

Identity Threat Detection and Response (ITDR) 2024: IAM Meets the SOC

Mike Neuenschwander

April 22, 2024

The nascent identity threat detection and response (ITDR) market is gaining tremendous momentum in 2024. Cisco and Delinea recently jumped into the market with their recent acquisitions of Oort and Authomize, respectively. Top cybersecurity companies BeyondTrust, CrowdStrike, and SentinelOne continue to make substantial investments in ITDR. Microsoft has leaned into ITDR by blending technologies from its Entra and Defender XDR products. Other vendors, such as Gurukul, Securonix, and Sharelock are attempting to broaden the definition of ITDR in various ways.

Given these developments, the market remains difficult to quantify. Arguably, there isn't even a real "ITDR market," because it's ultimately more like an activity or an identity protection platform. Many of these vendors don't even use the term ITDR in their products' names. But what is clear is that ITDR is a banner under which enterprise identity and access management (IAM) and security operations center (SOC) teams must unite.

So, what's your organization's best route to protecting identities and IAM infrastructure? This Leadership Compass evaluates the market dynamics for ITDR in 2024 and provides guidance on how your organization can take advantage of these critical technologies.

Contents

Executive Summary	4
Key Findings	4
Market Analysis	4
Market Size and Segmentation	9
Delivery Models	10
Required Capabilities	11
Leadership	12
Overall Leadership	13
Product Leadership	14
Innovation Leadership	15
Market Leadership	17
Products and Vendors at a Glance	19
Product/Vendor evaluation	20
Spider Graphs.....	20
BeyondTrust – BeyondTrust Platform	21
CrowdStrike – Falcon® Identity Protection	24
Delinea – Authomize Platform	27
Gurukul – Gurukul Platform	30
Microsoft – Entra ID + Defender XDR	33

Securonix – Securonix Platform	36
SentinelOne – Singularity Identity	39
Sharelock – Identity Security Platform	42
Vendors to Watch	45
Related Research	47
Copyright	47

Executive Summary

Identity Threat Detection and Response (ITDR) is a class of security solutions designed to proactively detect, investigate, and respond to identity-related threats and vulnerabilities in an organization's IT environment. ITDR solutions focus on protecting digital identities and infrastructure against a variety of attacks by threat actors.

ITDR is a crucial component of a comprehensive cybersecurity strategy, as identities have become the primary targets of attackers looking to gain unauthorized access to sensitive systems and information. By focusing on the security of identities, ITDR helps organizations protect against a range of threats, including credential theft, account takeovers, and insider threats.

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

In our research on ITDR, we found the following:

- The total market size of ITDR (including revenue, services, labor, fines, lawsuits, ransom payments, etc.) was in excess of \$2.4 billion in 2023, with very strong growth in 2024.
- ITDR is a use case, not a product and will likely be called by another name by 2025. In this report we propose “identity defense-in-depth” (IDID), but the market will eventually decide.
- 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.
- BeyondTrust, CrowdStrike, Microsoft, Securonix, and SentinelOne are market leaders, joined by Gurukul in product leadership.
- Consolidation has heated up in the ITDR market, with Cisco acquiring Oort and Delinea acquiring Authomize.
- 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

As the name suggests, ITDR takes its meaning from established security systems, such as EDR, XDR—well, and pretty much anything ending in a “DR” these days. It is certainly

comforting to believe that for any new attack surface we encounter we just simply douse some “DR” on it and suddenly we can go back to being safe. But in reality, it is an admission that any detection and response market—including the ITDR market—is a creation of threat actors, not of the cybersecurity industry.

But now that identity systems have themselves become the targets, things have become complex. No longer are we discussing endpoints, servers, networks, and firewalls; identities do not behave in these same ways. Identities are not a physical place or even a manageable thing. You cannot shut down a port of an identity; you cannot just run a virus scanner on it. The threat actors have finally found a door into the organization you cannot just close—the front door.

The insidious nature of identity-based attacks is that the attacker can parade around your infrastructure using legitimate, highly trusted levels of authentication and encryption to commit crimes without any fear of being noticed. They’re not the proverbial wolf in sheep’s clothing—they manipulate the sheep, instead.

This dynamic is completely uprooting our current models for threat detection and response. To deal with this type of threat, a new runbook must be written. As an industry, we’re still very early on in that process; but for the moment, we’re cautiously referring to this new practice as ITDR.

Though a catchy marketing mnemonic, the difficulty with this term “ITDR” is that it doesn’t capture the types of activities organizations must engage in to protect their user accounts and identity systems. None of the vendors in this report even use “ITDR” in the naming of their products: Microsoft uses “Entra ID + Defender for Identity,” CrowdStrike uses “Falcon Identity Protection,” SentinelOne calls their product “Singularity Identity,” while BeyondTrust, Cisco Oort, Delinea Authomize, Gurukul, Securonix, and Sharelock refer to their products as identity platforms. What’s going on here? Can we even refer to “ITDR” as a market?

Departmental Tension

The dilemma that vendors face in the ITDR market is that their products must serve the needs of two previously distinct departments within information security organizations: identity administrators (a function of IT) and the SOC (response team) department. Ransomware attacks have set these departments on a collision course, so ITDR vendors’ main purpose is to create a collaborative environment where IT can focus on visibility and identity posture and the SOC teams can take the lead in threat hunting and response. Suddenly, identity administrators are learning cybersecurity vocabulary and SOC analysts are learning all about IAM—and ITDR vendors aim to satisfy both teams at once.

Straddling these departments’ needs also means figuring out how to split the bill. Think of two large families sharing a meal at a fancy restaurant: who picks up the tab? Well, since it has “DR” at the end of the name, it must be the SOC’s responsibility; but then the SOC team is confused why they’re paying for anything with “identity” on it.

Realizing this, vendors have begun referring to their solutions as identity protection, identity posture, or identity platforms, with ITDR being just one of many use cases their offerings

provide. Likely, the next report we do on this topic will be something closer to “Identity Defense in Depth” (IDID), which has the serendipitous use of two IDs in the acronym—and it’s just plain fun to say out loud as “I DID.”

The ITDR Market in a Technical Framework

Mediating the interaction between teams of differing—and in some cases segregated—duties is no simple task. The technology underlying such a broad set of requirements must be holistic and comprehensive. In pursuit of compliance with NIST Special Publication (SP) 800-207, Zero Trust Architecture, it’s critical that the ITDR system won’t simply also be exploited. The five pillars in the image below illustrate how neither IT administration nor SOC teams have control over the entire process, but that visibility is broadly available.

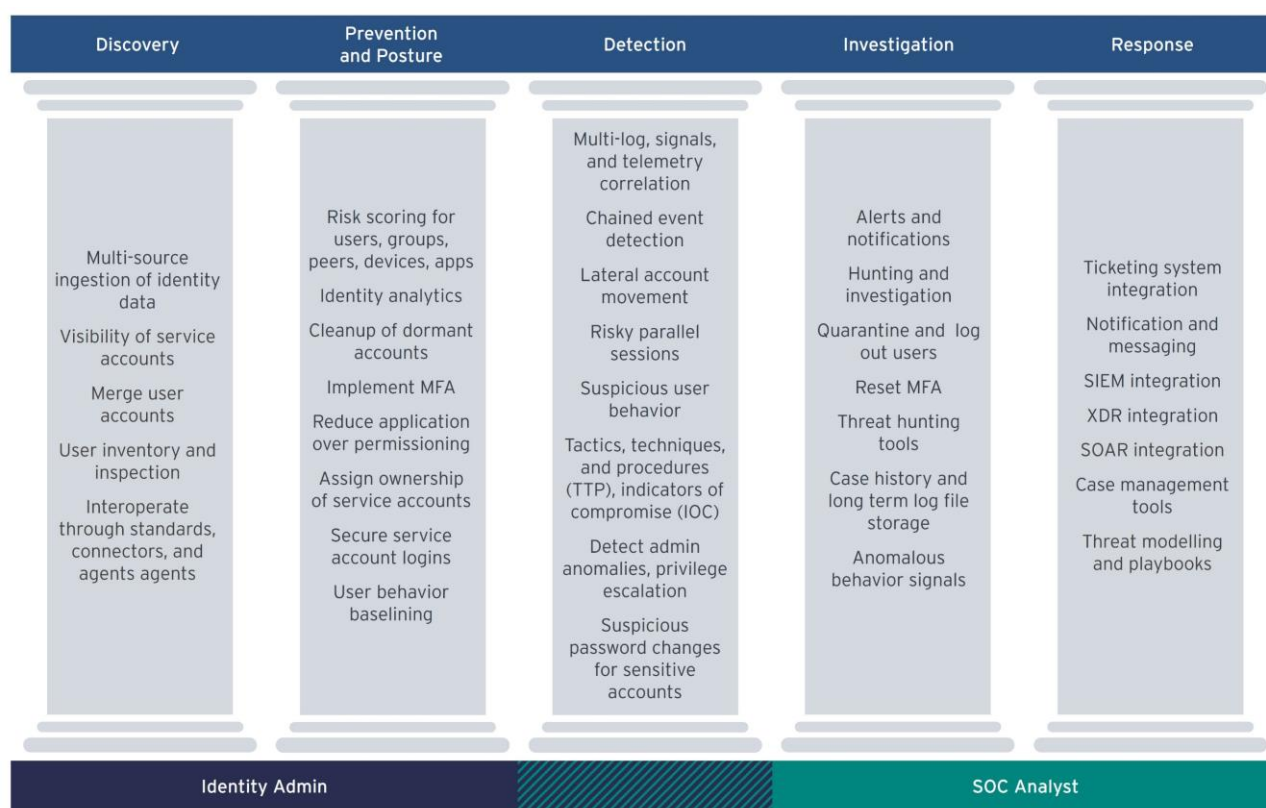


Figure 1: The five pillars of ITDR

These pillars support activities that range from administration of identity systems (on the left) to shared responsibilities in the center, then SOC-related responsibilities to the right. Given that administration and SOC teams need to collaborate through this process, tools that provide integrated views and tools improve the success of ITDR projects.

All vendors we reviewed are strong on administrative features. When integrating with SOC processes the solutions are split between integration with ITSM and SOAR solutions and native support for such tasks. For example, all the solutions we reviewed offer some form of case management. CrowdStrike, Delinea, Gurucul, Microsoft, Securonix, and Sharelock provide integration with SIEM and SOAR solutions. In addition, Gurucul, Microsoft, and Securonix provide integrated SOAR solutions with their ITDR. SentinelOne offers native integration with Microsoft environment, which improves mean time to repair (MTTR) without requiring SIEM or SOAR.

Still, it remains to be seen how enterprise security teams will take to these tools. It's likely SOC teams will want to remain with existing tools choices, but this means the richness of identity management data may not be quick at hand. Cisco Oort and Securonix offer correlated views and enriched log data, which help address the sparseness of identity data in classic SIEM and SOAR systems. Still, threat hunting in identity systems is greatly aided by a rich ITDR solution.

Dashboards and Visualizations

All of the solutions in this Leadership Compass offer similar user experiences in their administrative portals. Generally, this begins with a dashboard that provides an overall status of the identity fabric, an ability to drill into identified risks or events (usually based on specific user accounts affected), and to begin investigations into the nature of the risk or attack.

These administrative portals differ in how many playbooks are available, their use of AI and ML in assisting with discovery and explanations, and their depth of knowledge of identity products. So, selection of an administrative portal relies heavily on the needs of your organization.

ITDR Technical Architecture

To fulfil the requirements mentioned in the section above, the ITDR platform needs to provide certain components, while connecting to existing identity and security infrastructure. The following image illustrates how these components fit together conceptually.

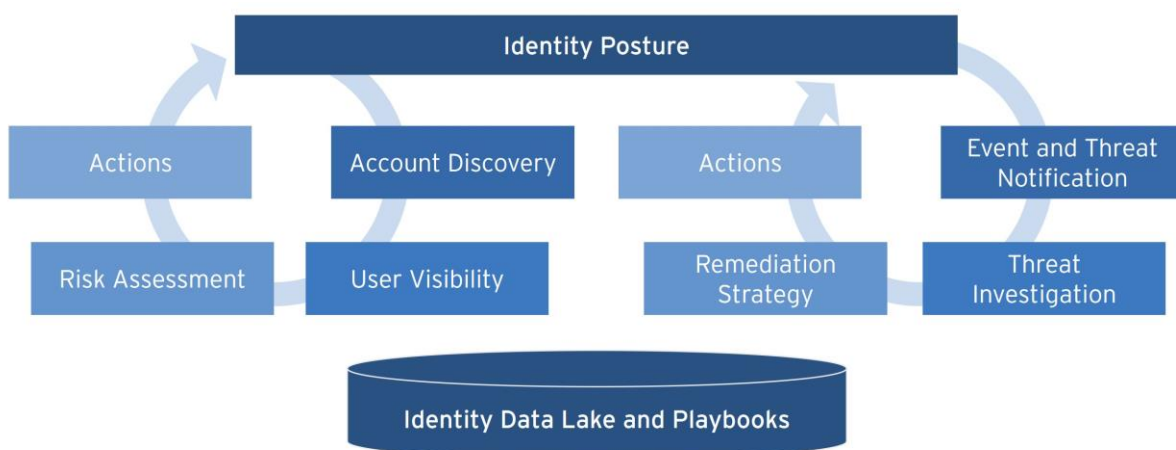


Figure 2: Conceptual architecture for ITDR solutions

ITDR products connect to IAM platforms and capture critical information in a database or data lake. The first step is to review all known accounts, identify their owners, and perform risk assessments on them. This process is repeated over time to ensure the identity posture is maintained. The process also watches for events or threats that arise through log files and (for CrowdStrike, Gurukul, and SentinelOne) network traffic. Once an incident is detected, the ITDR product alerts administrators and security analysts through a variety of channels. All products connect to ServiceNow, but a number of other ticketing services are supported, as well.

Market Size and Segmentation

The total market size for ITDR is trickier to establish than 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. In 2023, the amount of software sales alone in the “greater ITDR” market was about \$3.9 billion. Some fraction of that number is the real ITDR, but it’s clearly at least \$1 billion. A second reason is that this number doesn’t yet take into account the amount being spent on services, labor, lawsuits, fines, ransom payments, and other costs to protect identity systems. This number is easily in excess of \$1 billion. So, we estimate that the total value of the ITDR market in 2024 is in excess of \$2.4 billion.

What is indisputable is that vendors are experiencing phenomenal growth. Many thousands of customers are reaching out for ITDR products and will continue to do so. From our survey, we find that the compound annual growth rate (CAGR) for this market is in excess of 28% - and growing. CrowdStrike (NASDAQ: CRWD), a publicly traded company, illustrates this type of growth. According to their press release, CrowdStrike’s total revenue was \$3.06 billion, a 36% increase for its 2024 fiscal year. Not all of this revenue is directly attributable to ITDR, but it’s certainly indicative. As a result, we project the total ITDR market will approach \$3 Billion in 2025.

The following chart illustrates the growth of ITDR revenue from 2022 to 2026, discounting non-product expenditures such as services, internal costs, and ransom payments.

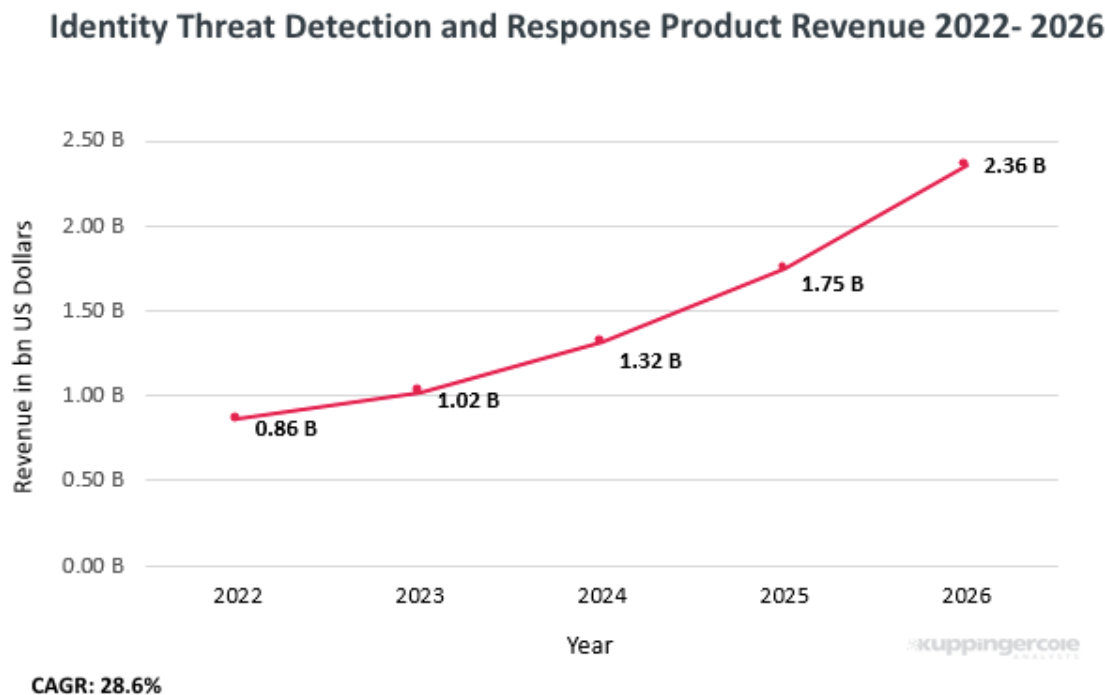


Figure 3: Growth in product revenue in the ITDR market

Delivery Models

Products in the ITDR market vary in the way they provide these components. The following table illustrates the various approaches available on the market today.

Vendor	Deployment	Hosted Environment	Delivery Options	Data Storage	Connector Model
BeyondTrust	SaaS or Pre-packaged virtual appliance	AWS, Azure, Google Cloud	On-prem, IaaS, SaaS	Data lake and Graph DB	API-based
CrowdStrike	SaaS	AWS, CrowdStrike SaaS	SaaS, Falcon Sensor for on-prem	Information not available	Falcon Sensor, Cloud APIs
Delinea Authomize	Kubernetes	AWS, Azure	Hosted SaaS	Database	Agentless / native API
Gurukul	SaaS, Microservices	AWS, Azure, GCP, Oracle, IBM, Private	SaaS, managed SaaS, Hybrid, On-prem	Gurukul SaaS or open choice, data lakes include Hadoop, HDP, CDH, EMR, HDInsight, Snowflake	API, Flat file, agent (Gurukul and 3 rd -party), database (JDBC direct connect), stream
Microsoft	Hosted Service	Azure	Hosted Service	Graph DB	Native, on-prem
Securonix	SaaS	AWS	SaaS	Snowflake / BYO Snowflake	API
SentinelOne	SaaS	AWS	SaaS	Data lake	Entra API, agent
Sharelock	Kubernetes	AWS	Serverless	ArangoDB, Elasticsearch, MongoDB	API

Table 1: Architectures of ITDR products, by vendor

Most enterprises are able to deploy any of these options, but some security teams may have preferences for architecture, cloud options, or deployment models.

Depth vs. Breadth

ITDR solutions vary significantly in their approach to integration. BeyondTrust, CrowdStrike, SentinelOne, and Semperis (included in our “Vendors to Watch” section) provide excellent

security for the Microsoft ecosystem, including Azure Entra ID, AD, and related technologies. These solutions offer large catalogs of known attacks and guidance on how to improve identity posture and how to proceed after a breach of Entra ID or AD.

In addition, BeyondTrust, CrowdStrike, Delinea Authomize, Gurukul, and Securonix collect signals from a wide range of platforms—even beyond the identity infrastructure that ITDR focuses on. These solutions provide broader visibility, but often without the nuance that's required for managing large Microsoft systems. Microsoft and Sharelock are somewhere in between these poles: Microsoft relies on general its purpose systems (Entra ID and Defender for Identity) and Sharelock provides a range of playbooks for various identity systems.

Market Segment—Organization Fit

Currently, in 2024, the ITDR market is fragmented and few of the vendors in this space compete directly with each other. Additionally, nearly all the vendors we report on have large numbers of customers, excellent financials, and quality offerings. The determining factor of which technology to move forward with (and there's really no time to wait) is through finding the best fit for your organization's needs—both now and in the next several years.

Some of the factors to consider when selecting ITDR solutions are:

- **Size of organization**—Large enterprises may have omnibus license arrangements with large vendors like Microsoft and CrowdStrike that limit flexibility in product selection.
- **Microsoft or Multi-cloud**—Enterprises that rely primarily or heavily on Azure and AD should evaluate vendors specialized in those areas, namely BeyondTrust, Gurukul, CrowdStrike, Microsoft, and SentinelOne. Organizations committed to AWS or Google Cloud should look elsewhere.
- **IAM requirements**—ITDR vendors vary widely in their integration with IAM systems. Most integrate with AD and Okta, but not all support Ping Identity, Onedidentity, Broadcom, or other platforms.
- **IGA requirements**—Similarly, ITDR integration with IGA systems is mixed.
- **Hosting requirements**—Organizations may require regional, private cloud, or regulated environments (such as FedRAMP) hosting. ITDR products differ widely on how these requirements are supported.

Required Capabilities

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

- **Platform:** The infrastructure supporting ITDR features and connectivity to IAM and other services.
- **Discovery and Visibility:** Surveying the organization's identity assets by connecting to authoritative systems and linking accounts to the responsible owners. The ITDR solution then provides continuous visibility into the state of the organization's identity assets.

- **Prevention and Posture Management:** Proactively identifies risks to an organization's identities and surfaces them to the administrative team. Also provides decoy accounts that test for intrusion.
- **Detection:** Identifying 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.
- **Investigation:** Analyzing detected activities to understand the scope, method, and impact of a potential identity threat. This involves correlating data from various sources to gain insights into the nature of the threat and identifying the affected systems or data.
- **Response:** Taking appropriate actions to mitigate identified threats and prevent future occurrences. This could involve adjusting security policies, implementing stronger authentication measures, revoking compromised credentials, or deploying patches to address vulnerabilities.

Leadership

The KuppingerCole Leadership Compass provides a comparison based on standardized criteria and can help you identify solutions that are suited to your organization's needs. Naturally, final product selection requires a more rigorous process through a Proof of Concept (PoC) or pilot phase, based on your organization's specific criteria.

The KuppingerCole Leadership Compass is a model that rates products—in this case, ITDR products—according to three leadership categories. These are:

- Product Leadership
- Innovation Leadership
- Market Leadership

Based on these ratings, we offer an Overall Leadership chart, which is an indicator of each vendor's performance for general applicability to the market. We'll begin with Overall leadership and then to the three categories that contribute to this designation.

The products we evaluate in this research are:

- BeyondTrust Platform
- CrowdStrike Falcon Identity Protection
- Delinea Authomize Platform
- Gurukul Platform
- Microsoft Entra + Defender XDR
- Securonix Platform
- SentinelOne Singularity Identity
- Sharelock Identity Protection

Overall Leadership

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 from each other 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.

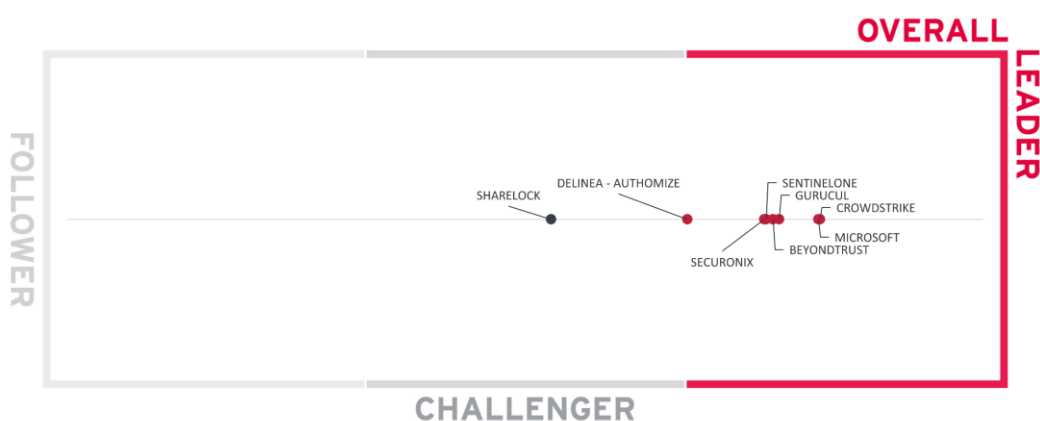


Figure 4: Overall ITDR Leaders

As mentioned above, this section assesses a vendor's overall performance, based on the three product categories described below. In the ITDR market, this is particularly nuanced, because this market hasn't yet coalesced around a well-defined set of features. For that reason, we recommend looking deeper into this report to gain a better understanding of what each of these ITDR solutions provide.

The Overall Leaders in the ITDR market are (in alphabetical order):

- BeyondTrust Platform—Ideal for heterogenous environments with PAM integration
- CrowdStrike Falcon Identity Protection—Excellent choice for Microsoft environments
- Delinea Authomize—Great for quick identity visibility and event detection
- Gurucul—Broad-based identity integration and event detection
- Microsoft Entra + Defender XDR—Organizations using or planning to use Microsoft Defender
- Securonix—Broad-based identity integration and event detection
- SentinelOne Singularity Identity—Excellent choice for Microsoft environments

Product Leadership

Product leadership is the next category examined. This view is based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

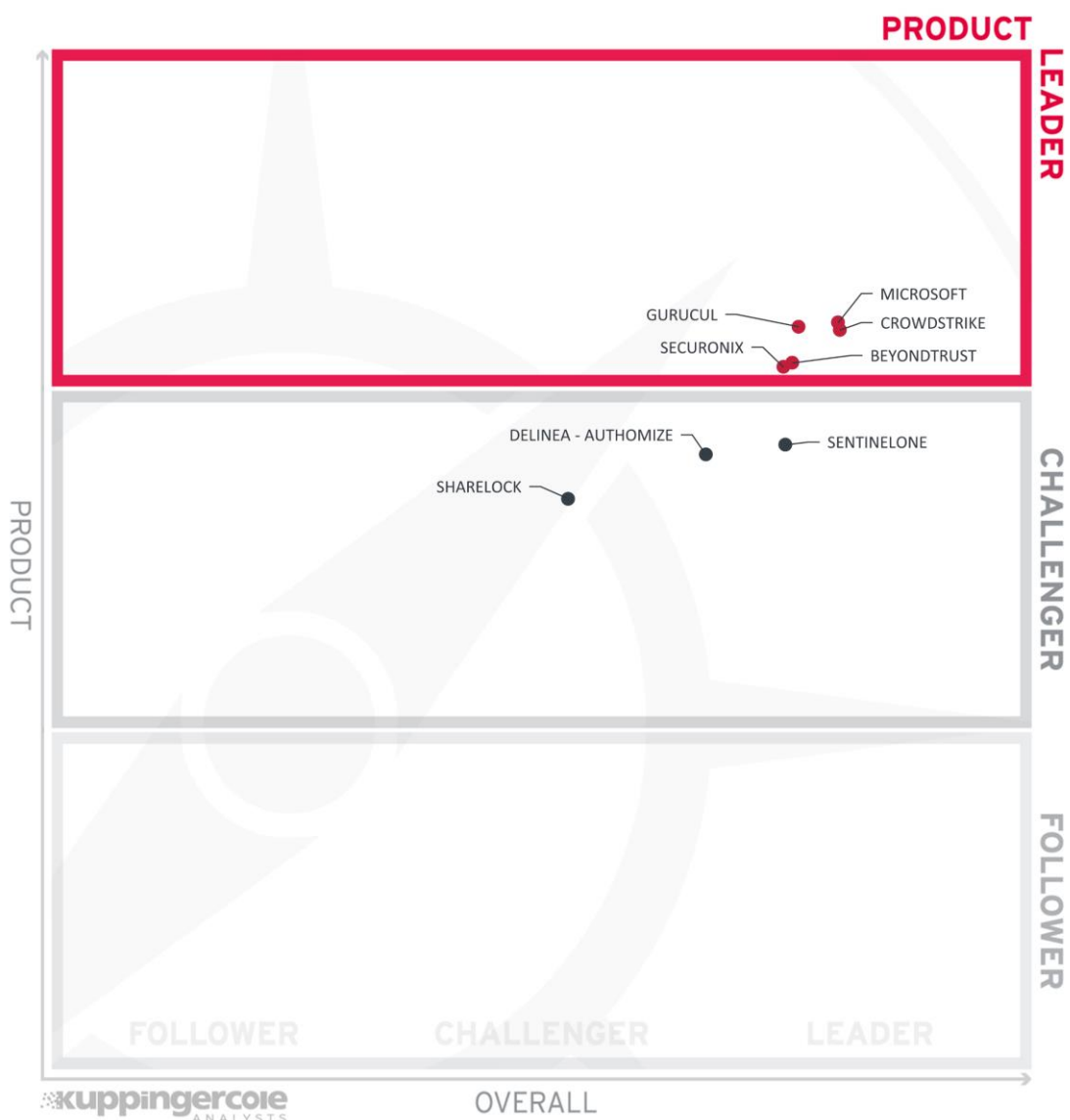


Figure 5: ITDR Product Leaders

Product leaders are ITDR solutions that excel in their forward-leaning technical architecture. Given the diversity of ITDR solutions, product leaders in ITDR tend to lead in particular categories, as described in previous sections. The ITDR solutions are in many ways ahead of their time, but the market is also evolving rapidly, with challengers growing in functionality and business metrics, as well.

The ITDR Product Leaders are (in alphabetical order):

- BeyondTrust
- CrowdStrike
- Microsoft
- Gurukul
- Securonix

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 based on the evaluation of innovative features, services, and technical approaches as defined in the Market Analysis section, above. 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.

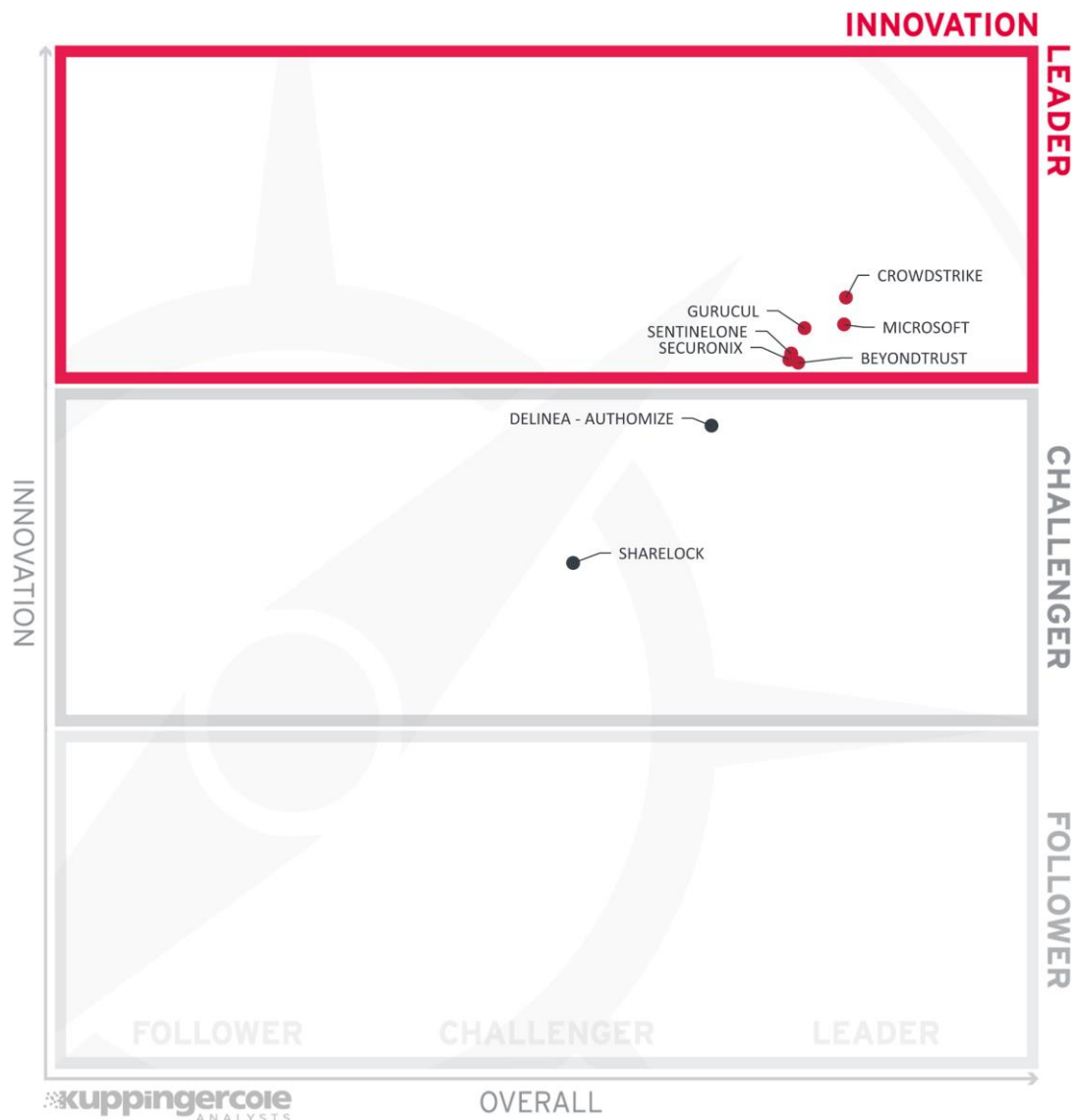


Figure 6: Innovators in ITDR

For many enterprise organizations, innovation is exciting to see, but difficult to justify. With so many legacy applications in tow, it's not easy to move to a cloud-first, avant-garde solution. And yet, innovative vendors are a window into the future. This section identifies the ITDR vendors who have built their architecture around the future.

Innovation Leaders are (in alphabetical order):

- BeyondTrust
- CrowdStrike
- Gurukul
- Microsoft

- Securonix
- SentinelOne

Market Leadership

Finally, we analyze Market Leadership. This is an amalgam of the number of customers, the number of transactions evaluated, the ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and 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.

We base this on factors such as the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies.

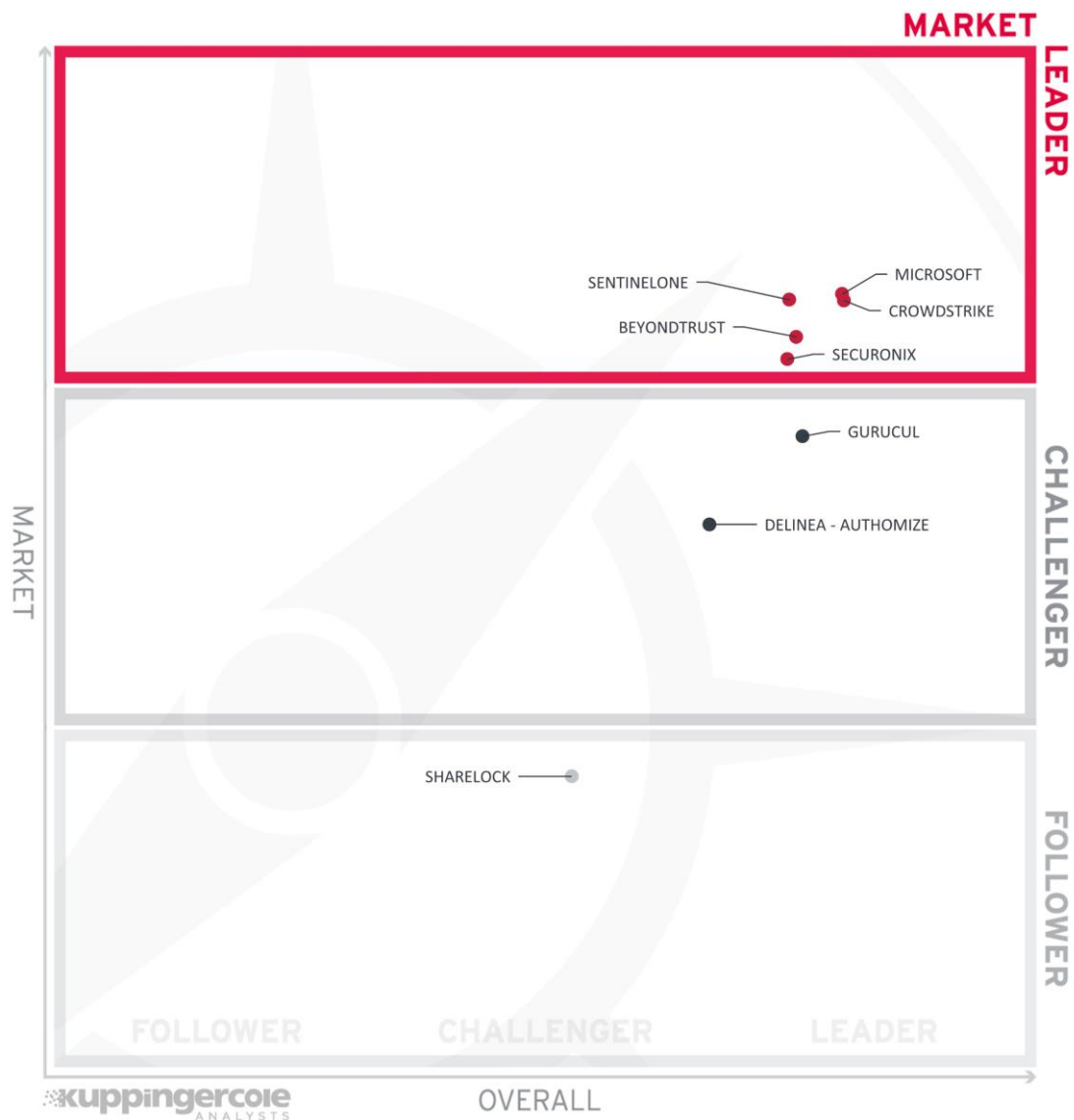


Figure 7: Market leaders in ITDR

The market leaders for ITDR have very strong financials, growth, and pipelines. However, in our research we found that all the ITDR vendors we covered are experiencing very strong customer acquisition and financial growth.

The following vendors are Market Leaders for ITDR (in alphabetical order):

- BeyondTrust
- CrowdStrike
- Microsoft
- SentinelOne
- Securonix

Products and Vendors at a Glance

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

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 2. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
BeyondTrust	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
CrowdStrike	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Delinea Authomize	Strong Positive	Positive	Positive	Positive	Strong Positive
Gurucul	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Securonix	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
SentinelOne	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
Sharelock	Strong Positive	Positive	Positive	Positive	Strong Positive

Table 2: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 3 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
BeyondTrust	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CrowdStrike	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Delinea Authomize	Positive	Neutral	Positive	Neutral
Gurucul	Strong Positive	Positive	Strong Positive	Strong Positive
Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Securonix	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SentinelOne	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Sharelock	Positive	Neutral	Weak	Weak

Table 3: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a review and rating for each product included in this KuppingerCole Leadership Compass. For many of these products, there are additional research reports available, providing more detailed information; you'll find links to much of our research in each vendor's section.

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 don't 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:

- **Account Discovery**—the solution's ability to detect accounts across a variety of platforms, include service accounts and orphaned accounts
- **User Visibility**—tools for inspecting accounts owned by a user or group
- **Risk Assessment**—automated risk scoring, behavioral analysis, and peer analysis to identify excessive privilege; also evaluates weak security (such as lack of MFA) on any accounts
- **Event Detection**—ability to notify of any critical change in risk for an account or alert on any detected attack, threat, or anomaly
- **Incident Investigation**—ability for analysts and administrators to review attacks holistically across platforms and assess risks
- **Remediation**—case management and integration with investigation platforms, identity-centric information on how to stop attacks, documentation for root cause analysis
- **Identity Posture**—tools for maintaining lowest possible risk to protected identity systems
- **Identity Deception**—the ability to deploy and monitor decoy accounts and assets in identity systems

Additionally, we provide a brief overall assessment of the product including our view of its strengths and challenges.

BeyondTrust – BeyondTrust Platform

Established in 2003, BeyondTrust is a privately held company within the Francisco Partners and Clearlake Capital portfolio. With a headquarters in Georgia, USA, BeyondTrust has demonstrated excellent growth of its Identity Security Platform and continues to invest significantly in its technology. BeyondTrust has a worldwide footprint, with a substantial presence in North America and Europe.

The BeyondTrust Platform is much broader than the company's ITDR solution—BeyondTrust also provides services to protect privileged identities, access, and endpoints. Identity Security Insights provides a broad view of an organization's IDM platforms. Password Safe, a Shared Account Password Management (SAPM) provides password vaulting, credential management, privileged session management features, auditing, monitoring, and recording of privileged activities. Active Directory Bridge enables organizations to manage Unix and Linux environments via Microsoft infrastructure.

BeyondTrust's approach to ITDR is uniquely platform agnostic. The solution offers native support for Microsoft Active Directory, Microsoft Entra ID, AWS, GitHub, IBM, Okta, OneLogin, Oracle, PingOne, Duo, Thales, SecureAuth, and Thycotic, as well as connectivity to a variety of XDR products. The platform is available for deployment in on-premises, private/public cloud (on multi-regional AWS and Azure clouds), and hybrid configurations. BeyondTrust's products are certified on applicable frameworks such as FIPS 140-2 cryptographic standards, ISO/IEC 15408 (Common Criteria), and SSAE 18 SOC 2. The platform also boasts a comprehensive suite of REST-based APIs, with documented and versioned APIs throughout their product portfolio.

As indicated in the spider graph below, BeyondTrust's ITDR solution excels in a majority of the categories measured, namely Platform, Account Discovery, User Visibility, Risk Assessment, Event Detection, and Incident Investigation. For example, at one customer, BeyondTrust was able to identify more than 15,000 accounts and then associate them with 5,000 identities—improving the visibility and manageability of the organization's identity surface. At another customer, BeyondTrust was able to notify Okta of a breach the company discovered based on the platform's ability to spot token reuse from multiple locations. BeyondTrust also uses its experience and connection to customers to enhance its identification of attacks and its use of rules in the event of a breach. The company refers to their approach as “identity first security”—an apt description of ITDR.

BeyondTrust continues to make improvements in areas of remediation and identity posture. The foundational pieces are already there: the platform notifies administrators through the usual communication and API methods via integration with email and alerts. Currently, BeyondTrust is working to build out direct responses to threats, and seamlessly integrates with SIEM such as Splunk and Elastic to deliver additional context for effective triage and investigation. The platform currently lacks native integration with SOAR products but provides webhook integrations that can be configured by customers to automatically send detections and recommendations to any of their preferred SOAR tools, ticketing systems, incident response tools, or communication channels like Slack and Teams. It is worth noting that many customers do not expect the ITDR solution to provide such functionality, deferring

instead to their established SOAR workflows. Still, BeyondTrust aims to play a larger role in remediation and identity posture solutions.

Overall, BeyondTrust is positioned as a growth-oriented, stable, and innovative company with a strong product suite that emphasizes identity-first security. The company can meet the dynamic needs of businesses of all sizes, technical environments, and geography. The platform is well rounded and well-integrated, capable of detecting complex threats and alerting administrators and SOC analysts of in-progress identity attacks.

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



Table 4: BeyondTrust's rating

Strengths

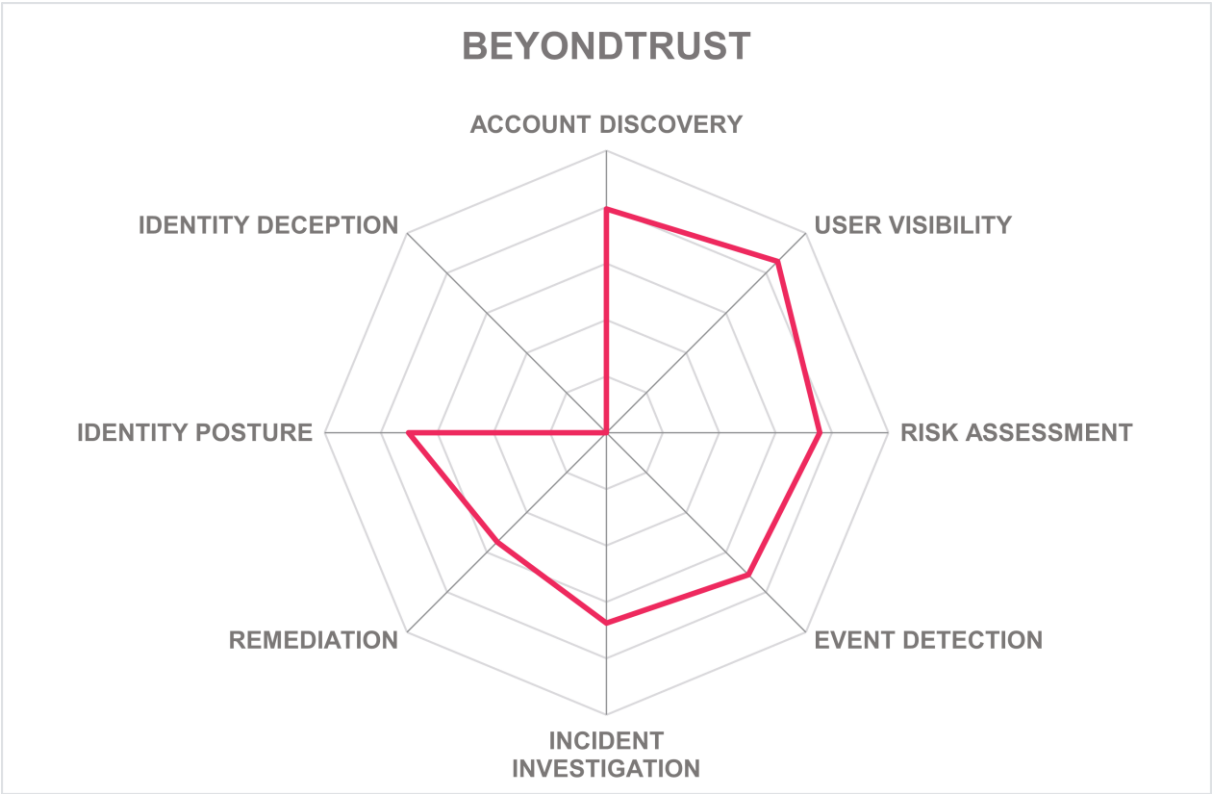
- Powerful product with flexible integration and deployment models
- Significant customer base and global partner ecosystem, as well as strong financials
- Maintains a research team that monitors threats and enables both product and customer teams to keep current on detection and response.
- Great use of intelligence to merge accounts and establish ownership of service accounts.
- A UI that guides analysts through incident responses, including helpful information in-product
- Automated recommendations, based on incident type

Challenges

- Working to build out stronger SOAR integration through webhooks with specific integrations
- Continuing to develop features for identity posture
- Moving toward real-time alerts and notifications
- No user risk scoring

Leader in





CrowdStrike – Falcon® Identity Protection

Established in 2011, CrowdStrike is a well-known, highly respected cybersecurity company. Headquartered in Austin, Texas, CrowdStrike is a publicly listed company. In CrowdStrike's view, ITDR is not really a standalone product—it's more of an activity that requires a platform. We've covered many such products in our Leadership Compasses on other areas that CrowdStrike participates in (see Related Research at the end of the document); in this review we focus on the company's ITDR capabilities.

CrowdStrike's product suite is anchored by its flagship CrowdStrike Falcon Identity Protection, which integrates into the broader Falcon Platform. It's also worth noting that CrowdStrike entered the ITDR market early with its acquisition of Preempt in 2020 leading to a mature product today.

Offered as a cloud-native SaaS service, the Falcon Identity Protection component requires a minimal on-premises footprint, requiring only a lightweight Falcon sensor on the AD domain controllers. This architecture also enables packet-level inspection and real-time alerting of suspicious events. The client approach also enables the product to force reauthentication based on time and activity.

Falcon Identity Protection excels at its deep coverage of Microsoft environments, including on-premises AD and Azure-based environments. The coverage ranges from aging AD protocols for domain controller replication, to password hash synchronization over AD Connect, to Azure based attacks on Entra ID. For example, Kerberos, LDAP(S), NTLM, and SMB protocols are all supported. The product is also capable of automatically distinguishing between user and service accounts and properly classifying them as such. The catalog of known attacks can detect pass-the-hash, golden ticket, and other internal attacks. The product also includes the ability to apply risk scores to accounts, which reduces noise for the SOC while improving the actionability of alerts.

The heavy focus on Microsoft AD and Azure, according to CrowdStrike, is that a very high percentage of successful attacks begin in those environments. Given the company's visibility into cyberattacks, that makes pretty good business sense. Integrations with IAM providers such as Okta and Ping come in the way of watching activity on LDAP groups and notifying Okta or a SOAR application of the event. The company plans to extend native integrations to other IAM platforms. Falcon Identity Protection does have connectivity to a number of SOAR solutions, but also provides an internal SOAR.

Given CrowdStrike's long history in InfoSec and SOC practices, Falcon Identity Protection offers unique features to help bridge identity administration—performed by IT—and identity security. It does this by providing guidance to InfoSec personnel who may not have deep knowledge of AD and Entra ID.

CrowdStrike's commitment to technical standards compliance is evident with certifications such as FIPS 140-2 and adherence to stringent frameworks like PCI-DSS v3.2, ISAE 18 SOC 2, HIPAA/HITRUST, and US FedRAMP. Their proactive stance on privacy, reflected in

their certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, underscores their dedication to data protection and compliance with GDPR.

The company's API ecosystem offers REST and GraphQL APIs for most of its functionalities, including real-time response to identity threats. This approach not only offers compliance with current tech standards but also portrays CrowdStrike's forward-thinking strategy, promising near-term enhancements to further open up their platform.

In short, CrowdStrike is a cyber industry force, and its Falcon Identity Protection demonstrates real attention to detail where threats are related.

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



Table 5: CrowdStrike's rating

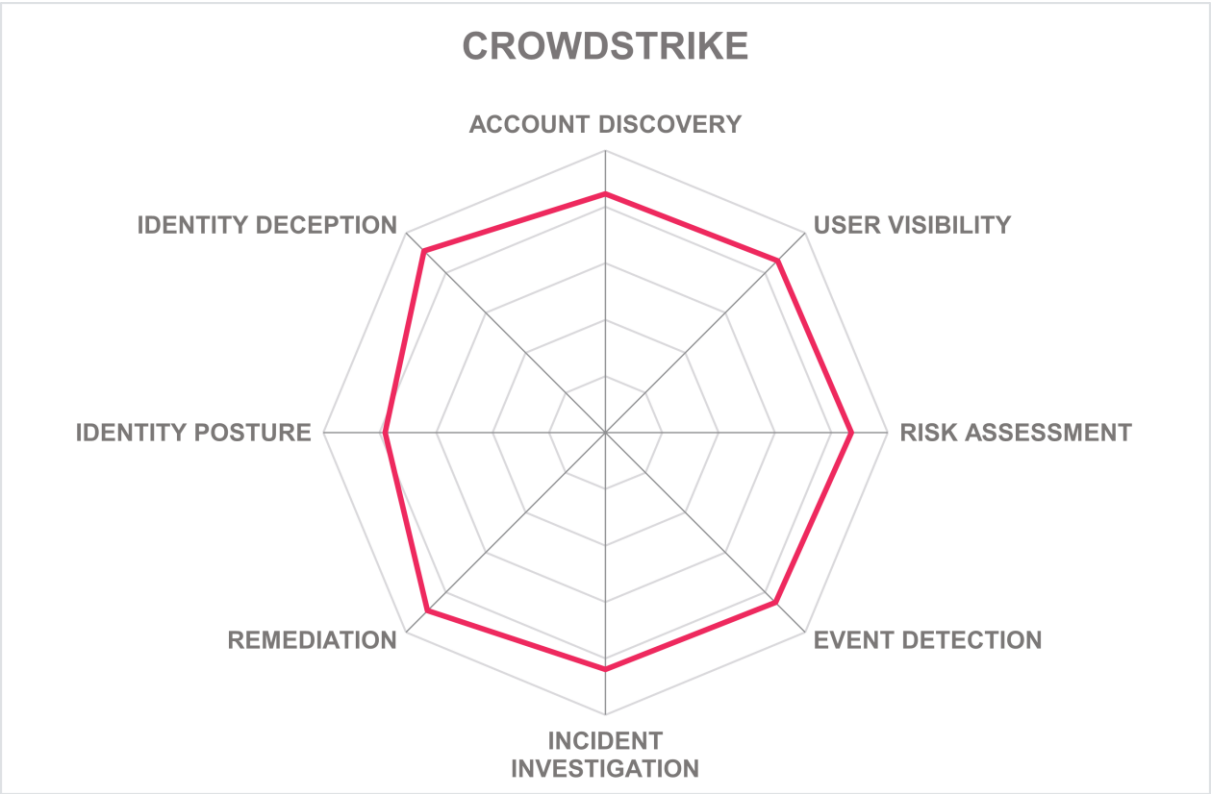
Strengths

- Established cybersecurity company with global presence and great resources
- Very strong protection for Microsoft environments; focus on Microsoft environments as the entry points to attack vectors
- Real time event detection and response
- Easy deployment model
- Dynamic user risk profiles

Challenges

- The higher commitment to CrowdStrike's larger platform could cause issues for some organizations
- The company's customer base is primarily in SOC departments, so will need to court identity administration teams

Leader in



Delinea – Authomize Platform

Authomize, established in 2019, is a recent entrant into the tech space that has swiftly made its mark, as evidenced by its [acquisition by Delinea](#). Though the company is not publicly listed, Delinea and Authomize have jointly developed a customer base over the previous two years, so the acquisition comes as an organic extension of the thousands of customers already in their mutual portfolios.

The centerpiece of Authomize's offerings is their platform, which—particularly in conjunction with Delinea's products—enables use cases for ITDR, CIEM, and security posture management. The platform also enriches SIEM and SOAR tools with identity context, and offers access reviews for regulatory adherence, all through a cloud-native, agentless approach. For this review, we consider the Authomize ITDR solution as a standalone technology from Delinea.

Architecturally, Authomize Platform is a SaaS solution, deployed on Kubernetes on Azure or AWS. It includes several avant-garde features such as decoy accounts for LDAP services and user behavioral analysis.

Authomize began its ITDR journey in creating visibility of identities and generating illustrations of relationships that make comprehending the complexity that large organizations face. To this end, Authomize has developed a system for agentless connectivity, over a dozen native API-based integrations and dozens more through SCIM, REST APIs, file uploads, or through OpenITDR (an Authomize technology). Native, agentless connectors include AWS, Azure Entra ID, GitHub, GitLab, Google BigQuery, Google Workspace, Okta, Ping, and Salesforce. The noteworthy bit about this list is that it demonstrates native connectivity to CIEM-managed platforms (AWS, GitHub, BigQuery) as well as IAM platforms and productivity applications. In this way, Authomize is unique in its scope, which covers identities across DevOps, identity systems, and business applications. Of note, understandably, is the platform's lack of integration with IGA solutions outside of Delinea.

As the Authomize platform acquires data, it automates account linking and reconciliation tasks to provide a condensed view of these identities. The dashboard offers risk scoring at a variety of levels and even identifies the type of risk the organization faces—such as account takeover—and tracks the organization's identity posture over time. The dashboard also shows these risks on a graph to attack paths listed in MITRE ATT&CK. With simple access to a wealth of data, an intuitive UI, Authomize excels at account discovery, user visibility, and risk assessment.

For event detection, Authomize offers a combination of integration with SCIM tools and direct event detection. The platform does provide many modes of user behavioral analysis, including failed login attempts, geo velocity, and usage patterns.

Similarly, for incident investigation and response, Authomize was just starting to mature in these use cases when Delinea agreed to acquire the company. Given the two companies' history of collaboration, it makes sense to formalize that relationship, because the technical alignment of their solutions provides its own business justification. Delinea is ranked as an Overall Leader in our [report on the PAM market](#), so the combination of the tools enables Authomize to rapidly realize their strategic vision for ITDR.

From a security perspective, with certifications in ISO/IEC 27001 and ISAE 18 SOC 2, Authomize aligns with globally recognized technical standards. Delinea will doubtless also assist in rounding out a broader set of security certifications.

Authomize provides RESTful APIs and webhooks to enable integration and extension but is still working to expose its full set of functionalities this way. Authomize also cooperates with Axiomatics and Delinea on a project called OpenITDR, a tooling framework for enabling adoption of ITDR solutions. The project is currently in a GitHub repository but is a recent entrant into the industry and has yet to find critical mass.

Overall, Authomize presents a compelling package with its innovative ITDR platform. The recent acquisition by Delinea may serve as a catalyst for further growth and consolidation in the PAM space.

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



Table 6: Delinea Authomize's rating

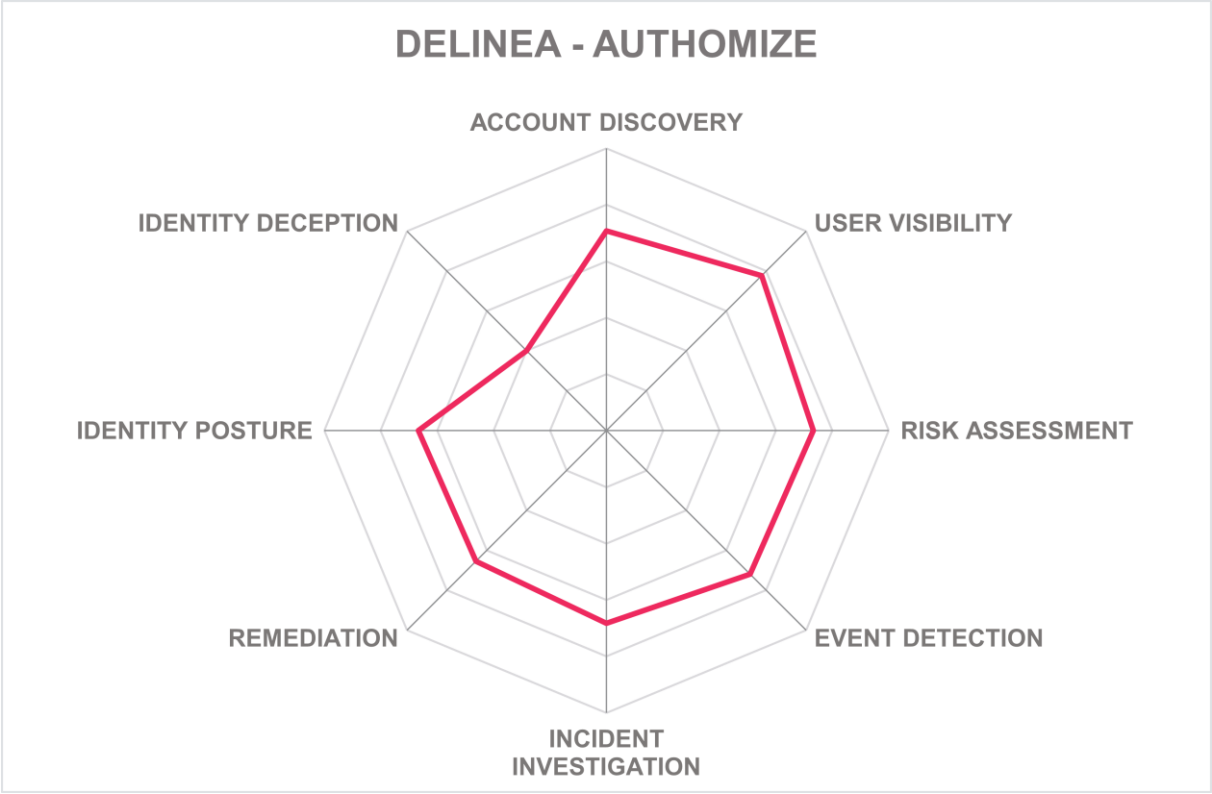
Strengths

- Strong visibility features across a variety of application environments
- Built-in security playbooks, behavioral monitoring, and risk engine accelerate account cleanup tasks
- Integration with Delinea has already been tested, making Authomize a great choice for Delinea's customer base
- Decoy account management for LDAP services
- Working on OpenITDR, an open framework for ITDR solutions

Challenges

- Merging business functions of the companies could take some time to smooth over, requiring some patience on the part of new customers
- As a Delinea product, Authomize isn't a good fit for organizations using other IGA tools (such as SailPoint or Saviynt)
- Lack of native support for IAM solutions from Broadcom, IBM, OpenText, or Oracle IAM platforms make Authomize a poor fit for organizations investing in those platforms
- Comparatively new product on the market and could require time to mature

Leader in



Gurukul – Gurukul Platform

Gurukul, established in 2010, is a leading provider in security analytics and operational technology. Headquartered in Los Angeles, California, Gurukul has established itself as a notable IAM vendor. Gurukul's international presence and customer base spans North America, EMEA, APAC, and Latin America, making the company a global player.

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. Gurukul's approach is to offer an "identity and access analytics platform" that provides SIEM, user and entity behavior analytics (UEBA), XDR, SOAR, and identity analytics with elements of PAM and IGA. The combination of these technologies also enables the platform to provide ITDR solutions, even though it's a use case not currently listed on the company's website.

Gurukul's platform features an automated data interpretation engine that creates data pipelines for any source. For example, sources may include IAM platforms, logs, network events, endpoint data, ITSM telemetry, and so on, but these sources don't require custom parsers, because Gurukul's AI-powered engine normalizes the data received. The idea is to rely more heavily on a trained ML engine than on native integrations, so potentially a greater number of data types and sources can be used without data cleansing or classification projects.

The platform is built to ingest significant amounts of data from a large number of applications into a native data lake or a Snowflake data lake. With this information, Gurukul offers AI-assisted visibility into the organization's identities and service accounts. The product also provides automated risk scoring of these accounts, based on a wide range of rules. For example, Gurukul checks for UEBA deviations, peer group deviations, rule and policy violations, access outliers, and dormant/rogue access, and then layers in threat intelligence, HR events, and watchlists to derive risk scoring and alerts. The platform offers flexibility in deployment models ranging from on-premises or virtual appliances to public or private cloud.

The company boasts an impressive partnership ecosystem, with alliances across various domains such as IAM, PAM, IGA, and CMDBs. Gurukul aligns with prominent standards bodies, incorporating FIPS 197, FIPS 140-2, NIST 800-57, ISO/IEC 15408 (Common Criteria), ISO/IEC 27001, and PCI-DSS v3.2. The Gurukul API and SDK highlights the product's open product architecture, allowing for extensive customer and tech alliance integrations.

In general, Gurukul provides an integrated approach to identity analytics. The company continues to expand internationally and offers training programs and support services. Gurukul's strengths are highlighted by their expansive data science team and a suite of over 2,000 analytical models. A potential area for improvement could be the expansion of their support for various languages and documentation, which is currently limited to a few major languages.

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

GURUCUL

Table 7: Gurucul's rating

Strengths

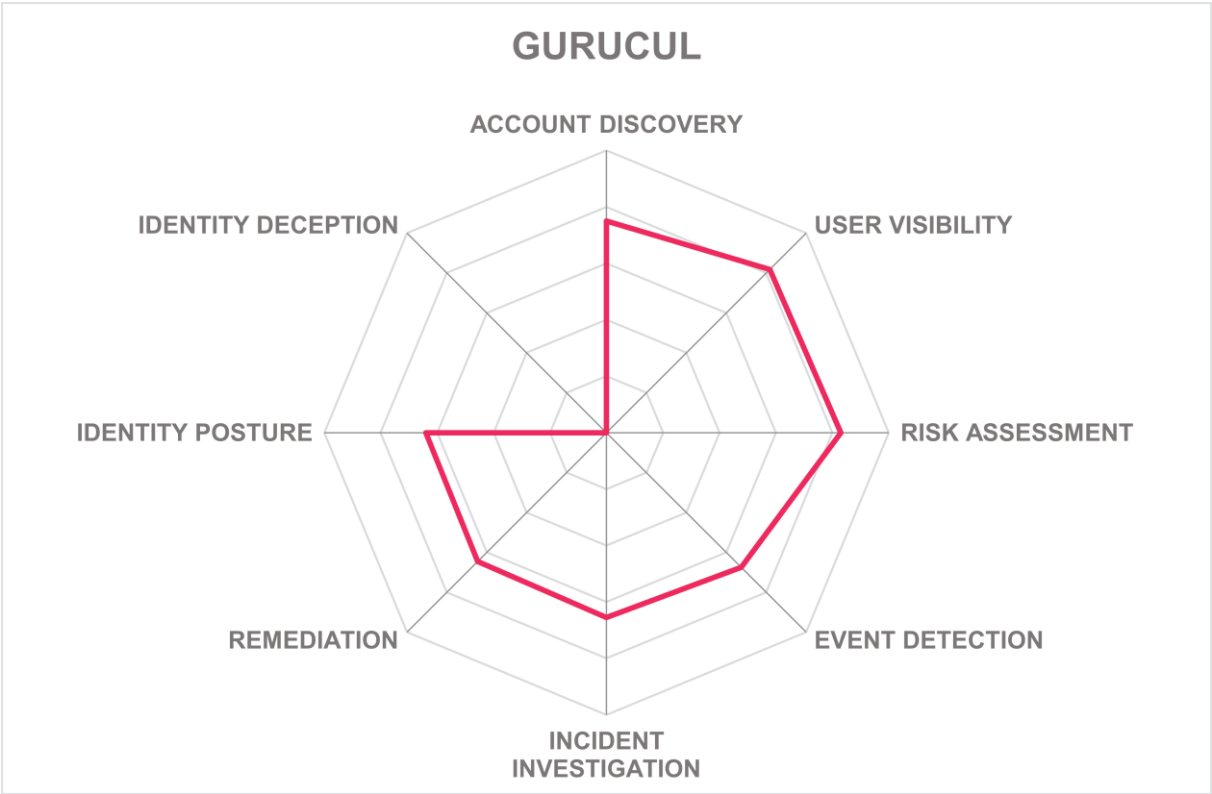
- Broad visibility and monitoring of user accounts
- Flexible deployment models with a simplified integration pattern
- Modern approach to identity analytics with integrated use of AI/ML technologies
- Pioneered UEBA and continues to promote behavioral analysis as a key ingredient to securing identity

Challenges

- For organizations looking specifically for ITDR products, Gurucul’s approach might not be a full-fledged fit

Leader in





Microsoft – Entra ID + Defender XDR

Microsoft is the behemoth in this field. The company is headquartered in Redmond, Washington, and is known for its extensive security efforts. Microsoft's ITDR suite consists of Microsoft Entra ID and Microsoft Defender XDR, which can be used jointly for enhanced ITDR capabilities. Microsoft Entra offers IAM solutions with tools for strong authentication and risk-based adaptive access policies. Microsoft Defender offers XDR features for that also coordinates actions across endpoints, identities, email, and applications.

One benefit in using both IAM and XDR tools is that Microsoft's approach to ITDR is refreshingly open, including integration with other cloud identity platforms such as AWS, Google Cloud, and Okta. Protections extend beyond the Microsoft ecosystem to secure email, virtual machines, and devices.

The solution also benefits from the strength of Microsoft's security teams, such as the Microsoft Incident Response team, which works directly with governments and large companies throughout the world. Telemetry data also can be fed from Sentinel. By embedding learnings from their security teams and monitoring products, Microsoft can improve the signal-to-noise ratio that hits the SOC.

The Defender interface also offers a feature called Microsoft Secure Score. This is essentially an assessment of your organization's security posture. Defender lists various security compliance tasks and rates how well you've implemented them. For example, Secure Score suggests removing dormant accounts from sensitive groups and then assists you in completing the task.

The solution also uses Microsoft Copilot for Security to help fuse signals from a variety of sources in Azure into a single high-confidence event. The UI then enables SOC analysts to have a consolidated view of the attack path with information on how to thwart it. Copilot for Security is able to create plain text descriptions of identified risks and offer natural language recommendations on what to resolve the situation. Responses can be in the form of direct action, a scheduled task, or creating more complex "initiatives." The built-in intelligence in the product also makes it easier both for IT administrators and SOC teams to quickly cooperate during events or breaches.

Microsoft adheres to numerous technical standards, including those from FIPS, NIST, ISO/IEC, PCI-DSS, ISAE, HIPAA/HITRUST, and US FedRAMP, showcasing a commitment to international compliance and security best practices.

Microsoft's products are known for their API accessibility, with Microsoft Graph allowing the integration of various Microsoft security products. API versioning, REST, and OData are supported, and the company offers SDKs along with a developer portal for assistance.

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



Microsoft

Table 8: Microsoft’s rating

Strengths

- World-class security expertise and resources
- Risk assessments and scoring for posture and users, with aid of Copilot for Security
- For organizations already committed to Microsoft infrastructure, this solution interoperates with and extends other critical services
- Strong security vendor with dedicated teams for XDR and cloud hardening

Challenges

- Tough competition from cybersecurity vendors
- ITDR solutions require licensing multiple products
- Broader integration with IAM platforms needed
- Organizations that can’t make a full stack commitment to Microsoft
- On premises AD implementations are still exposed

Leader in



OVERALL
LEADER



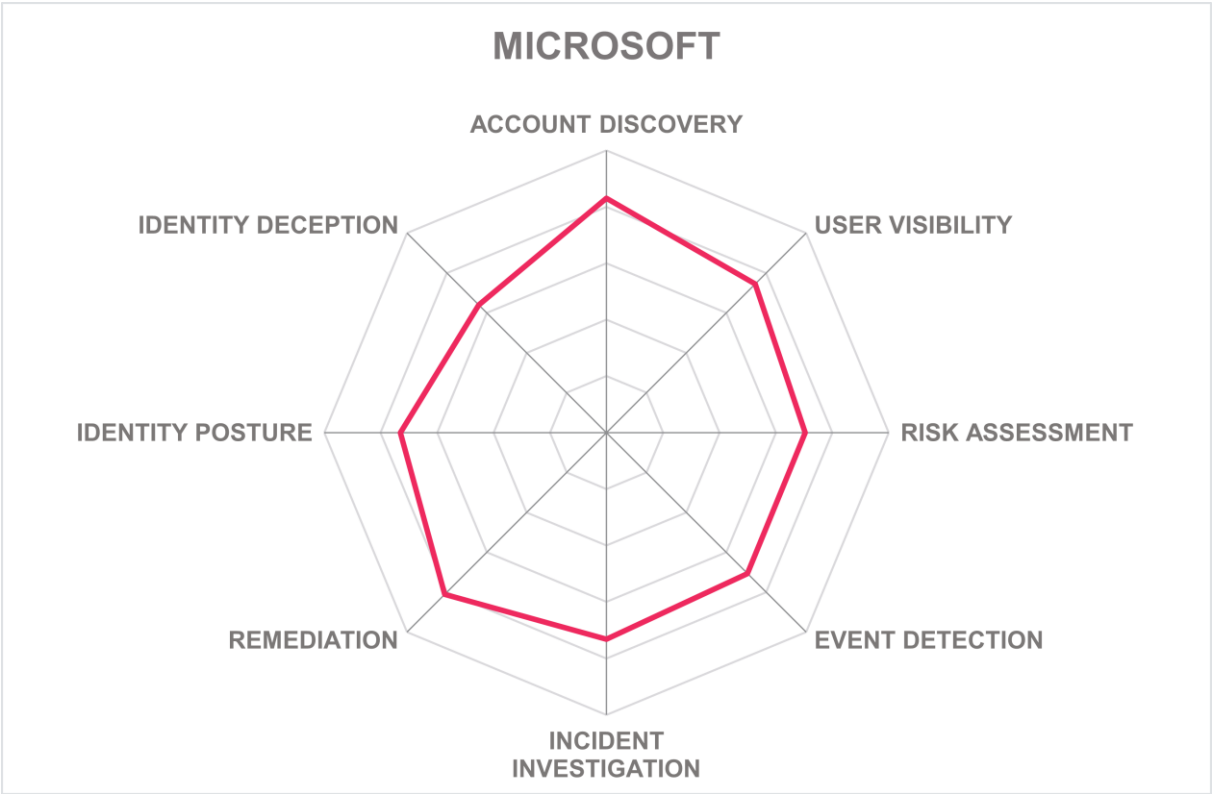
PRODUCT
LEADER



INNOVATION
LEADER



MARKET
LEADER



Securonix – Securonix Platform

Securonix, established in 2009, operates with a mix of private equity and venture-backed funds. Securonix's flagship product is Unified Defense SIEM. But even with this focus, the product offers strong ITDR capabilities.

Rather, Securonix offers the Unified Defense SIEM, a fully integrated suite that includes a single product, service, and platform. It is a comprehensive solution designed to cater to security information and event management needs with a "collect-detect-respond-contain" approach. Dubbed "next-generation SIEM," the platform is even more featured than most products that use that moniker.

Several years ago, Securonix re-platformed to the cloud with an underlying Snowflake data lake. Among other things, this architecture enables Securonix to offer customers a "Bring Your Own Snowflake," which enables significant features, such as a hot search with a one-year lookback, and integration with Securonix Investigate, enhancing context and collaboration capabilities. It's important to note that although Securonix is built on Snowflake, customers aren't required to provide their own licenses.

The platform makes extensive use of ML; this comes in several forms. First, the ML sets baselines and looks at what is normal and what might be violation as it detects deviations from norms. This baseline relates to peer groups as well as to individual accounts. The product also uses ML to enrich events and alert information with information from a variety of sources—and even create and manage account records using this data. It can compare emails from unknown domains and check it against its own list of embargoed or risky domains.

The platform's risk scoring features are likewise 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.

Securonix supports integrations with many third-party products and services, including the usage of OEM products like Snowflake and Polarity to augment its capabilities. Additionally, the platform integrates with major IAM products, such as from Microsoft, Okta, and Ping.

Securonix aligns with multiple technical standards and certifications, such as FIPS 140-2, NIST 800-57, ISO/IEC 27001, PCI-DSS, ISAE 18 SOC 2, and HIPAA/HITRUST. The product is undergoing US FedRAMP certification, demonstrating a commitment to adhering to stringent security standards.

The product offers extensive API support, primarily through REST, and covers data formats like CSV, JSON, XML, CEF, and LEEF. API versioning is supported, with authentication methods including SAML and key exchange, although it does not provide SDKs. The product's API openness is marked by the availability of a developer portal with comprehensive documentation.

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



SECURONIX
Security Analytics. Delivered.

Table 9: Securonix’s rating

Strengths

- Mature behavioral monitoring and risk scoring features
- Data enrichment in the event feed coalesces data from multiple sources and makes them available
- Integrated SOAR capabilities
- Respectable market penetration, growth, and funding make Securonix a stable company

Challenges

- The company’s general-purpose approach and focus on next-generation SCIM may interfere with deeper integrations with IAM products
- Lack of SDKs

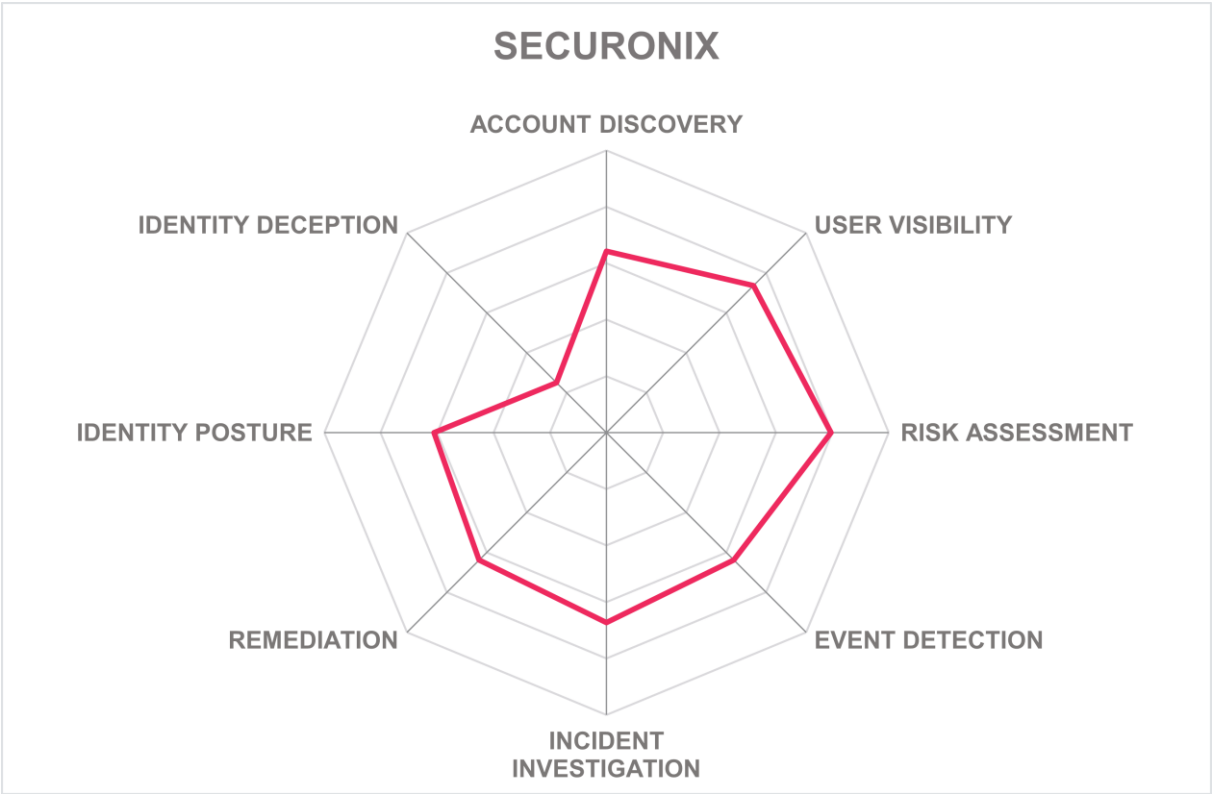
Leader in

OVERALL
LEADER

PRODUCT
LEADER

INNOVATION
LEADER

MARKET
LEADER



SentinelOne – Singularity Identity

SentinelOne, established in 2013, is a publicly traded entity on the NYSE. The company has positioned itself as a leader in cybersecurity with its advanced Singularity platform. It is headquartered in Mountain View, California.

SentinelOne's product suite, the Singularity Platform, offers enterprises protection over a variety of attack surfaces. The platform is backed by the Singularity Data Lake that provides a graph-structured view of identities and other data. The data lake architecture also enables long-term storage of data with rapid query response times. Recently, SentinelOne announced its acquisition of PingSafe, a CNAPP vendor. By integrating their products into a platform, SentinelOne's aim to offer a seamless, unified platform for protecting cloud workloads, endpoints, and identity systems.

The company's ITDR product, Singularity Identity, protects identities and reduces the attack surface through real-time infrastructure defense for Azure Entra ID and AD. A signature feature for the platform is deception-based endpoint protections. This feature manages sets of decoy users and groups that seem real to attackers, but in fact are in the environment only to detect attackers' presence. The advantage here is that if any activity is detected with the decoy credentials, it can almost be guaranteed to be initiated by attackers. This also helps detect attackers performing reconnaissance (recon) activities in the environment—one of the first steps threat actors take after the original breach.

Other notable features include detection of known attacks on AD, such as golden/silver ticket, DCSshadow, DCSync, pass-the-hash/ticket, and AS-REP roasting, and many more. Such specificity can reduce the number of false positives reported to the SOC compared to ML-based monitoring.

SentinelOne is also pioneering the concept of AiSecOps with their technology dubbed Purple AI, an LLM by SentinelOne that resides in their own data lake. Purple is trained specifically for SecOps usage and provides answers that are specialized to this field. Among the benefits this technology aims to achieve is to create an imbalance of effort that favors defenders over threat actors, unify signals and data in a single UI, offer holistic threat hunting, and provide a natural language interface for analysts and response teams. For example, the product suggests prompts and saves them in a notebook.

Singularity Identity complies with critical security standards. SentinelOne holds certifications such as FIPS 140-2, NIST 800-57, PCI-DSS v3.2, HIPAA/HITRUST, and US FedRAMP.

The Singularity Identity platform provides a wide array of APIs, supporting REST, gRPC, SOAP, Websockets, GraphQL, and TCP/UDP Socket APIs, signifying a high degree of openness. The absence of SDKs or a developer portal, however, indicates that while SentinelOne offers various API protocols, there might be limitations in terms of developer resources and community support.

In conclusion, SentinelOne stands as a formidable entity in the cybersecurity domain, boasting significant technological prowess, a solid customer base, and a clear commitment

to security standards compliance. Its ability to provide a unified solution for endpoint and cloud security positions it well in a market that is increasingly shifting towards integrated security platforms.

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



Table 10: SentinelOne's rating

Strengths

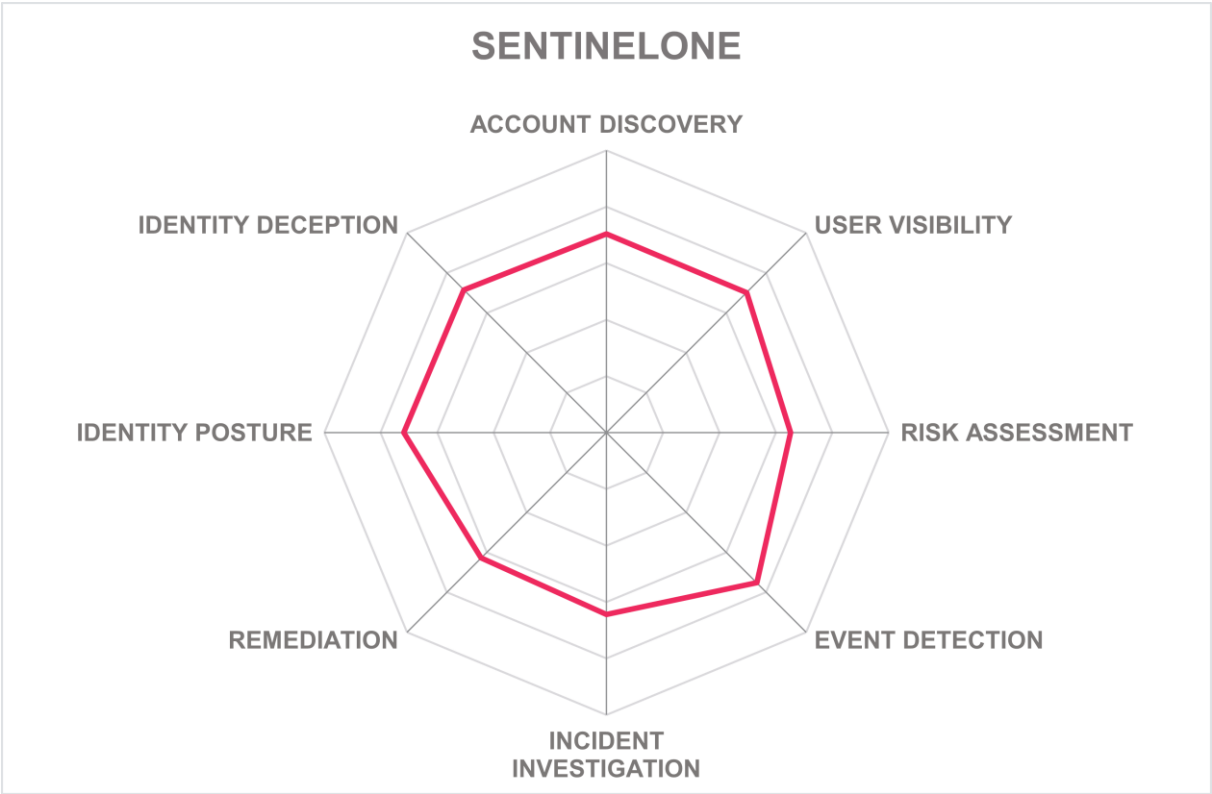
- Large customer base with strong growth forecast
- Mature products with a strong foothold in protections for Azure Entra ID and AD
- Strong use of AI and data lake technology provides for efficient threat hunting
- Ability to deploy decoy accounts and assets for added high-fidelity threat detection
- Wide coverage of API types
- Multiple security certifications

Challenges

- Emphasis on Azure and AD environments may be less appealing to organizations less dependent on Microsoft
- Passive approach to SOAR integration may not work logistically in some organizations
- Lack of SDK and developer portal dampens custom and 3rd-party integrations

Leader in





Sharelock – Identity Security Platform

Sharelock, a private entity self-funded by shareholders who successfully sold CrossIdeas to IBM, is now working to disrupt the market for identity security. Founded in 2019 and headquartered in Italy, the firm operates with a lean team. Nonetheless, despite being in an early stage, Sharelock showcases a robust commitment to research and development.

Sharelock Identity Security Platform (ISP) combines Identity Security Posture Management (ISPM) and ITDR. Sharelock's ITDR component focuses on real-time threat detection, leveraging indicators of behavior with Machine Learning (ML) sophisticated algorithms to detect anomalies and correlate them across identities, humans, and machines.

Built on Kubernetes, Sharelock ITDR operates in any Kubernetes environment, offering flexibility for cloud or on-premises deployment. Its native multi-tenant architecture enables partners to run it as a Managed Service. With robust infrastructure, it ensures scalability and reliability while incorporating a self-protecting security environment. This mechanism continuously inspects Kubernetes workloads and pods for signs of compromise or misconfiguration, enhancing security at multiple levels of operation.

Sharelock offers native integration with leading IGA products such as OneIdentity, SailPoint, and IBM. This integration enables Sharelock ITDR to tap into a repository of identity data managed by these solutions, providing high visibility into the organization's identity landscape. Sharelock uses this data to go beyond simple account-level visibility and delve into the intricate web of identity relationships, roles, and entitlements across the organization.

Sharelock's approach to building behavior baselines ensures accuracy by using a customer dataset of logs and Identity data rather than a generic dataset, minimizing false positives. Sharelock leverages unstructured data within its ITDR framework for enhanced threat detection. Despite the untapped potential in organizational data, Sharelock effectively categorizes files and folders, critical for identifying account and identity behaviors.

Sharelock's Threat Modeler is used for correlating anomalies with recognized threat tactics. Anomalies are mapped onto the severity kill chain and MITRE techniques and tactics. In Sharelock's platform, threats are distinct from notifications, with a life cycle until remediation. Security analysts are notified only when threat severity increases or progresses, streamlining response to evolving threats within the standardized terminology of the security landscape.

Sharelock ITDR features a comprehensive playbook for threat response, offering predefined actions and manual/automatic response options for flexibility. The playbook streamlines incident response, reducing response times. Key elements include a mix of automatic and manual responses, triggering actions like notifications, audits, recertification campaigns, and IAM workflow automation. Integration with incident management systems and centralized log management enhances threat analysis and reporting.

Sharelock integrates with companies' detection, workflow, and communications systems with REST APIs and JSON data formats.

Sharelock's has so far developed its business in Europe, but with shows great growth potential in the identity market.

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



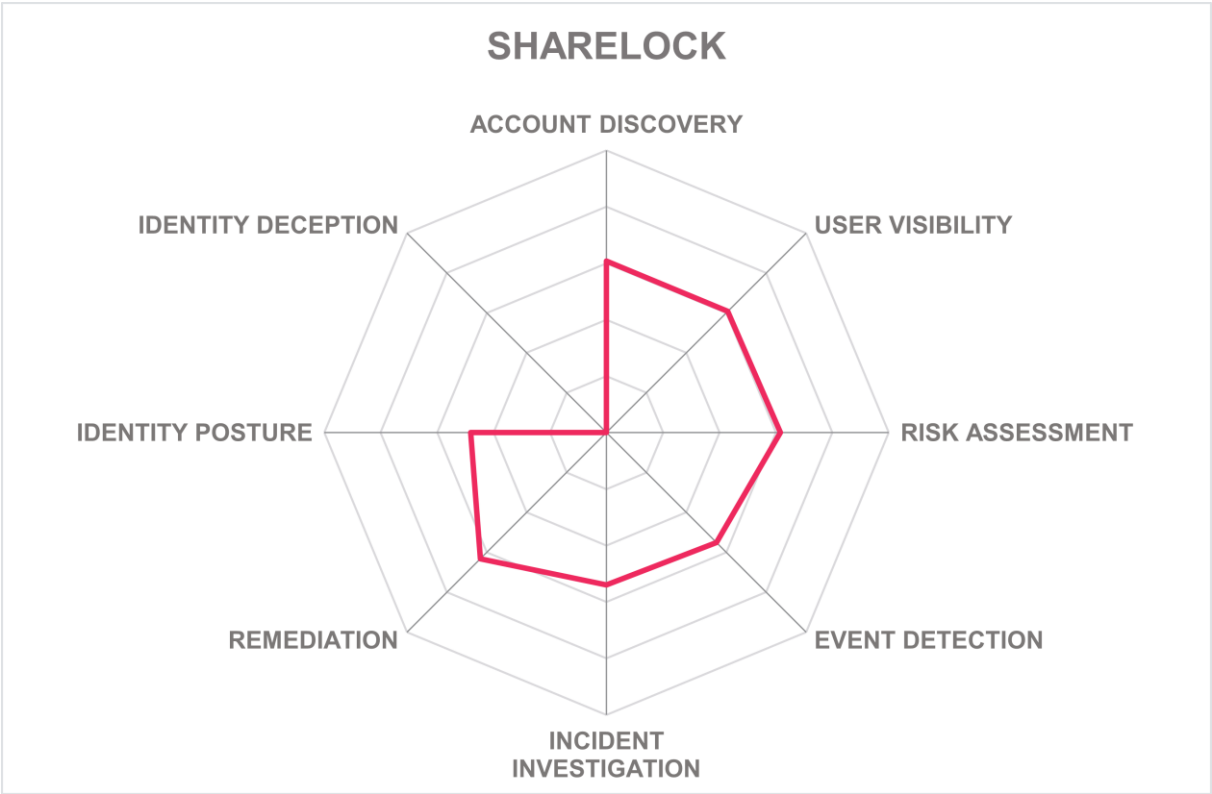
Table 11: Sharelock's rating

Strengths

- Innovative architecture with modern approaches to ITDR
- Use of AI to lessen the burden on organizations in making sense of their identity data
- Standard playbook available, including more than 50 predefined Indicators of Behavior (IoBs)

Challenges

- Need to grow the customer base across more geographic regions
- Stronger focus on operational parts of the company, such as sales, services, and other critical functions
- Stronger partnerships with companies that have established regional or global presence



Vendors to Watch

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

Cisco

Cisco recently entered the ITDR market with its acquisition of Oort, a US-based startup focused on ITDR technology. Prior to the acquisition, Oort had already managed to create a cloud-first model for securing identity systems.

Why worth watching:

Cisco is still working to integrate Oort's technology into its security stack, but Cisco now has the ability to become a formidable vendor in the ITDR and related markets.

Palo Alto Networks

Palo Alto Networks offers an ITDR module as part of its Cortex products, both in its Cortex Extended Security Intelligence and Automation Management (XSIAM) and XDR products. This approach reflects a SOC-centric approach to ITDR, with even detection and threat hunting at its core.

Why worth watching:

Palo Alto Networks has established itself as a major vendor in markets adjacent to ITDR, including SOAR and threat detection. The company's status and experience in such fields could lead them to capture a much larger presence in the ITDR market.

Semperis

Semperis offers an Identity Resilience Platform aimed at protecting and preserving Microsoft Entra ID and AD environments. A unique feature about the Semperis is the ability to rollback and recover Entra ID and AD after an attack has taken place.

Why worth watching:

Semperis has found a market fit that expands on the concept of ITDR. Many customers require the ability to restore their AD to a known good state rather than attempting go-forward fixes to a breach.

Silverfort

Silverfort offers an ITDR product that emphasizes authentication and MFA. The solution integrates with endpoint security and MFA to detect risky access patterns and then integrates with identity systems and SOAR solutions to restrict block access.

Why worth watching:

One of the best ways to reduce risk of identity-based threats is to implement MFA, but organizations still struggle to implement this security mechanism. Silverfort's approach offers the ability to roll out MFA while integrating authentication signals into IAM and SOC systems.

SPHERE

SPHERE provides tools to improve the posture and hygiene of organization's AD systems. The product provides visibility into user accounts, service accounts, groups, and policies and identifies areas of risk. SPHERE then provides automated processes to remediate such issues and maintain an organization's security posture.

Why worth watching:

For IT administration teams focused on AD, SPHERE provides an alternative that doesn't overlap with existing SOC tools for SIEM or SOAR. This focus enables the IT team to move forward with scoped projects readily.

Whiteswan Identity Security

Whiteswan Identity Security is an early-stage startup focused on protecting identity systems. The product offers deep integration with AD and applies a proxy approach to guard against even shell commands and internal attacks.

Why worth watching:

Whiteswan offers a slightly different mix of technologies for ITDR solutions than other vendors. The solution includes endpoint security, MFA, access control, and privilege management. With an experienced senior team and a growing list of customers, Whiteswan Identity Security is poised to make their presence known to the industry.

Zscaler

Zscaler is a global cybersecurity company that offers a cloud-based platform for Internet security, compliance, advanced threat protection, and other information security services. The company offers 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: [Intelligent SIEM Platforms](#)

Leadership Compass: [Cloud Infrastructure Entitlement Management \(CIEM\)](#)

Leadership Compass: [Cloud Security Posture Management](#)

Leadership Compass: [Security Orchestration Automation and Response \(SOAR\)](#)

Leadership Compass: [Privileged Access Management](#)

Blog: [Threat Detection and Incident Response](#)

Webinar Recording: [Effective Endpoint Security with Automatic Detection and Response Solutions](#)

Executive View: [Sharelock ITDR](#)

Webinar Recording: Mastering Global IAM for Cybersecurity Excellence: [From Zero Trust Principles to Identity Threat Detection & Response \(ITDR\)](#)

Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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

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

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