attacker tools, endpoints, decoys, and credentials, with triaged alerting based on site-defined risk scoring.

Incident response is driven by over 50 deception playbooks, which are editable and exportable in JSON. The solution integrates with a broad set of third-party tools including PAM, Access Management, SIEM, SOAR, and ITSM. However, recovery is limited with no remediation or rollback features. The Identity Attack Surface Management (IASM) capability provides proactive exposure assessment and is particularly useful in reducing risk before incidents occur. Acalvio's use of external-facing deceptions for credential leak detection represents a valuable approach to stopping adversaries earlier in the attack chain. That said, the platform lacks integration with IGA tools, which limits its applicability in environments where lifecycle governance is tightly coupled with incident response. While the solution delivers strong visibility and detection capabilities, it does not include behavior-based analytics or remediation workflows, narrowing the scope of its response posture. These tradeoffs reflect Acalvio's focused strategy but may require augmentation in more expansive ITDR deployments. The solution also identifies well-known attack methods such as password spraying, LSASS dumping, golden and silver ticket attacks, DCSync, DCShadow, pass-the-hash, golden SAML attacks, and Kerberos-based exploits.

Acalvio's solutions are best suited for organizations seeking high-fidelity identity threat detection that works independently of traditional behavioral baselines. Enterprises operating hybrid identity environments, including cloud and legacy AD, will find particular value in the platform's breadth of deployment options and integrations with SOC tooling. With strong presence in North America, EMEA, and APAC, Acalvio has proven fit for regulated sectors and large enterprises that prioritize deception as a layer of ITDR and seek targeted tools that integrate smoothly with existing SOC infrastructure.

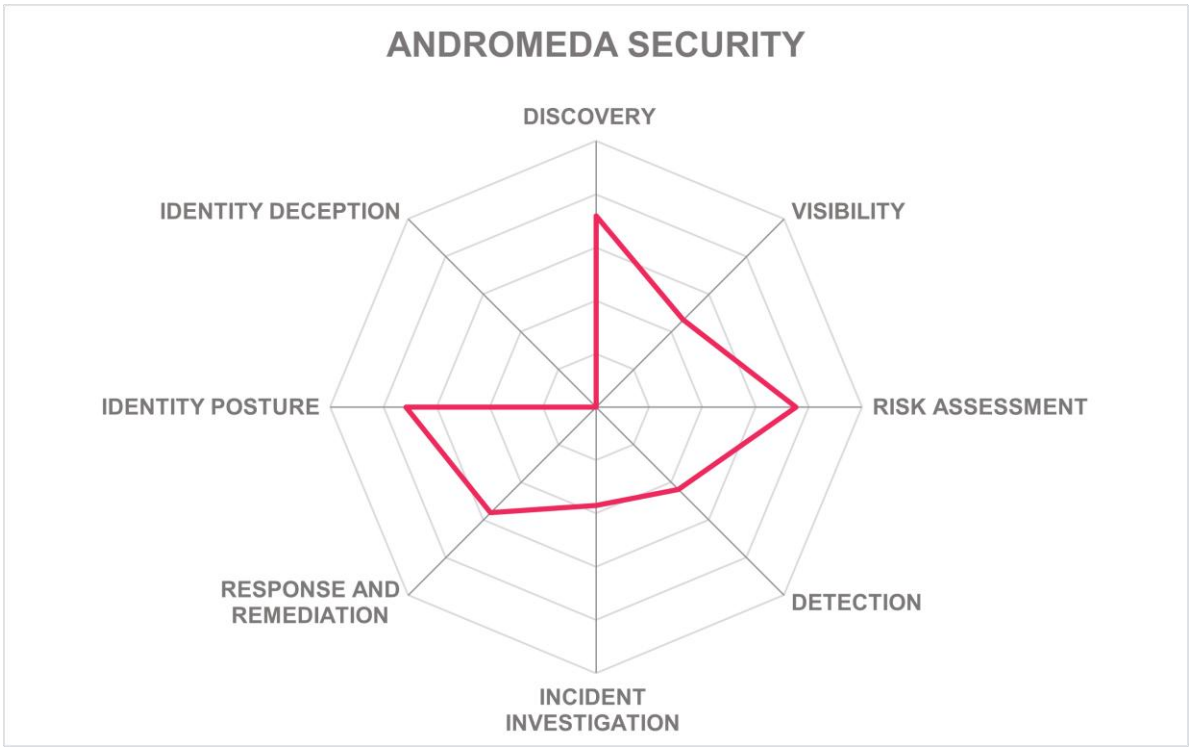
Strengths

- Deception-based detection reduces false positives
- Coverage for AD and major cloud identity systems
- External-facing decoys for leaked credential detection
- MITRE ATT&CK-aligned alert taxonomy
- Integration with leading SOAR and SIEM platforms
- Granular telemetry collection for correlation
- Customizable deception playbooks
- Broad deployment flexibility across environments

Challenges

- No integration with IGA tools
- Lacks support for UBA
- Limited remediation and rollback capabilities
- Requires strong SOC process maturity to operationalize
- Deception design may need tuning in complex environments

Andromeda Security – Andromeda Identity Security Platform



Based in San Francisco and founded in 2023, Andromeda Security offers an agentless, cloud-native platform tailored for securing both human and NHIs in hybrid environments. The Andromeda Identity Security Platform targets mid-market and enterprise customers in North America across industries such as finance, healthcare, insurance, and utilities. Licensing is based on both human users and NHI identities, aligning with its focus on cloud-native infrastructure. The solution is deployed as a public cloud service and supports REST and GraphQL APIs, with JWT-based authentication. While the platform is SOC 2 Type 2 and ISO/IEC 27001 certified, it lacks certifications such as FedRAMP.

Andromeda's core architecture, a unified identity-resource graph, enables its key capabilities by aggregating identity and asset data from cloud and SaaS platforms, mapping entitlements, and relationships across the environment. The platform builds continuous AI and machine learning baselines using log ingestion, including activity data, and integrates with sources such as cloud providers, identity providers, HR systems, applications, and IT service management tools to detect anomalies in real time. IdPs supported include Microsoft, Okta, Ping Identity, and Google Workspace. Discovery and visibility are enriched through detailed identity dashboards, risk scoring, and recommendations. Andromeda does not integrate with IGA tools but offers IGA capabilities as part of the platform. Posture management includes automated detection of misconfigurations and excessive privileges, supported by contextual insights. Detection methods leverage behavior and usage analytics

to flag compromised or overprivileged accounts. Correlation and investigation are based on posture, behavioral, and privilege-based risk models that jointly assess attack likelihood and blast radius. For response, the platform ships Python-based remediation playbooks for over 20 use cases, with actions including privilege reduction, reauthentication, step-up MFA, and alerting.

Andromeda's agentless architecture and focus on humans and NHIs allow it to address emerging challenges in cloud infrastructure where traditional PAM and IGA tooling struggle. The identity risk model, combining posture, behavior, and privilege dimensions, is well-structured and actionable, supporting automation and just-in-time access decisions that reduce operational overhead. While it supports ITSM integration with JIRA and can stream logs via Syslog, it does not currently integrate deception-based detection tools. Customization options for dashboards are limited, but improvements are on the roadmap. Support for forensic workflows and ticketing processes is also absent, potentially narrowing its use for SOC teams looking for full incident lifecycle coverage.

Andromeda is well-positioned for mid-sized organizations and cloud-forward hybrid organizations looking to consolidate identity threat detection and governance in a single platform. It provides out-of-the-box coverage for both workforce and NHIs in environments where credential sprawl and least-privilege enforcement are high-priority concerns. While its current market presence is limited to North America, the solution's scope and delivery model make it suitable for organizations seeking a focused ITDR and governance offering without the complexity of integrating multiple third-party tools. Enterprises undergoing cloud transformation initiatives may particularly benefit from their automated IAM tasks and AI-powered insights, especially where operational agility and control over NHIs are critical.

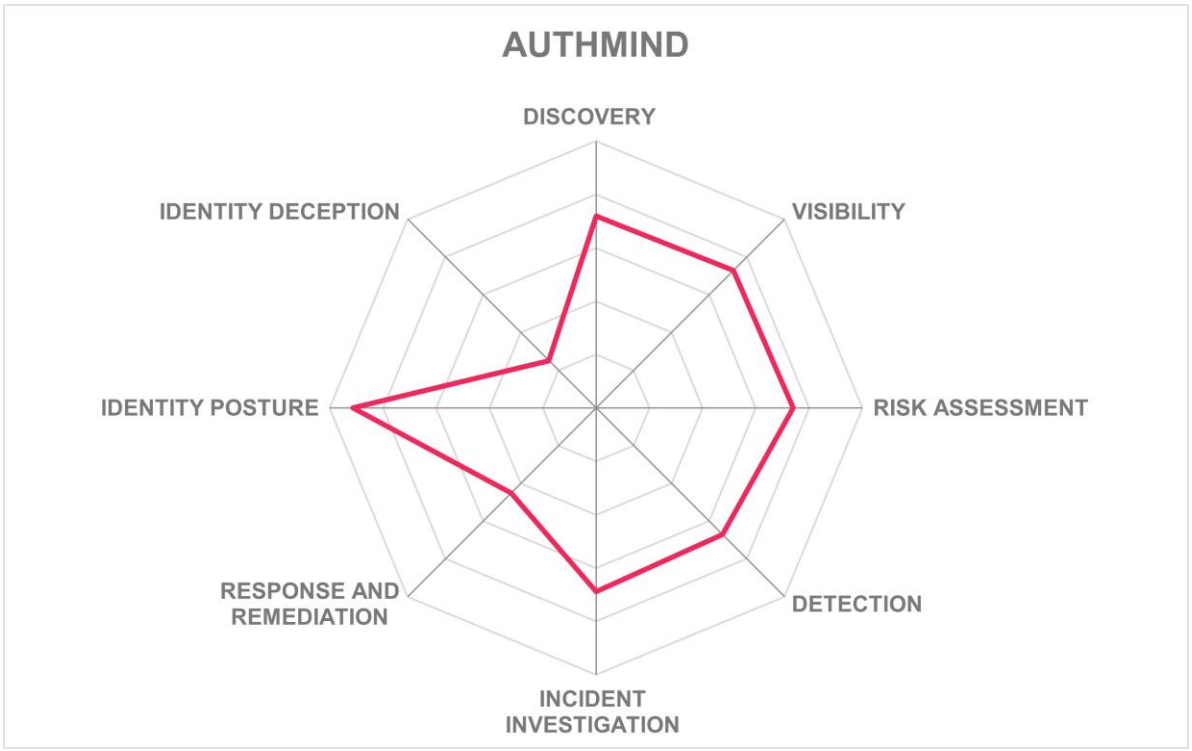
Strengths

- Strong focus on managing human identities and NHI sprawl
- Real-time anomaly detection via AI/ML
- Built-in Cloud PAM and IGA capabilities
- Unified identity-resource graph model
- Contextual dashboards with recommendations
- Agentless architecture for easy deployment
- Advanced behavioral and privilege risk scoring

Challenges

- Small partner ecosystem
- Relatively small market presence outside of North America
- No deception capabilities

AuthMind – AuthMind Identity Protection Platform



AuthMind, established in 2020 and headquartered in Washington, D.C., with additional offices in Pune, India, delivers an Identity Observability and Protection Platform purpose-built for ITDR. The company focuses on real-time identity observability across agentic AI, NHIs, and humans, supporting enterprises ranging from mid-sized organizations to large global firms. AuthMind offers flexible deployment options, including multi-tenant SaaS, single-tenant managed service, and private cloud environments. Licensing is based on a per-employee model and covers all humans, AI agents, and NHIs in the organization. For API Authentication JWT, OAuth 2, SAML, and OIDC are supported. API protocols supported include REST and Webhooks. AuthMind's customer base is strongest in North America, with growing traction in EMEA, APAC, and Latin America, and expansion efforts underway in Australia, Israel, and India through both direct sales and its partnership with IBM. Adoption has been strongest in financial services, insurance, healthcare, business services, and manufacturing.

The AuthMind Identity Observability and Protection Platform's architecture is designed to ingest data from IAM systems such as Microsoft, Okta, Ping Identity, IBM, One Identity, AWS, CyberArk, HashiCorp, and Google Workspace, with additional data sources of network flow logs, cloud audit trails, SIEM platforms like Splunk, QRadar, and Sumo Logic,

Data Lakes such as Cribl and Kafka, and EDR tools to provide unified identity observability. AuthMind's platform observes any access (agentic AI, NHI, or human) and correlates identity events to trace end-to-end access paths, enabling detection of blind spots such as unmanaged/local accounts, shadow directories, or control bypasses. Posture management capabilities highlight misconfigurations and credential risks, while its percentile-based risk scoring model prioritizes entities for investigation. The platform provides over 70 customizable playbooks that allow security teams to build detection and response processes without coding, sending alerts and findings to SIEMs, SOAR systems, or ITSM tools like JIRA and ServiceNow, and taking actions directly from the platform.

The product emphasizes visibility, correlation, and detection while leaving enforcement to existing security controls, while providing deep observability of agentic AI, NHIs, and human across the cloud, on-premises, and SaaS apps. The solution delivers continual risk assessments by focusing on real activity rather than static entitlement data. Challenges remain, including lack of rollback options and the lack of MITRE ATT&CK mappings for identity-specific TTPs also limits alignment with established frameworks. Despite these gaps, AuthMind demonstrates innovation through its identity observability model and breadth of integrations, positioning it as a distinct vendor in the ITDR market. The platform identifies AD attack methods such as golden and silver ticket attacks, DCSync, DCShadow, pass-the-hash, and Kerberos-based exploits.

AuthMind will be of particular interest to organizations struggling with unmanaged accounts, credential misuse, or shadow directories across hybrid and multi-cloud infrastructures. Its ability to reconstruct full identity activity paths allows SOC teams to enrich investigations, detect evasions of access controls, and triage incidents using contextualized risk scoring. With a unified architecture and a strong ITDR focus, the platform serves organizations seeking a feature-rich solution that prioritizes identity security without adding operational complexity.

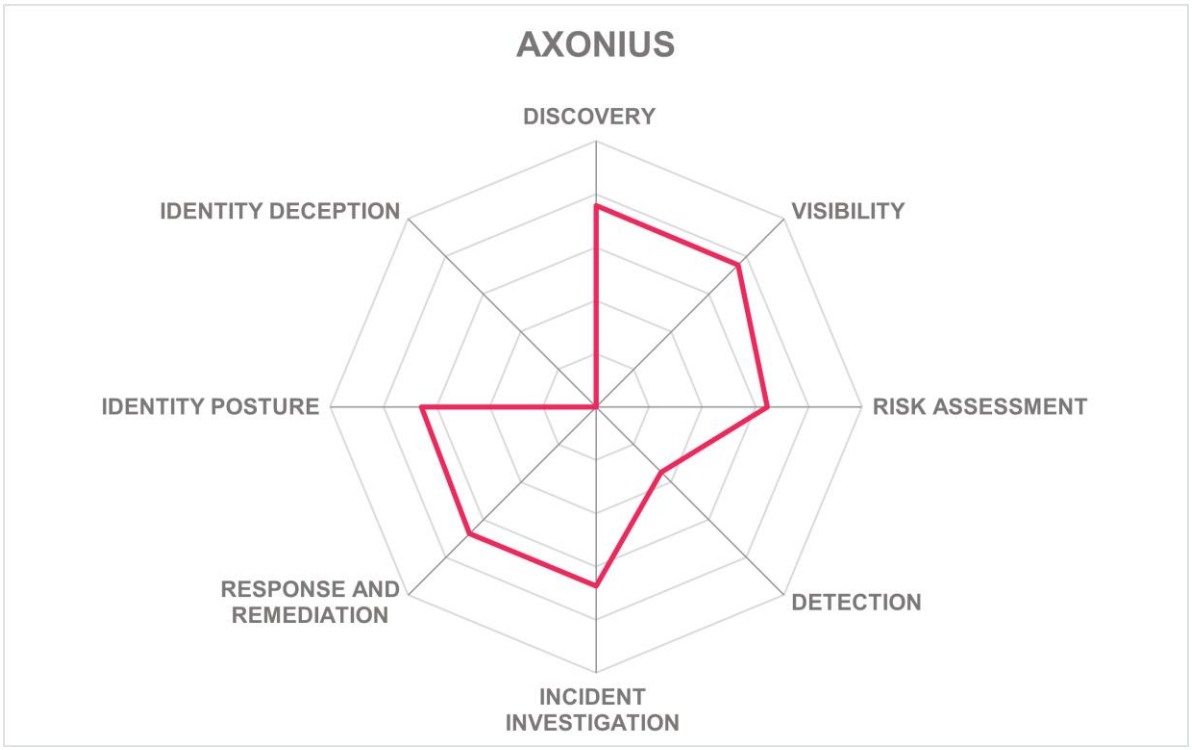
Strengths

- Correlation of identity, network, and cloud flows
- Percentile-based, tunable risk scoring model
- Over 70 customizable, no-code playbooks
- Broad SIEM, SOAR, and ITSM integrations
- Real-time detection of VPN, PAM, and ZTNA bypasses
- Flexible SaaS, managed service, and private cloud deployment
- Effective discovery of shadow accounts and directories

Challenges

- Missing FedRAMP certification
- Identity TTPs not yet mapped to MITRE ATT&CK

Axonius – Axonius Platform



Headquartered in New York and founded in 2017, Axonius has quickly established itself as a vendor focused on delivering identity-centric visibility, governance, and automation across complex IT environments. With additional offices in Israel and Brazil, the company serves enterprises of varying sizes across industries such as finance, retail, insurance, government, manufacturing, and utilities. Its core product for the ITDR space is Axonius Identities, a solution designed to unify fragmented identity data and strengthen security posture through enhanced lifecycle management, governance, and remediation capabilities. The licensing model is based on the number of human digital identities and NHIs discovered and managed. Axonius aligns its platform with key compliance requirements, including ISO/IEC 27001, HIPAA/HITRUST, SOC 2 Type 2, and FedRAMP. Axonius supports secure API access using OAuth2 and API keys, with optional JWT support for token-based authentication. SAML is used for user authentication via SSO but is not applied for direct API access. API protocols supported include REST. Deployment models include on premises, public and private cloud, virtual appliance, and managed service delivery.

Axonius Identities provides an identity-centric ITDR solution designed to discover, monitor, and control both human and machine identities across cloud and on prem-systems. Continuous identity discovery is a foundational capability, with the platform cataloging accounts, entitlements, permissions, and policy artifacts into a single management plane. Lifecycle management covers joiner, mover, and leaver scenarios. Governance features

include access requests, certification campaigns, peer group analysis, and role mining, all of which aim to right-size permissions and enforce least privilege. For security monitoring, Axonius supports user behavior analysis based on attributes such as device type, geo-velocity, IP address, and failed login attempts, alongside change tracking for account modifications. The solution provides AI-driven insights for policy optimization and supports incident detection techniques such as monitoring for MFA fatigue, impossible travel, and excessive entitlements. Response capabilities include more than 20 playbooks for actions like session termination, privilege reduction, account disabling, or triggering re-authentication, though rollback is not currently supported. For SOAR, the solution supports Palo Alto and ServiceNow.

Integration breadth is strong, covering IGA, PAM, access management, and ITSM vendors. The inclusion of machine identity management alongside human accounts positions the platform well for enterprises dealing with cloud service accounts and NHIs. GenAI enhancements further improve usability by enabling query creation and policy generation, reducing complexity for administrators. However, some limitations remain. Identity-centric TTPs are not mapped to the MITRE ATT&CK framework and event analysis does not currently trigger playbook recommendations. These gaps leave room for improvement, particularly for organizations seeking deeper automation or more advanced response orchestration. Still, Axonius Identities offers an innovative, identity-first approach to ITDR that stands out in its focus on unifying and operationalizing governance, lifecycle management, and detection.

Axonius primarily serves organizations in North America, though customer traction continues to expand in EMEA, APAC, and Latin America. The solution is particularly relevant for organizations operating in regulated industries where compliance, auditability, and access control enforcement are central requirements. Customers seeking an ITDR solution that integrates with leading IGA, PAM, and SOAR platforms, while also providing direct data collection from external sources, should evaluate Axonius Identities closely.

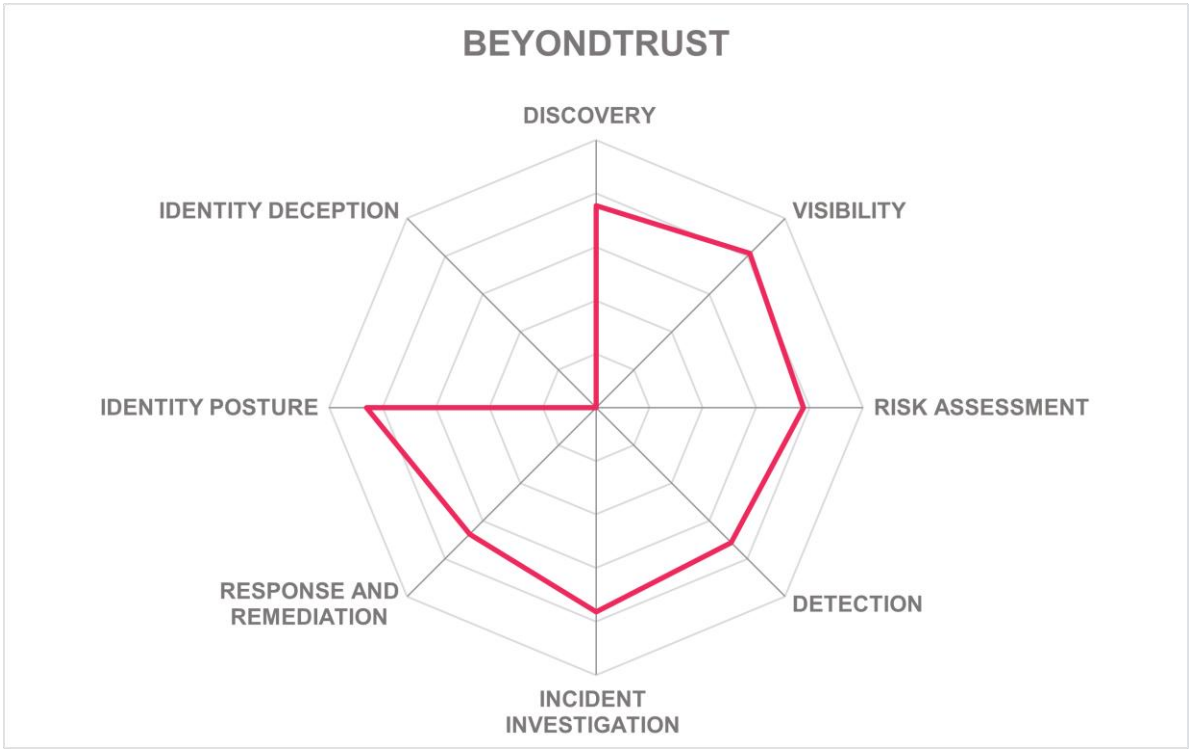
Strengths

- Unified catalog for all human and machine identities
- Continuous discovery of accounts, entitlements, and policies
- Strong support for lifecycle automation and governance
- Broad integrations with IGA, PAM, AM, SOAR, and ITSM systems
- AI-driven insights for least privilege enforcement
- GenAI for query and policy generation
- User behavior analysis for anomaly detection
- Flexible deployment options including managed service

Challenges

- No MITRE ATT&CK mapping for identity-specific TTPs
- Requires third-party tools for response actions
- No automated playbook recommendations from event analysis

BeyondTrust – BeyondTrust Pathfinder Platform



Leader in

Established in 2003, BeyondTrust is a privately held company within the Francisco Partners and Clearlake Capital portfolio. It has evolved from a PAM vendor into a company that addresses a range of identity-centric threats. The company's ITDR offering, the BeyondTrust Pathfinder Platform, builds upon its privileged access, remote access, and endpoint privilege management solutions to provide a unified approach to identity risk. Licensing options include per-user, per-node, per-appliance, and time-based models, supporting flexibility for different organizational scales. The platform can be deployed on premises, in private or public cloud environments, or as a virtual appliance. BeyondTrust is compliant with key standards including FIPS 140-2, ISO/IEC 27001, SOC 2, and FedRAMP. The solution supports API authentication via OAuth2, SAML, OIDC, JWT, and key exchange, with REST and webhooks available for integration. With customers across industries such as finance, healthcare, manufacturing, technology, government, and pharmaceuticals, BeyondTrust primarily serves mid-market and large enterprises in North America and EMEA, while expanding its presence in APAC and Latin America.

The Pathfinder Platform provides multiple integrated capabilities that span discovery, visibility, detection, and response. Identity Security Insights delivers real-time threat intelligence by mapping attack paths, scoring privileges, and detecting anomalies with machine learning models, presenting prioritized recommendations for containment. Its True Privilege Graph dynamically calculates privilege scores across domains, highlighting risks of escalation and lateral movement. Entitle enforces just-in-time access and revokes risky entitlements to minimize standing privileges. Password Safe secures privileged credentials with vaulting, automated rotation, and session recording. Privileged Remote Access supports secure, monitored connections for employees and vendors, while Endpoint Privilege Management enforces least privilege at scale, restricting unauthorized actions and blocking credential misuse. The solution also integrates with SIEM, SOAR, PAM, ITSM, and access management systems from leading vendors, with Webhook-driven extensibility to orchestrate automated responses. All detections are mapped to MITRE ATT&CK.

The True Privilege Graph provides a unique capability to model privilege relationships and escalation paths across complex environments. Its integration of privilege-centric controls such as credential rotation, just-in-time access, and session management into ITDR workflows enables faster and more effective response mechanisms. The extensive connector framework supports alignment with existing enterprise security tools and workflows. Another strength is the ability to correlate human and service accounts to prevent privilege misuse in machine identities. However, some areas present room for improvement, including the current reliance on external orchestration platforms for advanced playbooks and a relatively steep learning curve for teams seeking to operationalize the full set of capabilities. Expanding native automation options and simplifying configuration would further strengthen adoption.

BeyondTrust is particularly relevant for organizations with high privilege exposure and complex identity environments that demand visibility across both human and machine identities. It is well-suited for enterprises operating in regulated industries that require compliance-grade controls and audit capabilities. The platform’s broad integration support makes it a fit for organizations with existing investments in SIEM, SOAR, and PAM infrastructure seeking to extend those investments into ITDR. BeyondTrust’s solution should be considered by organizations seeking an ITDR platform with strong privilege intelligence, integrated remediation capabilities, and operational flexibility across multiple deployment models.

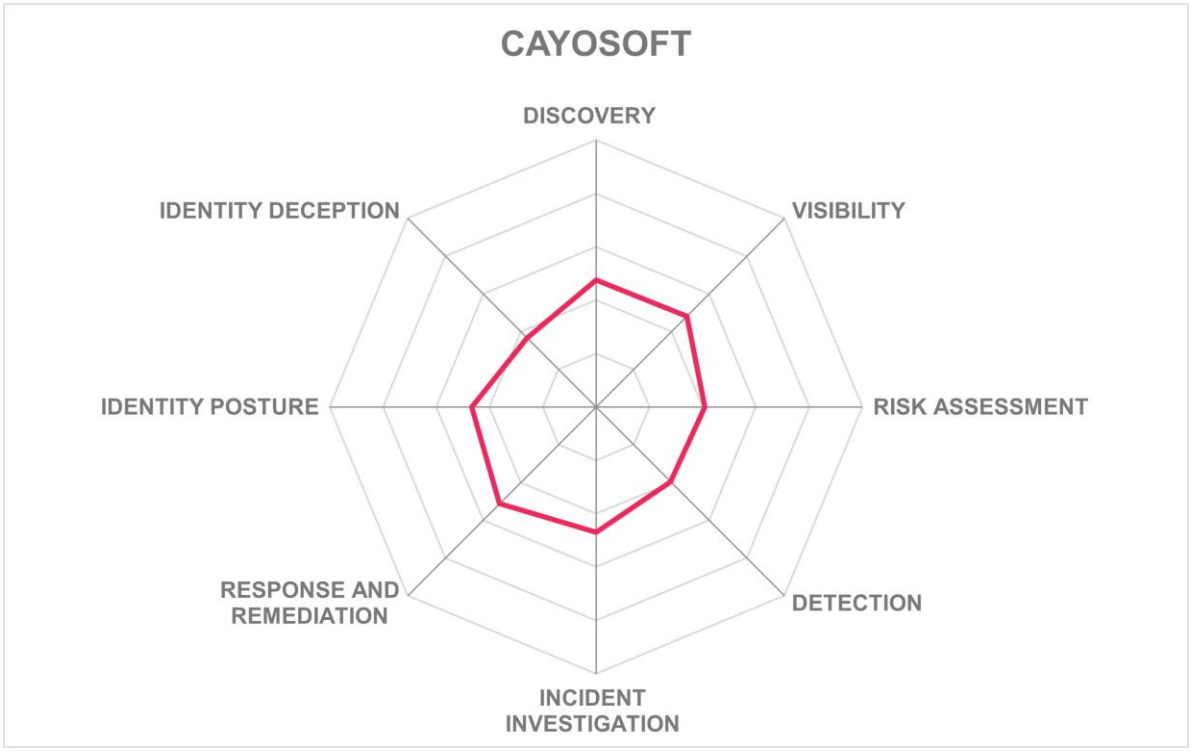
Strengths

- Strong integration of PAM and ITDR capabilities
- True Privilege Graph for privilege risk modeling
- Broad integration with SIEM, SOAR, ITSM, and PAM platforms
- Just-in-Time access with entitlement revocation
- Credential vaulting with automated rotation
- Privileged Remote Access with full audit trails
- Least privilege enforcement at endpoint level
- MITRE ATT&CK aligned detections and responses

Challenges

- Limited native playbook automation in current release
- Configuration complexity for smaller teams
- Dependence on external orchestration for advanced workflows
- No rollback options for automated remediation

Cayosoft – Cayosoft Guardian and Cayosoft Administrator



Cayosoft, founded in 2013 and based in Columbus, Ohio, is a privately held company specializing in identity management and protection for Microsoft-centric environments. Officially incorporated in 2018, the company has steadily expanded its offerings with a strong focus on securing and managing Active Directory, Microsoft 365, and Microsoft Entra ID deployments across on-premises, cloud, and hybrid infrastructures. The Cayosoft Enterprise Suite is built around two primary products: Cayosoft Administrator and Cayosoft Guardian. Licensing is based on per enabled user, and deployment can be delivered via software or as a virtual appliance across on-premises, private, and public cloud environments. The company has a strong presence in North America and is experiencing growing adoption in EMEA and APAC.

Cayosoft Administrator delivers delegated administration, policy enforcement, provisioning, and license management tailored to Microsoft environments. It eliminates standing privileged access by enforcing time-bound, approval-based elevation into restricted groups, aligning with PAM/IGA principles. With more than 250 prebuilt templates, it reduces customization needs while aligning administration with security and compliance goals. Cayosoft Guardian extends ITDR functionality through real-time monitoring, granular change tracking, and advanced rollback capabilities across Active Directory, Azure Entra ID, and Microsoft 365. Guardian's instant standby forest recovery introduces a patent-protected approach to rapid Active Directory restoration. ITDR capabilities include detecting misconfigurations, privilege

escalation paths, risky NHIs, and suspicious activities such as password spraying, brute-force attacks, SID History injection, and rogue domain controllers. Cayosoft Guardian also includes honey accounts for early attacker detection. In addition, integration with Have I Been Pwned (HIBP) provides compromised credential analysis, with expanded breach intelligence in development. While the solution lacks direct integrations with SIEM, SOAR, and ITSM, it supports log forwarding via Windows Event Logs, with alerting possible through email and Microsoft Teams. Its dual-layered risk scoring evaluates threats by severity and remediation complexity, though without AI/ML or contextual enrichment.

The combination of delegated administration, hybrid identity management, and instant forest recovery presents a strong value proposition for organizations deeply dependent on Microsoft technologies. Guardian's instant rollback and recovery approach provide clear operational advantages for reducing downtime and maintaining continuity in critical identity systems. At the same time, limitations are visible in the absence of machine learning for adaptive detection and lack of contextual risk modeling. Additionally, reliance on manual or external playbooks for response may limit organizations seeking fully automated remediation workflows. These trade-offs highlight Cayosoft's clear strengths in focused ITDR protection for Microsoft environments, alongside areas for growth in broader integration and advanced analytics.

Cayosoft's solutions are particularly well-suited for mid-sized and large enterprises relying heavily on Microsoft infrastructures, including organizations with hybrid or legacy Active Directory estates that require strong ITDR protections. Industries such as finance, government, manufacturing, and insurance benefit from Cayosoft's ability to manage delegated administration, monitor for identity-based threats, and rapidly recover directory services in the event of compromise. For enterprises looking to strengthen Microsoft Active Directory and Entra ID security posture, simplify administration, and ensure business continuity through advanced recovery, Cayosoft offers a compelling solution worth close consideration.

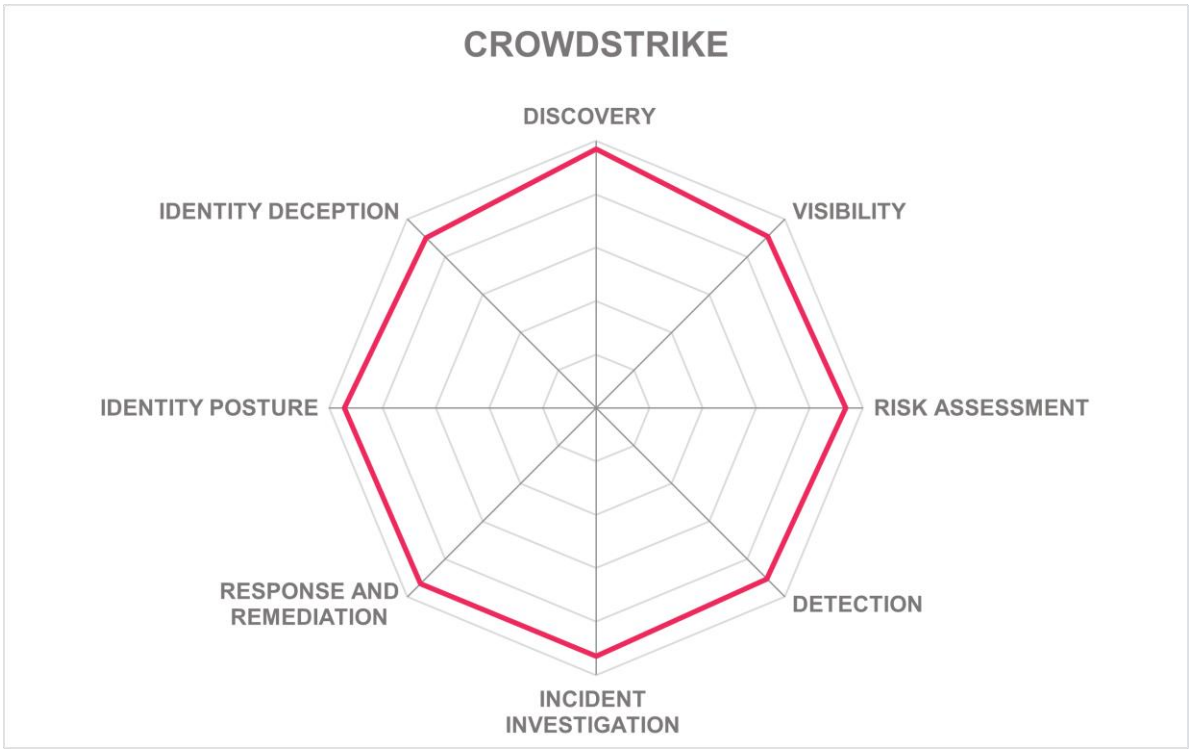
Strengths

- Suitable for Microsoft hybrid infrastructures
- Instant standby Active Directory Forest recovery
- Delegated administration with lightweight PAM features
- Over 250 prebuilt templates for identity workflows
- Real-time monitoring and rapid rollback capabilities
- Dual-layered risk scoring model
- Supports detection of AD-specific advanced attacks
- Flexible deployment across on-premises and cloud

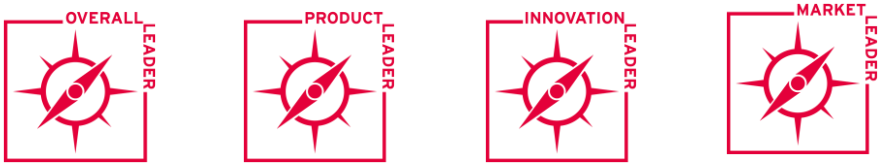
Challenges

- ISO/IEC 27001 certification in work
- No direct SIEM, SOAR, or ITSM integrations
- No use of ML or AI in detection
- Risk scoring lacks business context
- No native PAM or IGA integrations
- Needs more coverage for non-Microsoft environments

CrowdStrike – Falcon Next-Gen Identity Security



Leader in



CrowdStrike, founded in 2011 and headquartered in Austin, Texas, has established itself as a prominent security vendor focused on endpoint, cloud, and identity defense. Its SaaS-delivered Falcon platform provides security capabilities spanning detection, response, and prevention of identity-driven and adversary-based threats Falcon Next-Gen Identity Security is licensed on a per-user basis and is positioned to serve organizations of all sizes, from enterprises to mid-market customers, across industries such as finance, healthcare, retail, and the public sector. The solution is deployed within CrowdStrike's cloud infrastructure and integrates with major identity providers, SaaS services, and IT security tools. It includes regulatory compliance with frameworks such as FIPS 140-2, SOC 2 Type 2, HIPAA/HITRUST, FedRAMP, and others. In addition, their proactive stance on privacy, reflected in their certification under the EU-U.S. and Swiss-U.S. Data Privacy Frameworks. API authentication methods supported include OAuth2, OIDC, SAML, JWT, RADIUS, and key exchange, while API protocols provided include REST and GraphQL.

Given CrowdStrike's long history in InfoSec and SOC practices, Falcon Next-Gen Identity Security provides features to help bridge identity administration and identity security. It does this by providing guidance to InfoSec personnel who may not have deep knowledge of AD and Entra ID. The Falcon Next-Gen Identity Security platform provides visibility into identity

environments spanning Active Directory, Entra ID, Okta, Ping, and AWS IAM Identity Center, as well as SaaS applications through Falcon Shield. It offers a classification framework to distinguish between human and non-human identities, including service accounts and AI agents, applying AI-driven behavioral and attribute-based models. The solution combines discovery and posture management by continuously analyzing identity attributes, permissions, and group memberships alongside historical activity to highlight misconfigurations and excessive privileges. For detection, Falcon correlates identity-based anomalies with endpoint and cloud telemetry. Response capabilities include automated enforcement actions and 40+ pre-configured policies and 11 playbooks provided through Falcon Fusion. Integration with SIEM, SOAR, PAM, IGA, ITSM, and access management solutions ensures incident data flows across enterprise security operations, while Charlotte AI assists with triage, correlation, and reducing false positives.

A differentiator is Falcon Privileged Access, which extends ITDR into cloud PAM with Just-in-Time access controls designed to eliminate standing privileges in Entra ID and Active Directory environments. The solution also provides integrated or standalone Identity Segmentation capabilities and risk-based conditional access across hybrid environments. The breadth of third-party integrations is a further strength, allowing enterprises to align Falcon Next-Gen Identity Security with diverse IAM, IT, and security investments. However, certain elements could be expanded, such as broader out-of-the-box coverage for non-Microsoft environments, where current focus is strongest. Some organizations may also find the platform's complexity a factor in deployment planning and tuning for ITDR use cases. That said, CrowdStrike's consistent investment in expanding identity coverage and enhancing automation demonstrates a clear trajectory toward addressing these gaps and strengthening its ITDR capabilities further.

CrowdStrike primarily serves North America, with increasing adoption across EMEA, APAC and Latin America. The solution is valuable for organizations with hybrid identity deployments, particularly those balancing Active Directory with modern cloud identity services. Falcon Next-Gen Identity Security is also suited for security teams seeking to consolidate ITDR with endpoint and cloud defense under a single platform, as well as enterprises pursuing advanced AI-driven correlation and automated response at identity scale.

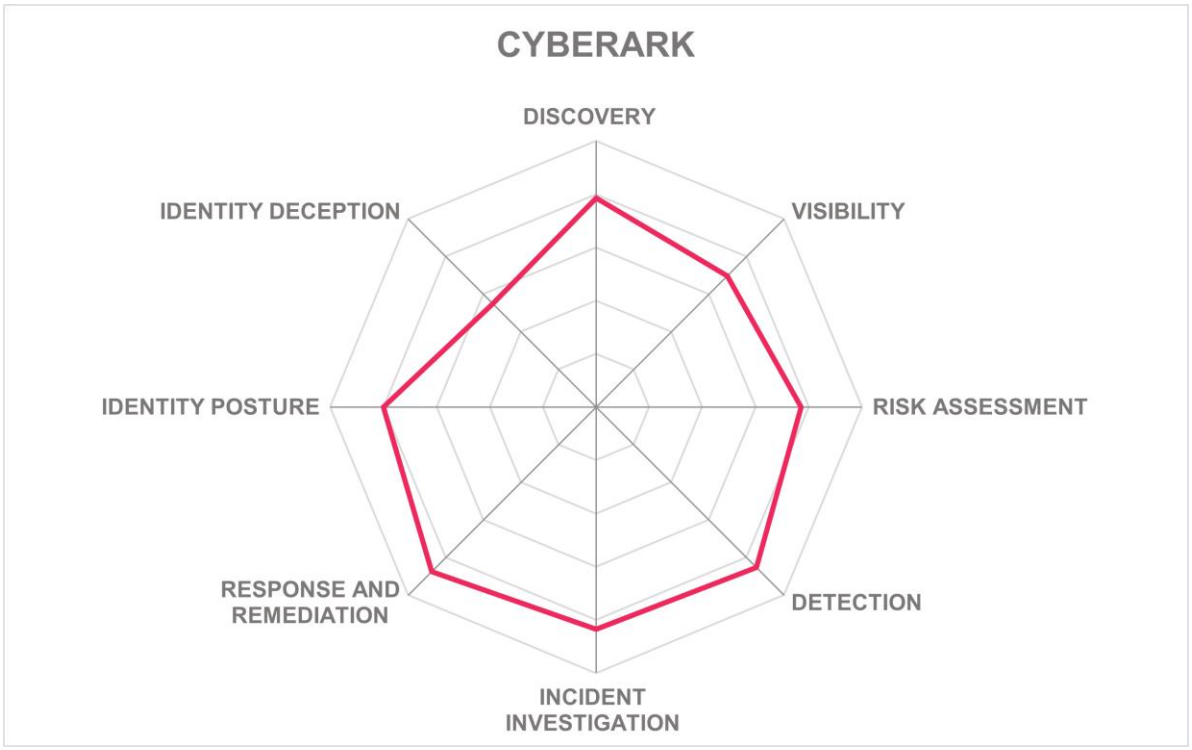
Strengths

- Dynamic user risk profiles
- AI-driven correlation across identity, endpoint, and cloud telemetry
- Adversary-focused analytics with Charlotte AI triage
- Extensive integration with SIEM, SOAR, IGA, PAM, and ITSM tools
- Just-in-Time privileged access for AD and Entra ID
- Honeypot account support for deception-based detection
- Strong regulatory compliance coverage across industries
- Pre-built playbooks and policy templates for automated response

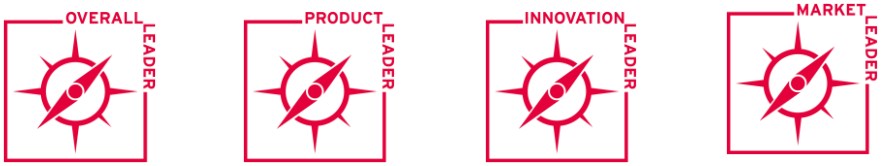
Challenges

- Customer base still concentrated in North America
- The platform's complexity may require additional planning and tuning.
- The company's customer base is primarily in SOCs, so they will need to court identity administration teams

CyberArk – CyberArk Identity Security Platform



Leader in



Having been in the market since 1999, CyberArk has established itself as a leader in Identity Security. Headquartered in Israel and the United States, the company maintains a global footprint across North America, EMEA, and APAC, with a smaller but growing presence in Latin America. In July 2025, Palo Alto Networks announced an agreement to acquire CyberArk, further solidifying its strategic position in identity security and threat detection. CyberArk primarily serves medium and large enterprises, though smaller organizations also adopt its offerings. Its customer base spans regulated industries such as finance, government, manufacturing, and healthcare. The company's licensing follows a subscription model, structured per user and time period, with modular licensing options based on capability and consumption tiers. API authentication methods supported include OAuth2, OIDC, SAML, and JWT. REST APIs are the primary interface for integration while Webhooks are available for event-driven workflows. Delivery options include SaaS, hardware appliances, virtual appliances, and containerized deployments, all designed to meet compliance standards such as ISO 27001, SOC 2, HIPAA/HITRUST, FedRAMP, and others.

The CyberArk Identity Security Platform provides a broad defense-in-depth solution with integrated ITDR capabilities across the entire identity lifecycle. Supported deployment models cover cloud, hybrid, and on-premises environments, with coverage extending across Windows, Linux, SaaS, and container-based infrastructures. Its ITDR functionality relies on real-time risk scoring, behavioral analytics, and the CyberArk CORA AI engine for anomaly detection. It integrates with Microsoft, IBM, Okta, One Identity, and Ping Identity. CyberArk's discovery and visibility capabilities include credential intelligence that uncovers weak or reused credentials, alongside detection of shadow identities and misconfigurations across cloud and hybrid systems. For posture management, the solution enforces least privilege through just-in-time and adaptive policies across human and machine identities. Detection methods combine endpoint telemetry, session monitoring, log correlation, and cloud entitlement insights to surface credential abuse, session hijacking, privilege escalation, and lateral movement attempts. Investigation and response workflows are supported with automated remediation, including session termination, privilege reduction, or account revocation.

The platform integrates natively with SIEMs, SOAR, ITSM, XDR, and access management tools. For example, the CyberArk Marketplace offers more than 300 pre-built integrations. CyberArk provides AI-assisted investigation with CORA AI, including automated summaries of SSH and web sessions, and remediation recommendations for unmanaged or misconfigured identities. CyberArk's privileged session isolation, threat-based access controls, and adaptive MFA capabilities provide a strong defense for sensitive identities. However, challenges remain in specific areas: integrations with IGA platforms are limited beyond vendors such as SailPoint and Saviynt. The intended acquisition by Palo Alto Networks may enhance long-term scale and reach, though effective alignment of product roadmaps and customer engagement models will be an important area to watch. CyberArk's platform is well-suited for organizations managing large-scale, heterogeneous environments spanning on premises, SaaS, and multi-cloud systems. CyberArk's ITDR capabilities are especially relevant for security teams looking for automated response workflows and strong integrations into existing SOC and ITSM tooling. Enterprises with broad privilege management needs, high compliance requirements, or reliance on service and machine identities will find CyberArk's approach to ITDR particularly attractive.

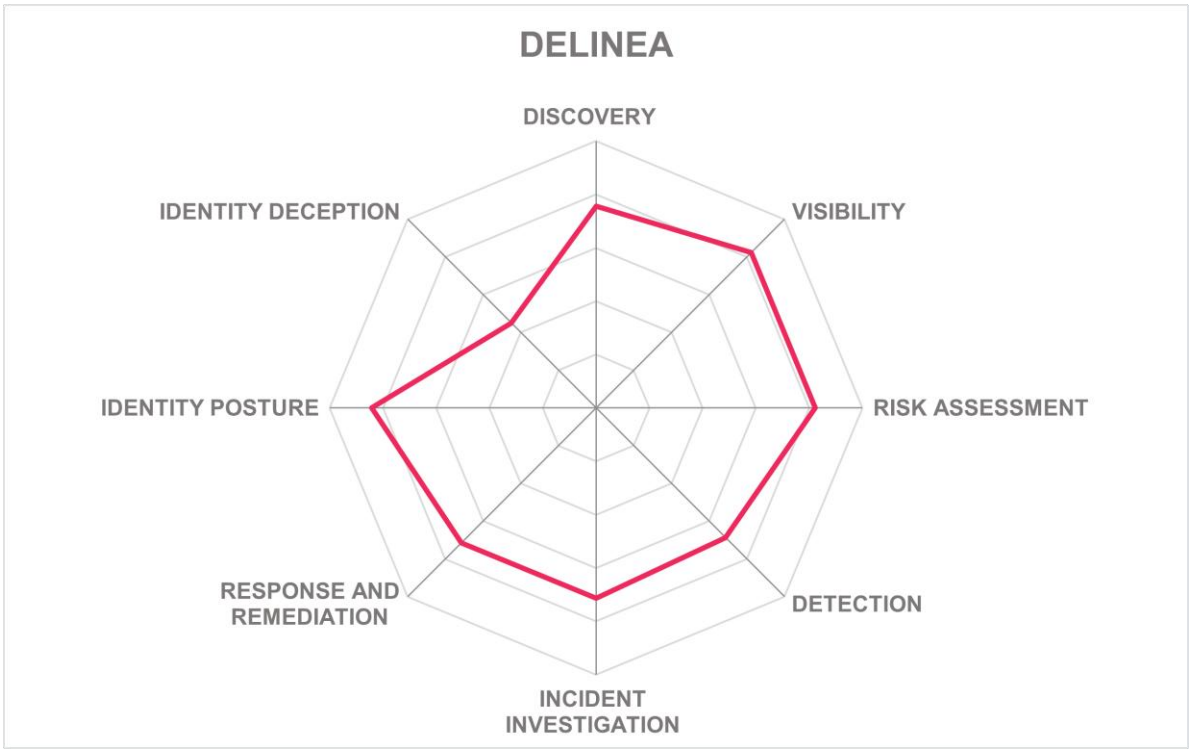
Strengths

- Embedded ITDR across entire platform
- Broad deployment and delivery models
- AI-powered threat detection and remediation
- Strong privileged session isolation and monitoring
- Credential intelligence and behavioral analytics
- Wide integration portfolio with SIEM, SOAR, and ITSM
- Flexible licensing by capability and scale
- Extensive compliance certifications

Challenges

- No support for access path visualization
- Limited native IGA integrations
- Complexity in deployment for smaller enterprise
- Heavy reliance on partner-supported integrations
- Alignment needed after intended Palo Alto Networks acquisition

Delinea – Delinea Identity Threat Protection



Leader in

Delinea, based in San Francisco, USA, emerged in 2021 from the merger of two established players in PAM. Building on this foundation, the company has expanded its portfolio to include IGA, CIEM, and ITDR. Its primary ITDR offering is Delinea Identity Threat Protection (ITP), available as part of the Delinea Platform or as a stand-alone SaaS solution. The licensing model is identity-based with unlimited connected applications. Deployment options include both on-premises and cloud service models. API authentication methods include OAuth2, OIDC, SAML, JWT, and key exchange, with support for REST and Webhooks. Compliance certifications include ISO/IEC 27001, US FedRAMP, UK Cyber Essentials, and SOC 2 Type 2. The solution targets mid-market and enterprise customers across multiple industries, including finance, manufacturing, government, education, and telecommunications, with regional coverage focused on North America, followed by EMEA, APAC, and Latin America.

Delinea ITP provides a unified platform for identity detection, monitoring, and response. Detection capabilities apply credential intelligence and UEBA to establish behavioral norms

and surface anomalies such as privilege escalation, credential reuse, or excessive permission use. Advanced analytics synthesize data across identity providers, SaaS applications, and cloud platforms to provide actionable insights for security teams. The solution integrates with Microsoft Sentinel and Splunk for SIEM, ServiceNow for ITSM, and both Microsoft Sentinel and ServiceNow for SOAR, enabling automated ticketing, alerting, and remediation workflows. Out-of-the-box playbooks support access revocation, permission right-sizing, session termination, and secret rotation. While current playbook capabilities are somewhat limited in customization, plans are in place to enhance these features. Risk scoring is customizable to organizational policies and can incorporate external inputs. AI initiatives, including Delinea AIDA, further extend these capabilities with real-time analysis of privileged sessions using LLMs and Optical Character Recognition (OCR), producing intent summaries, advanced detection, and automated remediation actions aligned with the MITRE ATT&CK framework.

Delinea ITP extends its ITDR capabilities to NHIs. The solution is designed to analyze and manage the access levels of NHIs across various environments. This includes automated processes and AI agents that may interact with different systems and data repositories. By enriching its unified risk engine with NHI-specific context, The platform surfaces threats including shadow accounts, excessive permissions, and misuse of credentials. In addition, the solution supports standard processes for case management, incident management, collection of forensic evidence, and ticketing. Delinea's deception capabilities use a dynamic, context-aware approach that lets customers define and deploy adaptive traps tied to real identity assets. Their Iris AI enhances detection and response by analyzing session activity, correlating user behavior with intent, and enabling AI-driven authorization decisions across the platform. However, the solution does not provide broad third-party response orchestration beyond its limited SOAR integrations. Broader SIEM support and IGA integrations are also absent.

With strong cloud integration, the platform supports quick deployments and scalability across different geographic regions. Delinea ITP is particularly relevant for organizations with high privilege management requirements. Enterprises adopting the Delinea Platform benefit from the convergence of PAM and ITDR in a single environment, and those with significant machine identity use cases will find the NHI-focused detection and remediation features valuable. Customers prioritizing AI-driven detection, faster triage, and integration into Microsoft Sentinel or ServiceNow ecosystems should also evaluate the solution. Delinea ITP provides a strong option for identity-centric detection and response, particularly where privilege management is central to security strategy.

Strengths

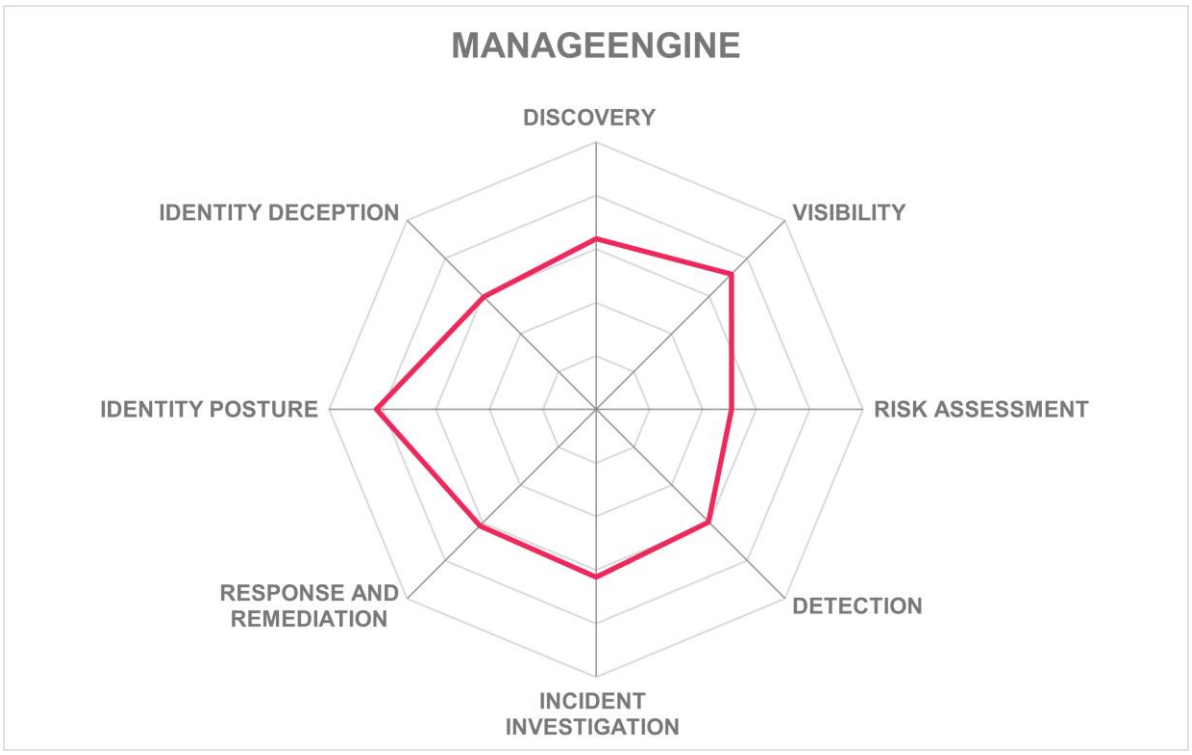
- Iris AI for authorization and analytics
- Strong integration of PAM and ITDR capabilities
- AIDA provides real-time AI-driven session analysis
- Human and non-human identity classification logic
- Continuous discovery of assets, entitlements, and misconfigurations
- MITRE ATT&CK aligned attack path mapping
- Pre-built remediation playbooks with automation options

- Integration with Sentinel, Splunk, and ServiceNow
- Compliance with ISO 27001, SOC 2, FedRAMP, and UK Cyber Essentials

Challenges

- Limited third-party SOAR integration support
- Restricted SIEM integration to only Splunk and Sentinel

ManageEngine – ManageEngine AD360, PAM360, and Log360



Leader in

ManageEngine, a division of Zoho Corporation founded in 2002 and headquartered in Texas, USA, offers a broad portfolio of IT management and security solutions. Its offerings span IT help desk, patch, and vulnerability management, SIEM, MDM, IGA, PAM, analytics, and low-code development tools. The vendor serves organizations of all sizes across a wide variety of industries, with subscription models based on metrics such as users, domains, or domain controllers. Deployment options include on premises and public cloud. Within the ITDR space, ManageEngine's focus lies in AD360, PAM360, and Log360, which together address identity governance, privileged access, auditing, detection, and remediation across hybrid IT environments. ManageEngine supports API authentication via OAuth2 and JWT and exposes REST and Webhook interfaces for integration with external systems. The company's solutions are certified against multiple global compliance standards, including ISO/IEC 27001, SOC 2 Type 2, HIPAA/HITRUST, and UK Cyber Essentials.

AD360, a unified IAM suite, combines identity governance, privileged access, auditing, detection, and recovery capabilities. ADManager Plus automates provisioning,

deprovisioning, and access rights management, while ADAudit Plus provides real-time change auditing and user behavior analysis. ADSelfService Plus delivers MFA, password resets, and SSO, while PAM360 enforces secure credential management, just-in-time access, and privileged session recording. RecoveryManager Plus adds resilience through granular Active Directory and Microsoft 365 recovery functions. Log360 operates as the SIEM and UEBA foundation, correlating logs across AD, cloud environments, and endpoints while integrating with Splunk and offering built-in SOAR capabilities. Visibility is strengthened through graphical mapping of privilege escalation paths and risk scoring using NIST SP 800-30 guidelines. AI-driven Zia Insights enhances detection and investigations by contextualizing log data, reconstructing incident timelines, and mapping alerts to MITRE ATT&CK techniques. The platform integrates with ITSM tools such as ServiceNow, JIRA, and Freshservice to support ticketing and incident workflows.

ManageEngine provides a modular, tightly integrated stack, where identity governance, privileged access, and SIEM work together without requiring third-party integrations. This in-house alignment reduces operational friction and provides organizations with a unified approach to ITDR. Its visual risk assessment and privilege path mapping stand out as capabilities that increase administrator awareness of exposure. However, challenges remain: the platform lacks role discovery, does not support rollback for automated remediation, and conditional access policy enforcement based on risk signals is absent. Additionally, while the built-in SOAR covers essential use cases, there is no support for third-party SOAR integration, which may limit flexibility for organizations running heterogeneous SOC environments.

ManageEngine primarily addresses organizations seeking broad ITDR capabilities integrated with wider IT operations and security functions. Its reach extends across North America, EMEA, APAC, and Latin America, serving enterprises from mid-market to large-scale environments. The solution is well-suited for industries with strict compliance requirements, such as healthcare, finance, and government, where auditing, reporting, and privileged access control are essential. Organizations that are already ManageEngine and Zoho customers may find it easy to add AD360 and Log360 to their security portfolios.

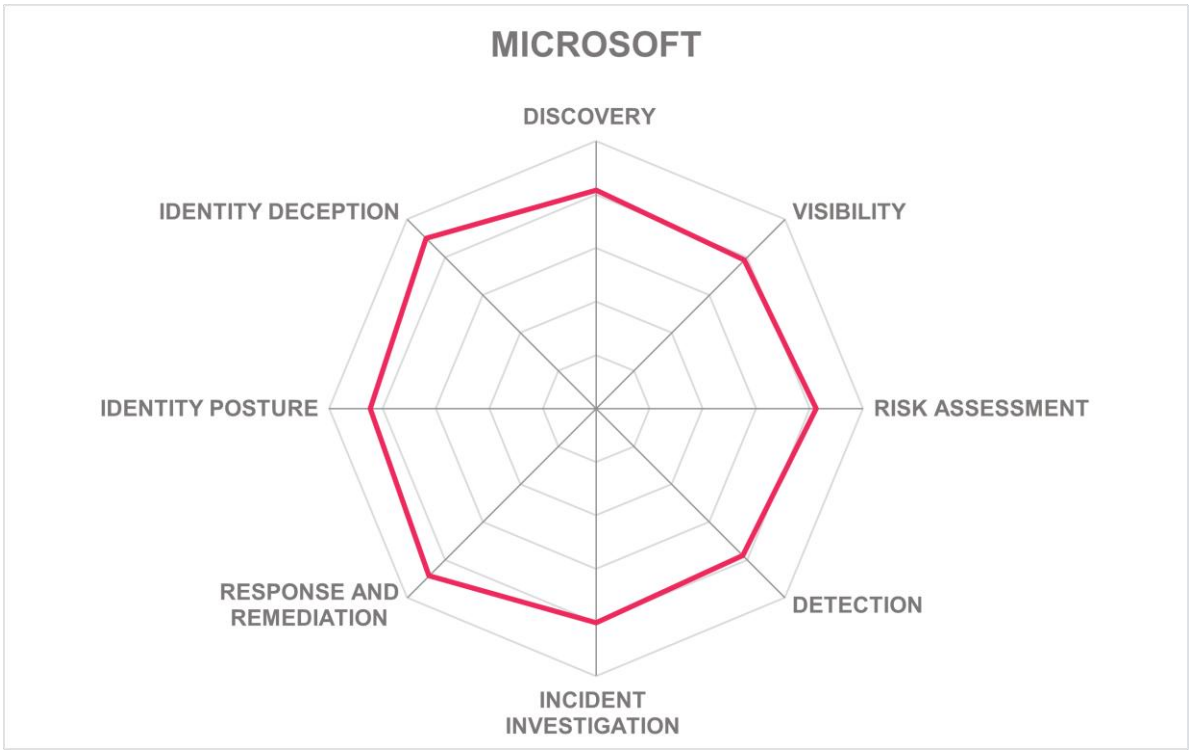
Strengths

- Modular suite covering IAM, PAM, SIEM, and ITDR
- Strong compliance certifications across multiple regions
- Visual risk maps of privilege escalation paths
- AI-driven incident insights and MITRE ATT&CK mapping
- Integrated UEBA for behavioral anomaly detection
- Automated remediation with drag-and-drop playbook editor
- Dark web monitoring for exposed credentials
- Broad ITSM integrations for incident management

Challenges

- No rollback options for automated remediation
- Conditional access policies not risk-triggered
- No third-party SOAR, IGA, and PAM integrations available
- Lack of support for SDN failover and performance optimization

Microsoft – Entra ID and Defender for Identity



Leader in

Founded in 1975 and headquartered in Redmond, Washington, Microsoft is one of the most influential players in both enterprise IT and cybersecurity. Its ITDR capabilities are delivered through Microsoft Entra ID and Microsoft Defender for Identity, which can be jointly deployed to provide advanced identity protection, detection, and response. Entra brings a mature identity platform that addresses workforce, customer, and workload identities with strong authentication, conditional access, and governance capabilities. Defender for Identity, deeply integrated with Microsoft Defender XDR, builds on this foundation to provide continuous monitoring and response against credential theft and lateral movement across both Active Directory and cloud environments. These services are delivered primarily as SaaS, with optional lightweight sensors for on-premises identity infrastructure and are available through the Microsoft E5 and E5 Security bundles. API authentication methods supported include OAuth2, SAML, OIDC, and JWT, while available protocols include REST and OData. Licensing is offered on a per-user basis. Compliance certifications cover a broad range of global security and privacy standards.

Microsoft's ITDR offering combines Entra's real-time risk evaluation and policy enforcement with Defender's ability to detect identity-based threats within broader attack campaigns. Entra ID Protection continuously assesses user and sign-in risk using machine learning, behavioral analytics, and threat intelligence, feeding directly into adaptive conditional access policies. Defender for Identity extends detection across domain controllers, AD Federation Services, and certificate services, providing deep visibility into credential misuse, dormant accounts, and lateral movement attempts. Deception techniques with decoy accounts add further detection precision. Microsoft Security Copilot enhances this with AI-driven summarization, recommendations, and contextual insights, supporting triage and response across identity incidents. Its new specialized agents, such as the conditional access optimization agent, can proactively refine access policies, while the risky user pane provides contextual risk analysis. Integration spans SIEM (Microsoft Sentinel, Splunk, FortiSIEM), SOAR (IBM Resilience, ServiceNow, Micro Focus), ITSM (ServiceNow, JIRA, BMC), IGA (SailPoint, Oracle), PAM (CyberArk, BeyondTrust, Delinea), and access management providers.

The platform's ability to correlate identity telemetry with signals across endpoints, email, cloud workloads, and SaaS delivers contextualized detections that accelerate investigations and drive coordinated response. Incident response is further supported by Microsoft Sentinel, which provides more than 200 prebuilt playbooks and customizable workflows, allowing organizations to automate containment actions such as isolating hosts, blocking malicious IPs, or disabling compromised accounts. Microsoft's scale also enables continuous enrichment of detections with global threat intelligence. However, challenges remain, including the complexity of deploying and managing such a broad suite across varied customer environments, potential overlap across product lines that can cause confusion, and the risk of vendor lock-in where organizations rely heavily on the Microsoft stack. Enhancements in usability and clearer product delineation would improve adoption in complex multi-vendor settings.

With global coverage across industries such as financial services, healthcare, government, and critical infrastructure, the company addresses use cases from insider threat detection and credential theft prevention to automated response. Microsoft's ITDR solutions are relevant to organizations of all sizes, though their strongest fit lies with enterprises that already operate within the Microsoft ecosystem. Security teams looking to consolidate identity and security operations under a unified model will find Microsoft's approach especially valuable.

Strengths

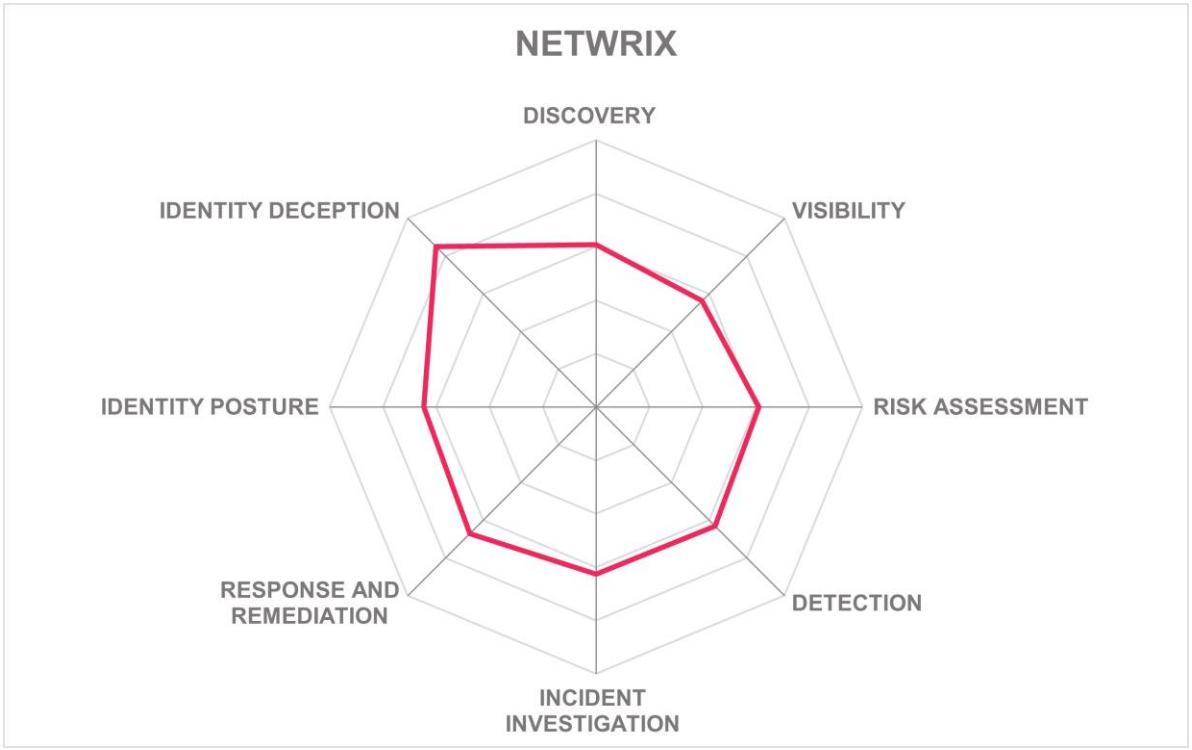
- Native integration between Entra and Defender
- Strong AI-driven Copilot capabilities for SOC and identity admins
- Real-time adaptive conditional access with risk scoring
- Automated attack disruption for identity-based threats
- Extensive integrations across SIEM, SOAR, and ITSM
- Rich global threat intelligence fueling detections
- Broad compliance certifications across global standards

- For organizations already committed to Microsoft infrastructure, this solution interoperates with and extends other critical services

Challenges

- Complex deployment across large, varied environments
- ITDR solutions require licensing multiple products
- More integrations for IGA and PAM would be beneficial
- Limited suitability for organizations without full Microsoft stack

Netwrix – Netwrix ITDR



Founded in 2006 and headquartered in Frisco, Texas, Netwrix Corporation delivers IT security and governance solutions to mid-market and enterprise organizations across North America, EMEA, APAC, and Latin America. Its customer base spans finance, healthcare, government, and manufacturing, supported by a network of system integrators providing consulting, implementation, and managed services. The Netwrix ITDR solution is built on a set of products including PingCastle, Access Analyzer, Threat Prevention, Threat Manager, Recovery for Active Directory, and 1Secure. While customers primarily deploy the software on-premises, public cloud support is available, and 1Secure delivers a SaaS option. Licensing follows a per-user model. Standards certifications such as ISO/IEC 27001 and SOC 2 Type 2 are not yet achieved but are on the roadmap. Supported protocols include REST, WebSockets, and AMQP, with authentication standards such as SAML, OIDC, and JWT.

Netwrix's ITDR solution provides broad visibility into Active Directory and Entra ID environments, detecting identity-centric threats including credential compromise, privilege misuse, and lateral movement. Discovery extends to service accounts, using machine learning to identify repeatable or anomalous activity and uncovering configuration weaknesses. For detection and investigation, Threat Manager applies customizable risk scoring models, derived from the PingCastle methodology, which prioritize critical exploits such as Golden Ticket attacks. Deception features include honeytokens to expose

credential-dumping tools. Response capabilities include over 30 customizable playbooks for automated or manual actions, and Threat Prevention enforces policy-based blocks against high-risk operations in Active Directory. It also features recovery options to address incidents, offering solutions to rollback changes in identity attributes and recovery from deletion events. Netwrix's unique patented Threat Prevention technology blocks high-risk Active Directory operations in real time. By stopping privileged-group changes, unauthorized domain-replication requests, LSASS credential-dump attempts, and other sensitive actions, it helps prevent identity-driven attacks such as DCSync. The solution also identifies well-known AD attack methods such as golden and silver ticket attacks, DCSync, DCShadow, and Kerberos-based exploits. Integration support is strongest with SIEM solutions, ServiceNow for ITSM and SOAR, and custom extensions via PowerShell, while native links to PAM and IGA rely on other Netwrix tools.

The ability to rapidly restore compromised directories stands out, alongside GenAI-assisted remediation guidance, which contextualizes vulnerabilities and helps administrators tailor corrective action. The customizable risk models provides organizations flexibility in tailoring ITDR to their environments. Challenges remain, including the lack of current compliance certifications which may constrain adoption in regulated industries. The SaaS offering, while present, is secondary to the on-premises model, which could limit appeal among cloud-first enterprises. Nonetheless, the combination of risk scoring, deception, response, recovery, and AI-driven contextualization positions Netwrix as a notable competitor in ITDR.

Netwrix's ITDR solutions are well-suited for mid-sized to large enterprises that rely heavily on Active Directory and Entra ID. The product serves customers seeking visibility, control, and remediation for identity-centric risks across hybrid environments. Organizations with established SIEM deployments or those already leveraging Netwrix Privilege Secure or Directory Manager will find particularly strong synergies. Netwrix ITDR is a solution that security-conscious organizations should evaluate for protecting critical identity infrastructures.

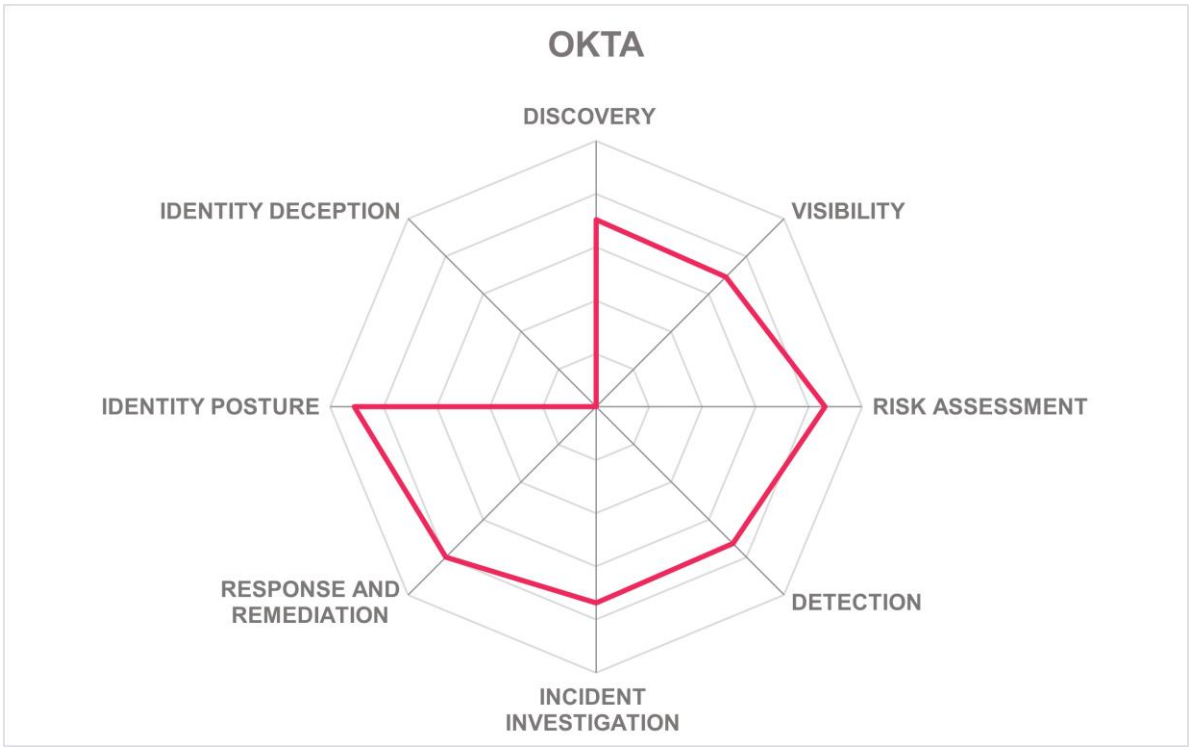
Strengths

- Strong Active Directory and Entra ID coverage
- Customizable PingCastle-based risk scoring
- Deception techniques for credential attack detection
- GenAI-driven remediation guidance
- Robust directory recovery capabilities
- 30+ playbooks for automated response
- Wide SIEM integration support
- Effective service account discovery with ML

Challenges

- SaaS execution and maturity must be ensured
- No ISO/IEC 27001 or SOC 2 certification yet
- Few out-of-the-box ITSM/SOAR integrations

Okta – Okta and the Auth0 Platform



Leader in

Okta, headquartered in San Francisco, California, has built its reputation as one of the most recognizable identity providers, serving both workforce and customer identity requirements. Founded in 2009, the company has expanded aggressively through acquisitions such as Auth0 (2021) for CIAM and developer capabilities, atSpoke for IGA, Spera Security (2024) for identity security and posture management, and Axiom Security (2025) for privileged access. The company offers its products exclusively as SaaS with native multi-tenant cloud delivery; single tenant options are also available. Auth0, its developer-centric CIAM platform, extends deployment flexibility with public and private cloud options. Licensing is available through per-user or per-month models, along with active user, transaction, and usage-based tiers. Okta's customer base spans diverse industries, including finance, healthcare, and technology, with regulatory certifications covering FedRAMP, SOC 2, ISO/IEC standards, HIPAA, and PCI-DSS.

Okta's ITDR capabilities span multiple areas across both the Okta and Auth0 platforms, designed to defend against account takeover, session hijacking, and other advanced identity

threats. Its ITDR approach is layered across the authentication journey, using adaptive MFA, credential intelligence, and contextual risk scoring to detect anomalies. Discovery and visibility are supported by ISPM, which surfaces over-permissioned accounts, unused entitlements, and risks across high-value resources. Identity Threat Protection with Okta AI (ITP) provides real-time detection and response to identity-based threats during and after authentication. Detection techniques include UBA, bot detection with over 60 signals, and machine learning–driven heuristics that generate composite confidence scores. ITP analyzes multiple signal categories including IP reputation changes, device context changes, network risk indicators, and third-party threat intelligence. The platform enriches detection through Shared Signals Framework (SSF) integrations with security vendors including CrowdStrike, Palo Alto Networks, Netskope, and others to enable bidirectional threat intelligence sharing that improves detection accuracy across the security ecosystem. This score dynamically adjusts throughout a session. Responses are both inline and orchestrated, ranging from adaptive MFA challenges and step-up authentication to automated workflows that trigger credential resets, and third-party incident response actions. Administrators can use pre-built or customized playbooks to terminate sessions via the Universal Logout feature, enforce new policies, or remediate suspicious activity through custom actions. Moreover, Okta integrates with SIEMs, ITSM platforms, SOAR solutions, and XDR tools to distribute risk signals and orchestrate incident response.

Okta extends its ITDR capabilities with a strong focus on securing AI agents and workloads. Administrators gain oversight of bots, workloads, and service accounts through ownership mapping, policy enforcement, and automated reviews and remediation. The platform also applies AI-based tagging to distinguish service accounts from human users. Another clear strength of Okta's ITDR capabilities is its expansive integration strategy, from workflows templates to SSF connections, making the platform versatile across enterprise security architectures. This framework enables cross-vendor collaboration to enhance threat detection and response capabilities. However, challenges remain, including potential complexity when configuring advanced workflows and reliance on SaaS delivery, which may not satisfy customers with strict data residency constraints.

With a primary concentration in North America but growing activity in EMEA, APAC, and Latin America, Okta has a global footprint suitable for multinational deployments. Organizations with advanced use cases around AI-driven identities or those seeking a unified approach across workforce, CIAM, and privileged access management will find the solution particularly relevant. This makes Okta a platform of interest for those looking to modernize their identity-based detection and response capabilities.

Strengths

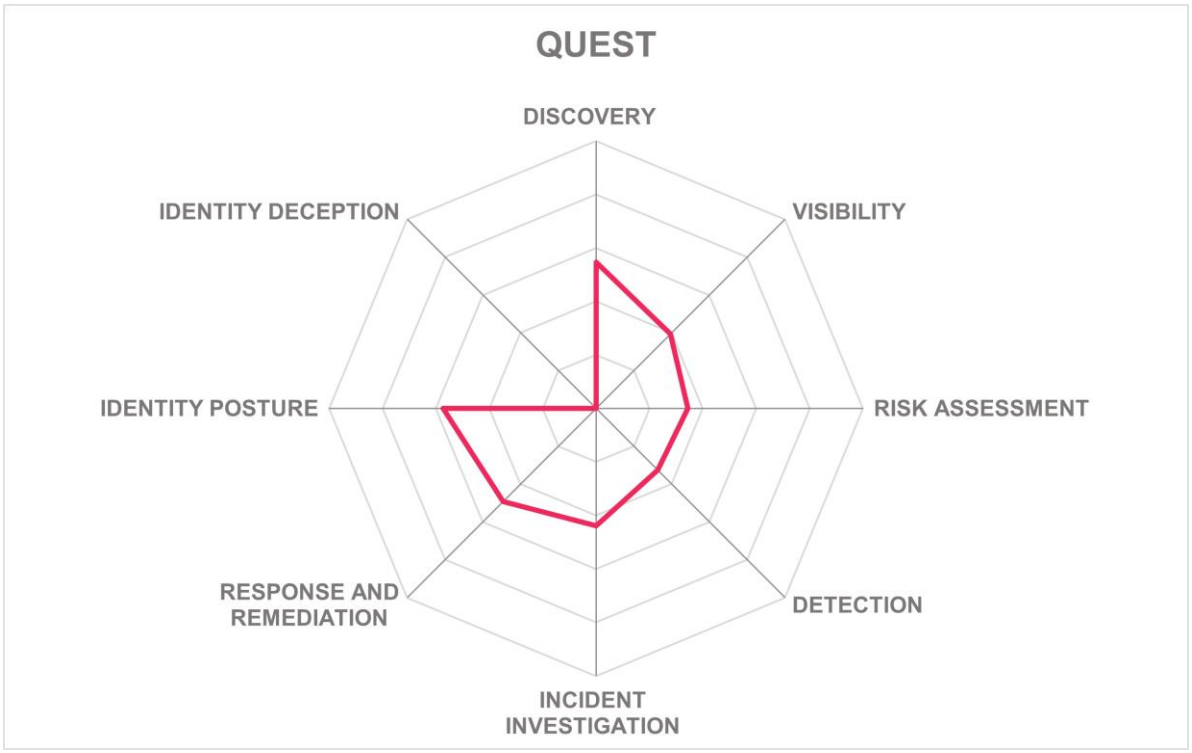
- Strong multi-tenant SaaS architecture
- Integrated Identity Security Posture Management
- Broad SIEM, SOAR, XDR, and ITSM integrations
- Continuous evaluation, adaptive MFA with contextual risk scoring
- Dynamic policy evaluation
- Universal Logout and other real-time actions for rapid remediation
- GenAI security and AI agent protection focus

- Credential intelligence with behavioral analytics
- Expansive library of workflow templates

Challenges

- No support for attack path mapping
- Investigation capabilities could be deeper
- Lack of role discovery features
- No identity-centric TTP mappings to MITRE ATT&CK
- No native decoy capability, reliant on partner integration

Quest – Quest Security Guardian



Quest Software, founded in 1987 and headquartered in Aliso Viejo, California, offers a portfolio spanning data management and governance, migration and modernization, identity, security, and backup and recovery. Within the ITDR space, the company provides Security Guardian, a solution designed to strengthen AD and Microsoft Entra ID environments against identity-based threats. Quest targets organizations across industries and geographies, with notable presence in North America, EMEA, APAC, and Latin America. Security Guardian is delivered via public cloud or hybrid deployment models, with licensing sold per managed identity on an annual subscription basis. Compliance frameworks include ISO/IEC 27001, US FedRAMP, and SOC 2 Type 2. The platform supports OAuth2 and OIDC authentication methods.

Security Guardian provides ITDR functionality tailored to hybrid identity infrastructures, integrating tightly with Microsoft environments. The platform is built around role-based models, supporting both predefined and custom roles, with assignments extending to Entra ID groups. Discovery and visibility capabilities identify misconfigurations, exposures, and service account anomalies, leveraging AI heuristics to distinguish automated activity from legitimate user sessions. Posture management is enabled through prioritized risk findings, while the Shields Up feature enforces Tier 0 lockdown to contain active threats and lock down identity configurations. Detection techniques combine generative AI-driven intelligence with behavioral analysis, supported by Security Guardian Intelligence (SGI), which generates

plain-language threat summaries and remediation guidance. Native playbooks remain limited, though integrations are available with Microsoft Sentinel for SOAR and with leading SIEM platforms. Planned roadmap items include decoy accounts, user-configurable risk weighting, and widget-based dashboards.

The platform extends to workload identities, covering service principals and managed identities in Entra ID. Audit and policy controls are enhanced via Security Guardian Audit, which provides real-time audit integration. However, several challenges remain. The lack of PAM, IGA, ITSM, and forensic case management integrations reduces its suitability for organizations seeking broad ITDR alignment across the IAM stack. Missing capabilities such as path visualization, identity analytics, and credential intelligence ingestion from third parties highlight further improvement areas. The platform also identifies identity-based attack methods such as LSASS dumping, golden and silver ticket attacks, DCSync, DCShadow, pass-the-hash, and Kerberos-based exploits.

Security Guardian is best suited for enterprises heavily reliant on Microsoft identity platforms, particularly those with large AD and Entra ID deployments requiring continuous monitoring, rapid containment, and prioritized remediation. Use cases where the product is most effective include detecting misconfigurations in hybrid AD, managing service and workload identities, and improving visibility into privileged roles and access. Organizations seeking deep Microsoft-native ITDR capabilities should evaluate Security Guardian, particularly if AD and Entra ID form the backbone of their identity infrastructure.

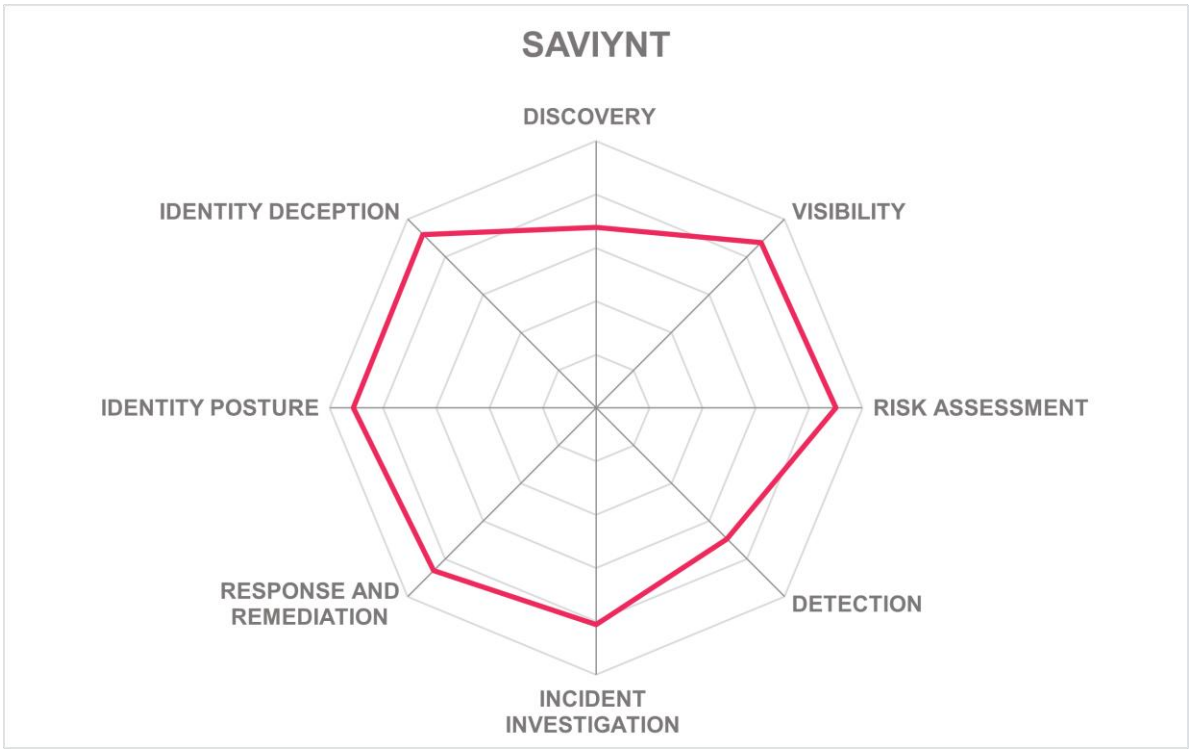
Strengths

- Strong focus on AD and Entra ID security
- Generative AI threat summaries and remediation guidance
- Dynamic Tier 0 protection for critical identity assets
- AI heuristics to detect anomalous service account activity
- Expanded workload identity protection in Entra ID
- Real-time audit integration with policy enforcement
- Agentic AI architecture with domain-specific learning

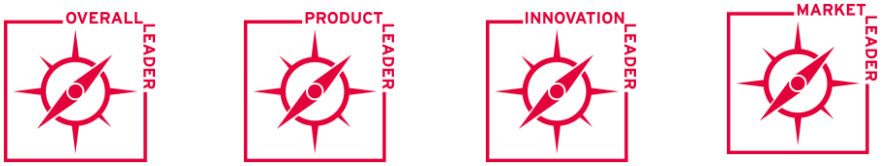
Challenges

- No path visualization or identity analytics
- Limited forensic and case management support
- Needs more coverage for non-Microsoft environments

Saviynt – Saviynt Identity Cloud



Leader in



Saviynt, founded in 2010 and headquartered in California, delivers a unified cloud-based identity security platform designed to meet the requirements of large enterprises and mid-market organizations. The company's flagship product, Saviynt Identity Cloud, integrates IGA, PAM, Access Governance, identity security posture management (ISPM), and ITDR capabilities. Offered under a per-user licensing model, the platform is available as SaaS, virtual appliance, or container-based deployment, with support for on-premises, public and private cloud, hybrid, and MSP-hosted environments. Saviynt primarily serves regulated industries such as financial services, healthcare, energy, and manufacturing. It offers extensive API support, including REST, RPC, gRPC, Webhooks, and OAuth 2.0-based authentication. Compliance is maintained with leading standards including ISO/IEC 27001, SOC 2 Type 2, NIST 800-57, FedRAMP, and France's SecNumCloud.

Saviynt ITDR is offered as part of Saviynt Identity Cloud. It is tightly interwoven with its ISPM and NHI modules, extending threat detection and response across both human and machine identities. The solution integrates with access management tools such as SecureAuth,

Broadcom, Entra ID, IBM, Micro Focus, Okta, and Ping Identity. It provides visibility through continuous discovery and classification of users, service accounts, workloads, and AI agents, ensuring that credentials, certificates, API keys, and tokens are tracked and governed appropriately. Posture management capabilities surface risks across SaaS, on premises, and cloud environments, supplemented by unified trust scoring that ingests contextual signals from security tools and vulnerability management platforms. Customers have the flexibility to adjust the weightages to these signals per their security and compliance policies. Detection employs behavioral monitoring, anomaly identification, credential intelligence, and deception techniques such as honeytokens and decoy accounts. For response, Saviynt provides customizable playbooks via a graphical editor, covering credential compromise, privilege escalation, lifecycle anomalies, and compliance violations. Additional playbooks address non-human and service account incidents, external or third-party identity issues, misconfigurations, compliance violations, and decoy access incidents, among others. Integrations with ITSM, SOAR, and SIEM platforms enable additional response types, while built-in IGA and PAM modules allow for tight policy enforcement and remediation actions such as privilege reduction, credential rotation, and just-in-time access.

Saviynt's ITDR solution provides continuous monitoring and rapid threat neutralization to reduce false positives and strengthen forensic capabilities against identity-driven attacks. The solution further distinguishes itself through its integration of identity governance with security operations. The breadth of functionality also introduces complexity, making it challenging for some customers to operate all capabilities quickly. Additionally, while integration breadth is strong, customers with heterogeneous identity estates may still face challenges in fully leveraging the platform.

Saviynt's solution is particularly relevant for organizations that must govern both human and NHIs across distributed environments. The platform appeals to organizations looking for converged identity security that extends beyond traditional IGA into ITDR, posture management, and NHI oversight. Enterprises pursuing a unified approach to discovery, detection, and response, especially those seeking to reduce identity-related attack surfaces across SaaS and cloud workloads, will find Saviynt's offering of notable interest.

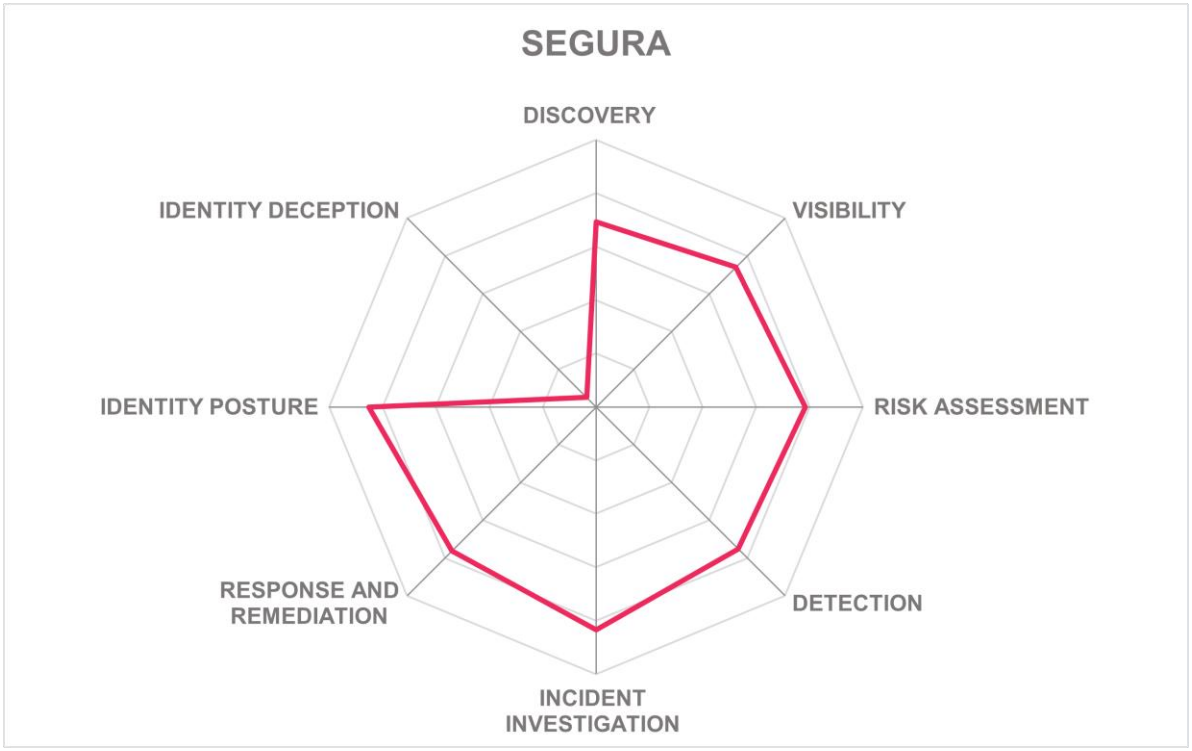
Strengths

- Converged identity security platform with broad coverage
- Strong support for human and NHIs
- Expanded capabilities for AI agent governance
- Unified trust scoring with customizable risk weighting
- Deception features including honeytokens and decoy accounts
- Granular service account governance and monitoring
- Comprehensive incident playbooks with graphical editing

Challenges

- Response alerting methods limited to email only
- Deployment complexity across large enterprise estates
- Integration challenges in heterogeneous environments
- Customer base concentrated mainly in North America, but with growing presence in EMEA and APAC

Segura – Segura 360° Privilege Platform



Leader in

Segura, founded in 2001 and headquartered in São Paulo, Brazil, delivers a broad range of privileged access and identity security solutions under its Segura 360° Privilege Platform. Formerly known as senhasegura, the company has evolved into a recognized provider of PAM, CIEM, Certificate Lifecycle Management (CLM), and ITDR capabilities. Segura supports deployment in on-premises, public and private cloud, and hybrid models, with delivery available as SaaS, managed service, hardware appliance, or container-based form factors. Licensing is based on per user and per node. Its regional strength remains in Latin America, but it is steadily growing its footprint in North America, EMEA, and APAC. Industries served include finance, manufacturing, and insurance, among others. The solution supports REST, gRPC, and Webhooks, alongside authentication standards such as OAuth2, OIDC, SAML, and JWT. It is also compliant with ISO/IEC 27001 and SOC 2 Type 2.

Segura's ITDR capabilities are embedded within its modular platform. It integrates with Microsoft, Okta, Ping Identity, and Google Workspace. Discovery and observability are delivered through credential intelligence features that map active accounts, session behavior, and unused or orphaned credentials. Posture management is advanced through its Cloud Entitlements module, which provides attack path analysis, criticality weighting, and guided remediation tailored to organizational risk context. The solution incorporates GenAI to improve usability, automate policy creation, and accelerate remediation. It generates recommended remediation scripts, giving administrators clear and actionable steps to address risks. Segura applies continuous identification to validate users during live sessions by analyzing command and behavior patterns, while its contextual risk scoring evaluates location, device, IP, and session attributes. Detection combines anomaly recognition with user behavior analytics to dynamically adjust privileges or trigger alerts. Response options are reinforced through more than 200 predefined workflows for credential rotation, access revocation, and automated remediation, with support for integration across SIEM, SOAR, ITSM, and IGA platforms.

Segura recently introduced the Quantum Connector, a universal secure bridge for cloud, OT, IoT, CPS, and on-premises systems that applies quantum-resistant encryption. Built on FIPS 203, 204, and 205 algorithms in line with NIST's PQC guidance. Segura's recognition for rapid deployment and intuitive use are additional strengths that position it well for mid-market enterprises. However, the product could be improved by expanding its integrations with third-party PAM tools and by adding support for automated incident analysis with correlation and case assembly, which would help analysts with their workflows.

While some modules may overlap with broader IAM capabilities, the consolidated approach provides significant value for organizations seeking PAM, CLM, CIEM, and ITDR within a single platform. Its coverage of IT, OT, and cloud environments makes it suitable for enterprises with OT infrastructures, while its regional strength in Latin America provides value for organizations operating or expanding in that market. Customers evaluating flexible deployment and a vendor with broad integration into SIEM, SOAR, and ITSM ecosystems should consider Segura.

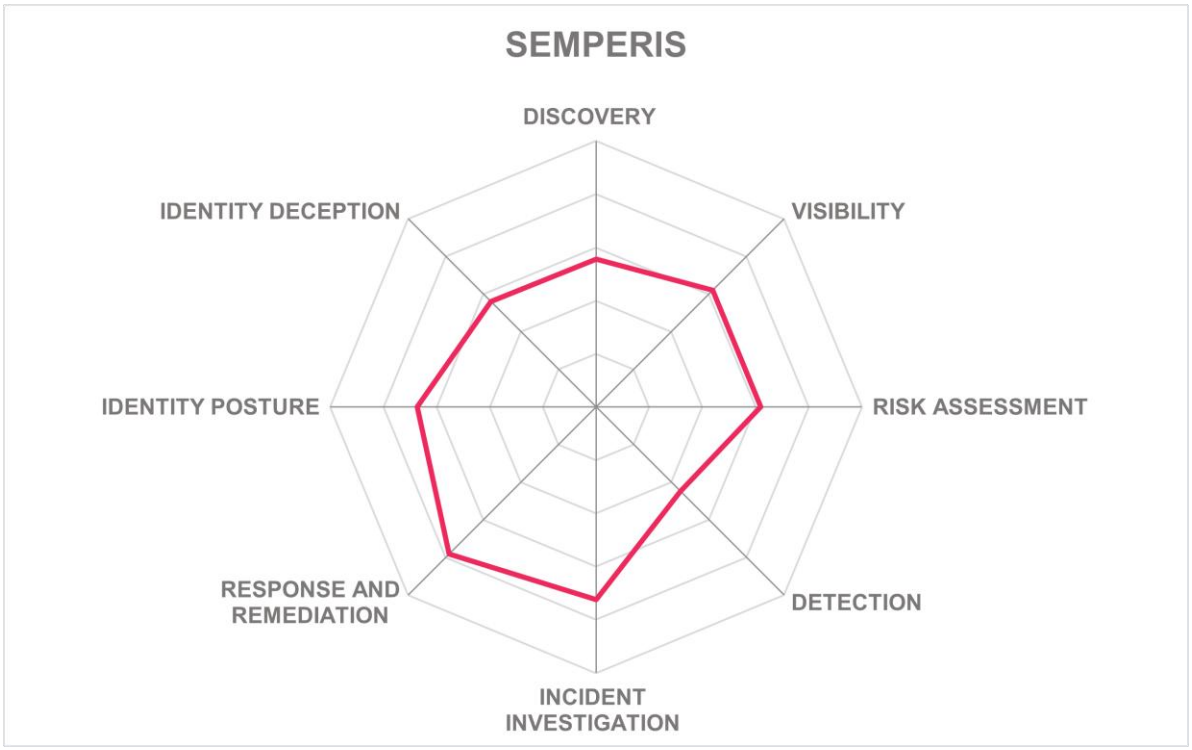
Strengths

- Broad ITDR and PAM functionality in one platform
- Strong integrations with SIEM, SOAR, and ITSM solutions
- GenAI applied for remediation and policy automation
- Continuous identification for real-time user validation
- Attack path analysis with guided remediation in CIEM
- Wide deployment and licensing flexibility
- Strong regional presence in Latin America
- Recognition by analyst firms for usability and customer support

Challenges

- Limited integrations beyond PAM-related toolsets
- Recent rebranding may cause market confusion
- No automated incident analysis or correlation of events
- No case assembly of incident data for analysts
- Missing rollback options for automated remediation

Semperis – Active Directory Threat Detection and Response



Semperis, founded in 2015 and headquartered in Hoboken, New Jersey, has established itself as a specialist in Active Directory (AD) and identity system security. Its product portfolio includes Active Directory Forest Recovery (ADFR), Directory Services Protector (DSP), DSP Identity Runtime Protection, Disaster Recovery for Entra Tenant (DRET), Delegation Manager for AD, Lightning Intelligence, and Ready1. The company focuses on identity system resilience and recovery, with licensing models based on per-user/identity subscriptions for SaaS offerings, while professional services are priced on a time-and-materials basis. Deployment options cover on-premises, private and public cloud, and hybrid scenarios, with delivery as SaaS, virtual appliance, or containerized models. Semperis primarily serves mid-market and large enterprises across North America, with increasing presence in EMEA, APAC, and early adoption in Latin America. Compliance with ISO/IEC 27001, HIPAA/HITRUST, and SOC 2 Type 2 underlines its enterprise security posture.

Semperis' core capabilities address the entire identity threat lifecycle. The DSP platform delivers continuous posture assessment for AD and Entra ID, detecting misconfigurations and reducing attack surfaces. AI-powered ITDR capabilities provide anomaly detection, behavioral analytics, and attack path analysis with customizable scoring models, uncovering credential misuse, privilege escalation, and lateral movement. For response, Semperis supports 12 playbooks that can be customized via coding or templates, though the platform does not yet recommend specific playbooks automatically. Automated prevention and

response actions include disabling accounts, reducing privileges, isolating endpoints, or denying access. Its recovery capabilities stand out with automated forest-level restore for AD and post-breach forensics that remove attacker persistence. Parallel restore functions enable recovery without disrupting ongoing operations. Additionally, the Semperis Identity Forensics & Incident Response (IFIR) team provides hands-on support during and after breaches, combining deep expertise in identity systems with methodologies for containment, eradication, and recovery. The solution also identifies attack methods such as golden and silver ticket attacks, DCSync, DCShadow, pass-the-hash, and Kerberos-based exploits.

The integration of attack surface reduction, detection, forensics, and recovery in one platform provides a unique value proposition for enterprises that depend heavily on AD. While the product offers strong Active Directory integration, its support for non-AD cloud identity systems remains less comprehensive, which may limit its applicability in hybrid and cloud-native environments. That said, support for Okta has expanded significantly over the past year, including the introduction of Okta-specific security indicators in the Purple Knight tool. However, GenAI features are currently limited. Also, Semperis does not provide credential intelligence, as its core business is protection and recovery of AD and Entra ID. These constraints aside, Semperis demonstrates innovation in combining prevention, recovery, and identity forensics into a single platform designed for critical enterprise environments.

Semperis focuses on end-to-end identity crisis management, from tabletop exercises to real-world incident response. Organizations with complex hybrid environments will find strong support for AD security hardening, identity forensics, and cyber resilience planning. Its services appeal to security teams that require expert-guided incident response and rapid recovery of identity infrastructure. North America remains the company’s strongest region, but its growth in EMEA and APAC indicates increasing global traction. Enterprises seeking cyber crisis management specifically tied to identity and AD should evaluate Semperis, particularly where stringent regulatory and operational continuity requirements demand mature disaster recovery and forensic capabilities.

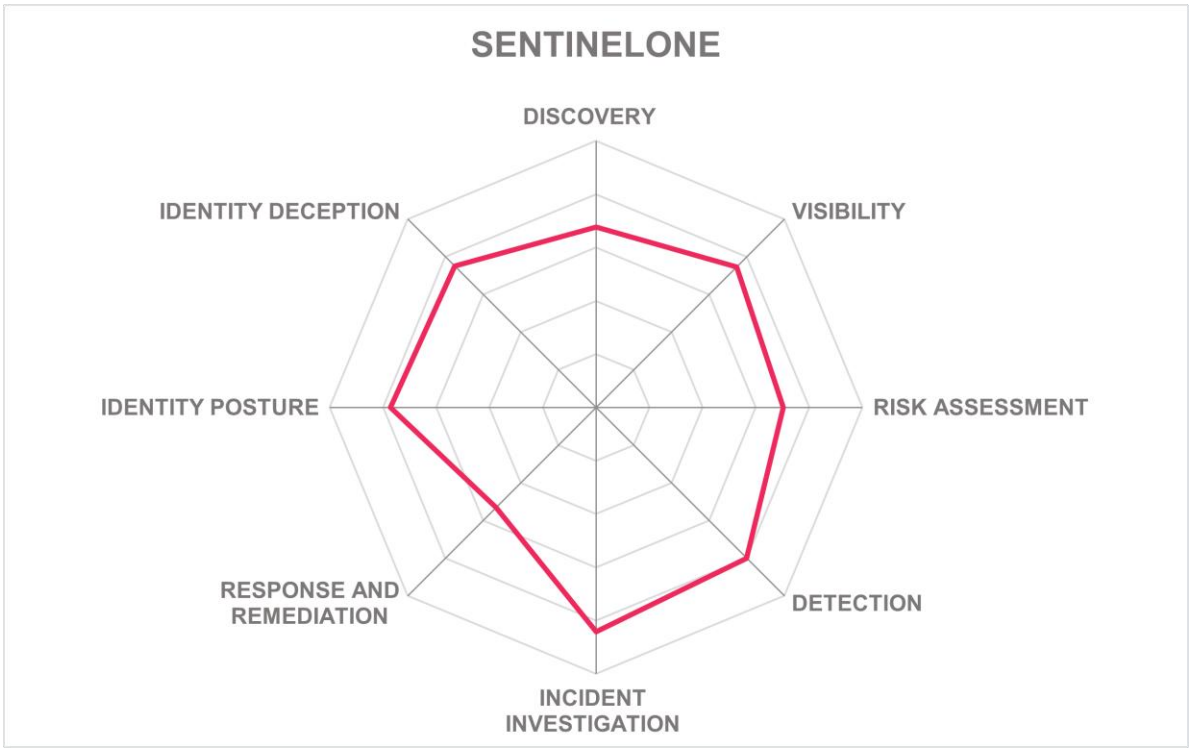
Strengths

- Strong specialization in Active Directory protection
- Advanced automated disaster recovery for AD environments
- Parallel restore and post-breach forensics capabilities
- Broad SIEM and ITSM integration support
- Comprehensive cyber crisis management and remediation services
- Attack surface reduction for AD and Entra ID

Challenges

- Limited GenAI capabilities for ITDR functions, but improvements are on the roadmap
- Lack of interoperability with PAM tools
- No automated correlation of relevant events for incident analysis
- Narrow coverage of non-AD identity systems
- No graphical visualization and configuration of risk evaluation policies for admins

SentinelOne – Singularity Identity



Leader in

SentinelOne was founded in 2013 and is based in Mountain View, California. Its flagship Singularity Platform covers protection for endpoints, cloud workloads, and identity infrastructures, priced by per-user, per-node, and per-server licensing models. The company primarily serves North America, with a growing presence in EMEA, APAC, and Latin America. SentinelOne holds certifications including ISO/IEC 27001, HIPAA/HITRUST, US FedRAMP, and others, reflecting its alignment with regulated industries such as healthcare, government, and financial services. API authentication methods supported include OAuth2, SAML, and JWT. Its ITDR product, Singularity Identity Security, specifically addresses identity threats with detection, response, and remediation capabilities for both on premises Active Directory and cloud identity providers including Entra ID, Okta, Ping Identity, Duo, and SecureAuth.

Singularity Identity Security operates as an integrated module within the Singularity Platform, delivering real-time identity protection and attack disruption. The product combines posture management with identity-focused detection, allowing enterprises to continuously assess and remediate misconfigurations, vulnerabilities, and excessive entitlements across AD and

cloud identity providers. Deception-based techniques are a defining feature, using decoy users, groups, and credentials to identify reconnaissance activities and active attacks, ensuring early detection of malicious behavior. The platform also identifies well-known AD attack methods such as golden and silver ticket attacks, DCSync, DCShadow, pass-the-hash, and Kerberos-based exploits. Its Singularity Data Lake enables long-term data storage and rapid query performance, providing defenders with contextual correlation and investigation tools. Integration is extensive, with REST, gRPC, GraphQL, WebSockets, and SOAP APIs supported, as well as connections to SOAR, SIEM, ITSM, and XDR platforms through the Singularity Marketplace. The integration of Purple AI, SentinelOne's LLM-powered SecOps assistant, is a notable platform-level differentiator. It enhances the overall threat hunting, investigation, and response experience across the platform through natural language queries.

SentinelOne's approach to ITDR reflects a broader market trend (by EPDR and XDR vendors) toward fusing endpoint, identity, and cloud defense into a single operational framework. Anchored in the same data lake and detection fabric as SentinelOne's EDR and XDR components, Singularity Identity Security delivers unified visibility through a single agent and console. Correlated alerts and shared context across endpoint and identity layers enable faster threat investigation and streamlined response. Overall, the platform combines strong technical capabilities with innovative detection methods that differentiate it in the ITDR market.

Organizations with complex Active Directory and cloud identity deployments, particularly those in regulated sectors such as finance, healthcare, and government, will find Singularity Identity Security's blend of posture management and deception-based detection particularly relevant. The product is well-suited for security operations teams looking to unify endpoint, cloud, and identity defense within a single platform and benefit from advanced AI-assisted investigation tools. Enterprises seeking to reduce identity-related risk exposure, gain continuous monitoring of AD and cloud identity providers, and integrate identity defense with broader SOC workflows will find SentinelOne's ITDR approach highly applicable to their use cases.

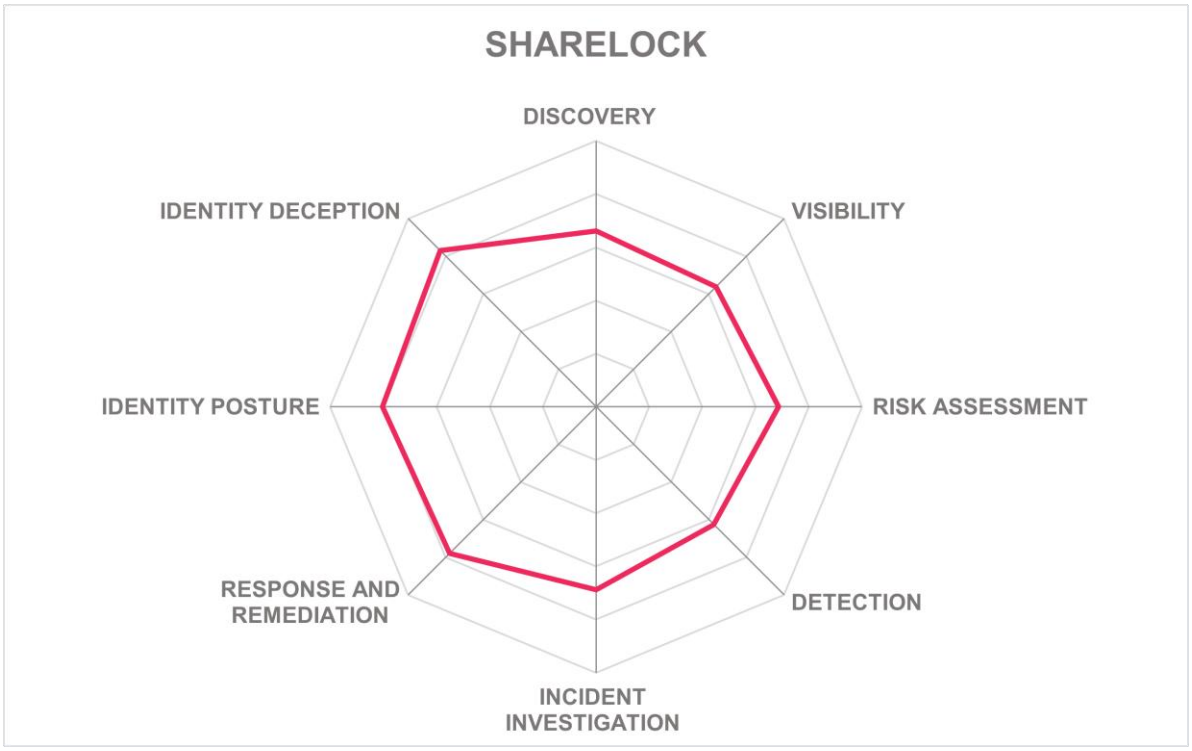
Strengths

- Strong deception-based identity protections
- Extensive Active Directory and cloud identity providers coverage
- Integration with SIEM, SOAR, XDR, and ITSM platforms
- Singularity Data Lake with long-term query performance
- Broad API protocol support for integrations
- Prescriptive posture management with remediation rollback
- Compliance with multiple major security standards

Challenges

- Limited community-driven development resources
- Potential complexity for smaller organizations
- May be less appealing to organizations less dependent on Microsoft

Sharelock – Sharelock Identity Security Platform



Leader in

Sharelock, founded in 2019 and headquartered in Rome, Italy, delivers its Identity Security Platform. The platform unifies ITDR and ISPM in a native solution. It is designed for medium, mid-market, and large enterprises and is offered through flexible licensing. For on-premises deployments, it is user-based, and for SaaS it is user-plus-application. Deployment models include public or private cloud, on-premises, and hybrid environments, with delivery available as SaaS, container-based, or managed service. The platform is ISO/IEC 27001 compliant and supports API authentication methods such as OAuth2, OIDC, and SAML, while integration is facilitated through REST and Webhooks.

The solution integrates with Microsoft, Okta, and One Identity. It establishes continuous discovery and visibility by centralizing identity and entitlement data in an internal SIEM (Elasticsearch) and a specialized graph database (ArangoDB). Behavioral anomaly detection extends to post-authentication activity on endpoint systems, monitoring fine-grained actions such as SAP TCODE usage across users, machines, and applications. Baselines are dynamically established using AI-based analysis. Detection techniques map anomalies to MITRE ATT&CK and flag threats including privilege escalation, insider misuse,

and lateral movement. Automated posture management eliminates ghost and orphaned accounts, enforces least privilege, and audits MFA adoption. Automated posture management eliminates ghost and orphaned accounts, enforcing least privilege principles, and conducting MFA adoption audits through intelligent policy recommendations. Response and remediation are handled through out-of-the-box playbooks as well as customizable workflows orchestrated by Agentic AI agents, including the Security Investigation Autopilot (SIA) that reconstructs incident timelines and generates contextual remediation steps. This system executes forensic investigations across integrated environments and performs multi-signal correlations via over 20 ML algorithms. The platform's Domain-Specific Language Models (DSLM) enable natural language policy descriptions and intelligent service account recognition. Integration options span SIEM/SOAR (Splunk, QRadar, Azure Sentinel), One Identity for PAM, and ITSM platforms like JIRA.

Sharelock differentiates itself through its use of Agentic AI, an automation framework that eliminates the need for manual queries by enabling autonomous AI agents to investigate anomalies, enforce posture, and perform remediation. This GenAI-driven platform not only automates routine security hygiene but also adapts over time through operator feedback and contextual learning. While the platform is feature-rich, challenges remain. Sharelock does not provide native credential intelligence, instead depending on integrations for exposure monitoring. The solution is relatively young compared to long-established competitors, which may affect global presence. However, the company is innovative and has therefore potential for growth.

Sharelock’s customer base centers on enterprises in Europe across industries with high demands for compliance, risk management, and scalable identity protection. Use cases where Sharelock is particularly strong include continuous posture assessment, detecting anomalous activity across both users and machines, automating investigation and remediation of identity-related threats, and maintaining integrity of administrative logs for compliance. Enterprises with limited analyst capacity or those looking to reduce manual investigation burdens will find Sharelock’s Agentic AI platform especially relevant. As European organizations expand their ITDR strategies, Sharelock provides a distinctive option for those prioritizing advanced automation and unified identity security operations.

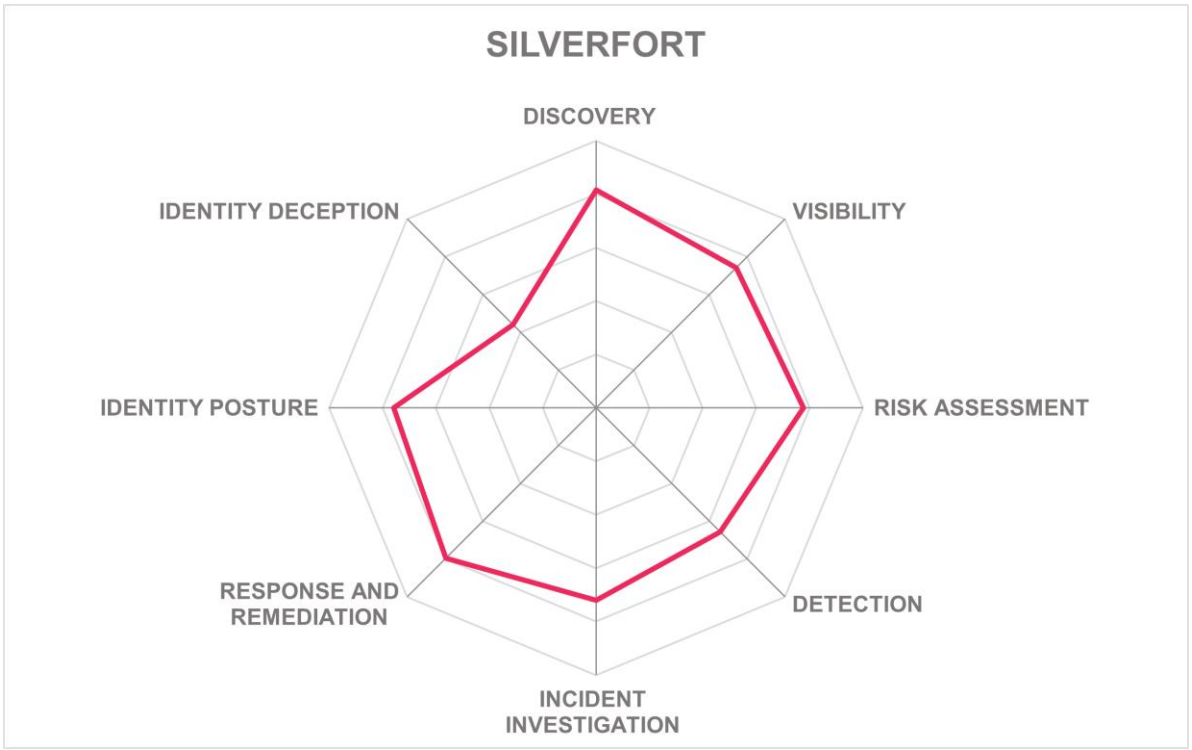
Strengths

- Unified ITDR and ISPM in a single platform
- Agentic AI enables autonomous investigations and remediation
- Strong coverage for human and non-human entity behavior
- Centralized data in internal SIEM and graph database
- Out-of-the-box playbooks with customizable workflows
- Integrations with IAM, PAM, SIEM, SOAR, and ITSM
- Scalable architecture supporting millions of identities
- Immutable logging with tamper protection for compliance

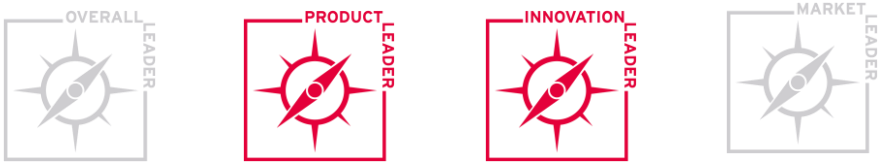
Challenges

- A small partner ecosystem
- Lack of access path visualization and mapping of identities
- Heavy reliance on autonomous AI adoption

Silverfort – Silverfort ITDR



Leader in



Silverfort, founded in 2016 and headquartered in Tel Aviv, Israel, delivers an ITDR platform designed to address identity-based threats across on-premises, cloud, and hybrid environments. Its solution, Silverfort ITDR, operates without requiring changes to existing servers or the deployment of endpoint agents, easing implementation across diverse infrastructures. Licensing follows a per-user model, and the company maintains compliance with standards such as FIPS 140-2, NIST 800-57, ISO/IEC 27001, and SOC 2 Type 2. Silverfort integrates into existing IAM infrastructures including Active Directory, Azure AD, and SAML-based IdPs. With customers spanning finance, healthcare, manufacturing, government, and media, the company has established a global footprint across North America, EMEA, and APAC, and is expanding into Latin America. In November 2024, Silverfort strengthened its offering by acquiring Rezonate, extending coverage into cloud workloads, applications, and infrastructure.

Silverfort's ITDR solution centers on its patented Runtime Access Protection (RAP), which intercepts and analyzes every authentication request from human IDs and NHIs. RAP integrates with existing IAM systems and enforces inline controls to detect and prevent malicious activity without disrupting legitimate access. The solution can identify tactics such as lateral movement, Kerberoasting, brute-force attempts, and privilege escalation. It provides deep visibility into shadow identities, dormant accounts, legacy protocols, and other exposures through real-time discovery and credential intelligence. Silverfort applies a customizable risk scoring model, combining severity, impact, and confidence levels, with recent releases weighing suspicious behavior indicators more heavily than static posture metrics. The policy engine enables organizations to enforce MFA, block risky access, or escalate authentication dynamically. Through integrations with SIEM, SOAR, XDR, IGA, PAM, and ITSM systems, Silverfort extends response actions to external workflows, sharing telemetry and triggering automated remediation. Together with Rezonate's ISPM and NHI security, the platform delivers discovery, detection, prevention, and remediation within a single environment.

Its ability to enforce inline policies without modifying existing systems or relying on endpoint agents is a notable differentiator. Another strength is the flexible and granular policy framework that adapts to real-time risk context. However, some challenges remain: native playbooks for incident response are not supported, placing reliance on integrations with SOAR or SIEM tools for automation. Similarly, dashboards cannot be customized. Despite these considerations, the platform demonstrates strong innovation and strategic positioning in ITDR.

Silverfort's solution is well-suited for enterprises that require identity security across complex hybrid infrastructures, particularly in regulated industries. Its partnership-driven approach with other security vendors, including integrating deeply with XDR and other identity security solutions, strengthens its competitive position in the ITDR market. Typical use cases include discovery and remediation of hidden identities, enforcing MFA and conditional access across diverse environments, and detecting anomalous authentication patterns that suggest compromise. Silverfort is particularly relevant for organizations seeking a single platform to consolidate ITDR, ISPM, and NHI security capabilities with strong integration into existing IAM and security operations tools.

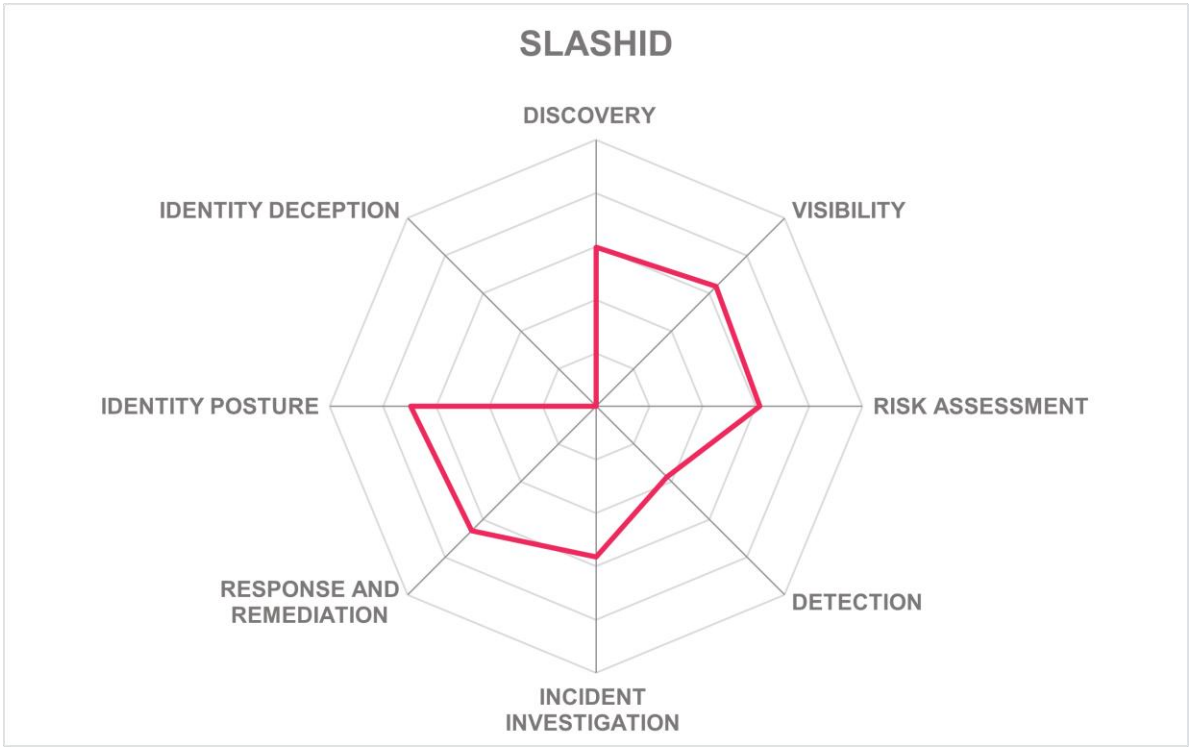
Strengths

- Inline enforcement without endpoint agents
- Patented Runtime Access Protection technology
- Broad coverage of legacy and critical systems
- Deep integration with IAM, SIEM, SOAR, and ITSM
- Flexible, granular, and customizable policy engine
- Risk scoring model adaptable to organizations
- Expanded scope via Rezonate acquisition
- Strong compliance with global security standards

Challenges

- No native incident response playbooks
- No customizable widget-based dashboards, but the solution integrates with SIEM and SOAR tools to provide real-time data feeds for customer's existing dashboards

SlashID – SlashID Identity Protection



SlashID, founded in 2022 and headquartered in New York, is a young but ambitious provider of identity security solutions. Its Identity Security platform is designed to bring visibility, posture management, threat detection, and remediation capabilities across both human and NHIs. Delivered as a SaaS offering in the public cloud, SlashID supports per-connector and per-user licensing. SlashID's regional focus spans North America, EMEA, and APAC, addressing identity threats for organizations of all sizes. The company emphasizes industries with stringent identity and compliance demands, including finance, insurance, healthcare, and government. While SOC 2 Type 2 certified, they have not yet obtained ISO 27001 certification.

The platform provides broad ITDR capabilities that include identity discovery, risk scoring, detection, and automated response. Its cross-environment visibility extends to cloud services and on-premises environments through connectors and a virtual appliance for on-premises data sources. The platform monitors unauthorized access, privilege escalations, and lateral movements, while detecting and preventing shadow applications and phishing through a browser extension. Risk scores combine severity of detected issues and potential blast radius, with policies configurable to reflect organizational risk tolerance. SlashID's platform is equipped for in-depth incident analysis, providing insights into identity events using historical data, which aids in detection and response. Response capabilities range from manual

actions via the UI to automated workflows through SOAR integrations such as ServiceNow and Tines. SIEM compatibility is supported via OCSF, while ITSM systems like JIRA and ServiceNow are covered. Playbook options include privilege reduction, account disabling, session termination, and re-authentication triggers. Integrations with IGA and PAM solutions support access reviews and privileged identity oversight, while LLM-powered incident summaries enhance investigations.

SlashID offers capabilities that extend beyond typical ITDR functions. Its browser extension for phishing and unmanaged app detection provides visibility, detection, and prevention capabilities that are not commonly available in other ITDR tools. SlashID provides a fine-grained access graph that can be queried in plain English through an LLM interface, making investigation, GRC tasks and posture monitoring significantly easier. Additionally, its blast radius analysis aids in understanding the potential impact of identity breaches, providing essential forensic details. However, as a relatively new vendor, SlashID faces challenges in breadth of integrations, currently limited to SailPoint for IGA and CyberArk for PAM product, with no support for access management tools. Dashboards remain non-customizable. Current integration with other security solutions remains limited, although further expansion is planned.

SlashID is relevant for organizations that must secure both human and NHIs in environments where traditional controls fall short. Enterprises looking for ITDR with novel detection methods, identity risk scoring, and lightweight SaaS delivery should evaluate SlashID, especially where ease of investigation and phishing detection at the browser level are pressing requirements.

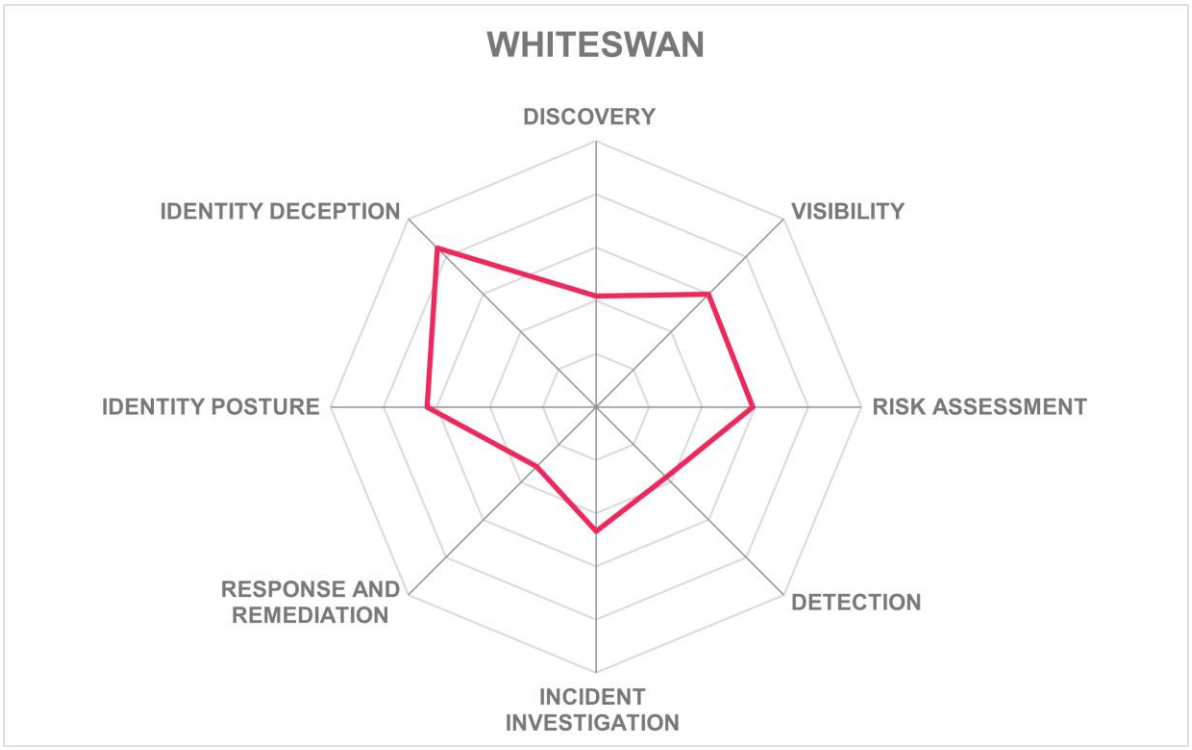
Strengths

- Coverage across human and NHIs
- Browser extension for phishing, URL filtering, and shadow app detection
- Customizable policy framework and risk scoring
- Natural-language queries for investigations, GRC, and governance
- Visibility across cloud, on-prem, and shadow IT environments
- Automated remediation capabilities minimizing manual intervention
- Strong focus on serving both IT security and governance requirements
- Generative AI support for policies and configurations
- Flexible integration with multiple cloud services and identity providers
- LLM-powered identity summaries for investigations

Challenges

- Dashboards are not customizable
- Missing integrations with access management tools and others
- Small partner ecosystem
- Limited market presence due to startup nature and emerging status

Whiteswan Identity Security – Whiteswan ITDR



Whiteswan, established in 2023 and headquartered in San Mateo, California, delivers an ITDR platform designed for organizations experiencing operational fatigue from managing multiple point solutions to defend against identity-centric threats. Its product, Whiteswan ITDR, is available through per user, per server, and per time period licensing, with deployment across on premises, private and public cloud, SaaS, container-based delivery, or managed service. The company primarily serves mid-market organizations in APAC, while expanding its reach into North America and EMEA. Supported environments span Windows, Mac, Linux, and major cloud platforms such as AWS, Azure, and GCP. While offering a wide range of deployment options, the platform has not yet been certified against SOC 2 Type 2 or ISO/IEC 27001.

The solution provides multi-environment coverage with Windows and Linux agents capable of exposing hidden accounts, unauthorized cron jobs, and fileless insider activity. Whiteswan has introduced capabilities for Linux ITDR by piecing together hidden and fragmented identities from system files. Its deception techniques include decoy service accounts, lures deployed at the endpoint level, and mimicry technologies designed to trap attackers. User activities are continuously monitored with a risk engine that applies UBA techniques to evaluate attributes like IP, geo-location, velocity, and device type. The platform extends visibility across identities, attack paths, and potential vulnerabilities, and it supports forensic analysis to aid investigation and refine policies. Response capabilities include automated

actions such as session termination and access revocation to contain threats, though native playbooks are not yet included. Integration support covers Microsoft Sentinel and Splunk for SIEM, ServiceNow for ITSM, and Microsoft/Okta for access management, but it lacks PAM connectivity and SOAR integrations.

Whiteswan differentiates itself with strong Linux-focused ITDR, granular enforcement of MFA, and Deep Active Directory ITDR with deception-driven detection. Its capabilities for uncovering hidden Linux identities and providing TPM-based just-in-time access address areas that are less frequently covered by vendors focusing mainly on Windows or broader identity infrastructure. However, challenges remain: the absence of credential intelligence, gaps in compliance certifications, and missing SOAR and PAM integrations limit the product's reach. The lack of playbook-driven orchestration also constrains response automation. Overall, Whiteswan shows innovation in Linux ITDR and contextual risk modeling but would benefit from expanding integrations and compliance coverage.

The platform is well suited for mid-sized organizations that need visibility across Windows, Linux, and multi-cloud infrastructures, particularly those with Linux-heavy environments where hidden accounts and privileged misuse are common concerns. Its use of deception techniques, behavioral analytics, and contextual risk scoring is valuable for organizations prioritizing detection and investigation while seeking selective automated containment actions. Enterprises with diverse infrastructures may also consider Whiteswan for evaluation, especially when Linux identity protection and granular activity controls are key requirements.

Strengths

- Strong Linux ITDR capabilities
- Flexible licensing options
- TPM-based just-in-time access
- Deception-driven detection techniques
- Granular MFA for activity control
- Behavioral analytics with baseline deviation detection
- Real-time risk scoring for high-risk activities
- Broad deployment options, including SaaS and managed service

Challenges

- No credential intelligence support
- Limited native playbooks for orchestration
- Lack of SOAR integrations
- Missing PAM and IGA connectivity
- No SOC 2 Type 2 or ISO 27001 compliance

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 Security

Astrix Security was founded in 2021 and has its headquarters in New York, United States. Astrix is a cybersecurity company specializing in Non-Human ITDR, focusing on assets like API keys, OAuth apps, service accounts, and AI agents that traditional IAM, SIEM, and XDR tools fail to govern.

Why worth watching: Its platform uses ML-driven anomaly detection and behavioral analysis to uncover secret leaks, vendor breaches, and AI misuse, while automating remediation with guided investigations, credential rotation, and policy enforcement.

Gurucul

Gurucul, established in 2010, is a leading provider in security analytics and operational technology. Headquartered in El Segundo, California, Gurucul has established itself as a notable behavioral analytics vendor.

Why worth watching: The company takes a unique approach to the identity market, in that its product line is a blend of solutions that other vendors provide in discrete packages. Gurucul's approach is to offer an "identity and access analytics platform" that provides SIEM, UEBA, XDR, SOAR, and identity analytics with elements of PAM and IGA.

Oasis Security

Oasis Security was founded in 2022, and it is headquartered in New York, U.S. The company focuses on ITDR for NHIs. It uses proprietary technology to create behavioral profiles of NHIs, continuously monitoring authentication activity to detect anomalies and match them against known threat patterns.

Why worth watching: The platform provides organizations with real-time visibility, guided remediation, and preventive security controls, helping them investigate incidents quickly, reduce exposure to future attacks, and strengthen defenses against the growing wave of NHI-related threats.

Securonix

Established in 2009, Securonix is based in Plano, Texas. The company's flagship product is Unified Defense SIEM. But even with this focus, the product offers strong ITDR capabilities.

It is a comprehensive solution designed to cater to security information and event management needs with a “collect-detect-respond-contain" approach.

Why worth watching: The platform’s risk scoring features are well featured. Its behavioral monitoring covers both personal and entity accounts; every violation is given a risk score and attributed to the account. Threat modeling features enable security analysts to build kill chain workflows for cutting off or escalating an event.

Zscaler

Zscaler was founded in 2007, and it is based in San Jose, California. The company offers a cloud-based platform for Internet security, compliance, advanced threat protection, and other information security services. It provides a Zero Trust Platform that provides security as a service that reduces the need for specialized on-premises security tools.

Why worth watching: With its large footprint in security, Zscaler can play an important role in any ITDR solution.

Related Research

Leadership Compass: Identity Threat Detection and Response (ITDR) 2024
Leadership Compass: Cloud Security Posture Management.
Webinar: Cloud Security in the Age of Generative AI
Leadership Compass: Container Security
Leadership Compass: SASE Integration Suites
Advisory Note: Security Organization Governance and the Cloud
Advisory Note: Cloud Services and Security
Blog: Cloud Security Alphabet Soup

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..