ISG Provider Lens™

# Cybersecurity – Services and Solutions

Analysing the cybersecurity market and comparing provider portfolio attractiveness and competitive strengths

Customized report courtesy of:

KUDELSKI SECURITY

**QUADRANT REPORT | 2025 | U.S., GLOBAL**

Table of Contents

**Page 1 of 2**

Page 2 of 2

*Report Author: Gowtham Sampath*

## The evolving complexity of cyberthreats in the U.S. demands adaptive resilience and AI-centric security

### Current state of the U.S. cybersecurity threat landscape

The cybersecurity threat landscape in the U.S. remains highly dynamic, presenting continuous challenges for organizations. Analysis of recent incidents by industry and public sector organizations reveals ongoing evolution in adversary tactics and a concerning increase in the scale and impact of attacks.

**Recent data breaches and their impact:** The frequency and impact of data breaches affecting U.S. enterprises and service providers have shown a concerning upward trend throughout 2024. The ransomware attack on Change Healthcare, a subsidiary of UnitedHealth Group, significantly impacted the healthcare industry in February 2024. This incident disrupted medical claims processing nationwide and exposed the sensitive data of over 100 million individuals, leading to an estimated financial impact exceeding $3 billion for UnitedHealth Group. The financial services industry also remains a frequent target, with institutions facing persistent threats aimed at disrupting operations and exfiltrating sensitive financial data. Furthermore, the breach of the cloud data platform Snowflake in May 2024 demonstrated the expanding attack surface in cloud environments, affecting over 100 of its customers, including major corporations such as AT&T and Ticketmaster. These high-profile incidents serve as reminders of the persistent challenges in preventing sophisticated intrusions and the substantial financial, operational and reputational consequences they impose.

**The rise of ransomware and extortion tactics:** Ransomware continues to be a dominant threat in the U.S. cybersecurity landscape, with increased frequency and sophistication of attacks in 2024. The average ransom demand in the year's first half surged to more than $5.2 million, highlighting the significant financial stakes involved. Double extortion tactics,

**Security** integrated with **business strategy** is integral for **digital** and **AI transformation** initiatives.

involving both data encryption and exfiltration, are now commonplace, increasing the pressure on organizations to pay demands. Industry analysis highlights numerous ransomware attacks targeting critical infrastructure and various sectors, emphasizing the need for proactive prevention and robust recovery strategies to ensure business resilience.

**Increase in AI-related attacks:** Threat actors are rapidly adopting and adapting AI technologies, including generative AI (GenAI), to enhance the effectiveness and scale of their malicious activities. This includes automating spear phishing campaigns, generating convincing deepfakes for social engineering and accelerating the identification of software vulnerabilities. AI-enhanced malware attacks have emerged as a primary concern for IT professionals, with a significant percentage identifying it as the most concerning AI-generated threat. This rapid access to cutting-edge technologies allows adversaries to reduce the time required to exploit vulnerabilities, compromise data and build ransomware, creating a significant challenge for defenders.

**Trending cybersecurity capabilities in the U.S. market**

In response to the evolving threat landscape and increasing regulatory pressures, several cybersecurity services and solutions are gaining significant traction within the U.S. market, with a growing emphasis on enhancing organizational resilience. This shift reflects an urgent need for advanced technologies and strategies to safeguard critical assets and adapt to dynamic security requirements.

- **AI for cybersecurity and cybersecurity for AI:** The U.S. market is witnessing a significant focus on both leveraging AI to enhance cybersecurity capabilities and addressing the unique security challenges posed by AI systems themselves. AI-powered systems can process massive amounts of data in real time, identifying anomalies and vulnerabilities that would be hard to detect manually, thereby enhancing threat detection and response. Simultaneously, there is a growing awareness of the need for *Cybersecurity for AI* to protect AI models, training data and AI-powered applications from adversarial attacks and vulnerabilities. The awareness encompasses addressing data poisoning, evasion attacks and interruption of service attacks targeting AI systems. Industry frameworks and guidelines, such as the NIST AI Risk Management Framework, are being developed to help organizations manage the risks associated with AI and ensure its secure development and deployment. This dual focus on AI as both a security enabler and a potential target is crucial for building a resilient digital ecosystem.
- **Continuous Threat Exposure Management (CTEM):** The CTEM framework emphasizes continuously identifying, assessing and mitigating risks posed by cyberthreats across an organization’s entire attack surface. Unlike traditional periodic assessments, CTEM embeds real-time monitoring and adaptive cyber risk management into daily operations, allowing organizations to strengthen their security posture and stay ahead of potential breaches. Industry experts anticipate that organizations prioritizing CTEM will be significantly less likely to experience successful cyberattacks, highlighting its importance in forward-thinking security strategies.
- **Zero trust architecture:** The adoption of zero trust security principles is gaining significant momentum across U.S. enterprises as organizations strive to secure their increasingly gaping network perimeters. Implementing zero trust often involves key components such as identity and access management (IAM), which is rated as highly important for cloud strategies. Microsegmentation, which isolates every asset to limit lateral movement, is also recognized as crucial for accelerating zero trust initiatives.
- **Analytics and automation:** Organizations are increasingly turning to advanced analytics and automation technologies to enhance the efficiency and effectiveness of their security operations. These solutions help streamline detection-to-response workflows by connecting various security tools, automating repetitive tasks and codifying incident response processes through playbooks. The evolution of

these capabilities has moved toward AI-driven solutions that can interpret data, identify patterns and make real-time recommendations. Key use cases include automated phishing response, ransomware containment, insider threat detection and vulnerability management.

- **Cloud security solutions:** As hybrid and multicloud environments become the norm, the need for comprehensive and integrated cloud security solutions will only continue to grow. This has increased demand for Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP). These platforms provide crucial capabilities such as preventing misconfigurations, enforcing security best practices and offering runtime protection for cloud workloads. The trend toward DevSecOps is further deepening the integration of CWPP and CSPM into the CI/CD pipeline, enabling automated security and compliance checks throughout the application development lifecycle.
- **Managed Detection and Response (MDR):** The ability of MDR services to act as an outsourced security operations center (SOC), providing scalable and cost-effective advanced protection, is a key driver for their widespread adoption and contribution to cyber resilience. Unlike basic monitoring tools, MDR combines 24/7 monitoring, advanced threat detection leveraging AI and threat intelligence, and rapid incident response capabilities. MDR providers offer proactive threat hunting, actively searching for hidden risks before they escalate into major incidents.

**U.S. cybersecurity regulatory and compliance environment**

The cybersecurity regulatory landscape in the U.S. continues to evolve, increasing demands on organizations to ensure compliance and build resilience.

- **Emerging regulatory trends and proposed legislation:** The regulatory landscape is becoming dynamic, with new rules and proposed legislation indicating a growing emphasis on cybersecurity and resilience. New rules on cybersecurity incident disclosure for publicly traded companies underscore the increasing focus on transparency and accountability. Ongoing discussions around potential federal data privacy law could further reshape the regulatory environment. There is increasing regulatory attention on the cybersecurity of critical infrastructure industries, reflecting the need for enhanced resilience against sophisticated threats. The trend of states enacting their own data privacy laws is also continuing, with several new laws taking effect in 2025 in states such as Iowa, Delaware, Nebraska, New Hampshire and New Jersey, adding to the complexity of the compliance landscape.
- **Industry-specific regulations and guidelines:** Certain industries in the U.S. operate under specific cybersecurity regulations tailored to their unique risks and the criticality of their operations. The financial services industry, for example, is subject to regulations from bodies such as FINRA and the New York Department of Financial Services (NYDFS), emphasizing cyber resilience. The healthcare industry must adhere to HIPAA, and the energy industry faces guidelines from the Department of Energy. These industry-specific regulations highlight the need for tailored security solutions and expertise to ensure resilience within these critical areas.

**Key enterprise cybersecurity challenges in the U.S.**

U.S. enterprises face a complex and evolving set of cybersecurity challenges that impact their ability to maintain operational and business resilience.

- **The evolving threat landscape:** The increasing sophistication and volume of cyberthreats continue to challenge enterprises' resilience. Threat actors constantly develop new techniques, including AI-powered methods and exploit emerging vulnerabilities, demanding a proactive and adaptive security posture.
- **Supply chain vulnerabilities:** The increasing reliance on complex supply chains introduces vulnerabilities that attackers can exploit, impacting the

resilience of enterprises. Industry reports indicate that supply chain challenges are a leading barrier to achieving cyber resilience for many organizations, often due to a lack of visibility and oversight into supplier security levels. Ensuring the security of the entire supply chain, including device integrity, secure development lifecycles and real-time monitoring of third-party vulnerabilities, is essential for maintaining a resilient security posture.

- **Convergence of IT and OT security gaps:** The convergence of IT and OT environments introduces unique security challenges, as OT systems often have different security requirements and vulnerabilities than traditional IT systems. Addressing these specific security gaps is crucial for ensuring the resilience of critical infrastructure and industrial operations.
- **Talent shortage and skills gap:** The persistent shortage of skilled cybersecurity professionals remains a significant impediment to building resilient security teams within U.S. enterprises. Talent shortage impacts an organization's ability to effectively implement and manage security controls, respond to incidents and maintain a proactive security posture necessary for resilience.
- **Complexity of security environments:** The increasing complexity of modern IT environments, encompassing on-premises, cloud, mobile and IoT/OT systems, poses a significant challenge to maintaining a unified and resilient security posture. Integrating disparate security tools and achieving comprehensive visibility across these environments are critical for effective threat detection and response, which are essential for resilience.

**Addressing enterprise challenges: The role of cybersecurity service providers**

Cybersecurity service providers are essential partners for U.S. enterprises in addressing the multifaceted challenges they face and enhancing their overall business resilience.

- **Strategic risk assessment and digital investment protection:** Cybersecurity service providers are moving beyond traditional security assessments to offer strategic risk assessment services that align with an enterprise's broad business objectives and digital transformation initiatives. They help organizations quantify cyber risks in business terms, translating technical vulnerabilities into potential impacts on revenue, operational continuity and brand reputation. This includes aligning security postures with industry-specific contexts and understanding unique industry trends, compliance requirements and -specific threats. Service providers are instrumental in demonstrating the ROI from protecting digital transformation investments and critical assets. For instance, they can help track KPIs such as reduced unscheduled downtime, improved customer trust scores and quick threat remediation times, directly linking cybersecurity investments to business outcomes and managing overall business risk. This strategic partnership ensures that security is not just a cost center but a driver of innovation and business growth.
- **Navigating complex regulatory and AI governance landscapes:** The increasingly complex and demanding regulatory landscape, particularly with the rising complexities from AI and GenAI deployments, can be a significant burden for enterprises. Cybersecurity service providers possess specialized knowledge of various regulations and compliance frameworks, such as HIPAA, PCI DSS and state privacy laws, while ensuring adherence. With the rapid adoption of AI, service providers are crucial in helping organizations establish robust AI governance frameworks, manage AI-related risks (such as data poisoning and model manipulation) and ensure compliance with emerging AI-specific regulations and guidelines such as the NIST AI Risk Management Framework. Such expertise is particularly valuable for organizations operating in highly regulated industries and those heavily investing in AI.
- **Providing effective and consolidated security solutions:** Beyond cost-effectiveness, there is an increasing

focus among service providers to help clients reduce tool sprawl and consolidate their security operations platforms. This consolidation leads to cost savings and improved operational efficiency as disparate tools are integrated into a more unified and manageable security ecosystem. Service providers are relying on shared infrastructure and expertise across multiple clients to deliver enterprise-grade security services, contributing to a resilient and manageable security posture.

- **Augmenting internal security teams and talent development:** Next-generation SOC and MDR providers effectively augment internal security teams, offering 24/7 monitoring, advanced threat detection and incident response capabilities, enhancing enterprises' ability to respond to and recover from incidents, thus improving resilience. Service providers also contribute to talent development by offering specialized training and upskilling programs, helping to bridge the industry's skills gap.

**The evolving landscape of Technical Security Services (2025)**

Technical Security Services in 2025 will be characterized by a significant increase in the adoption of analytics and automation-driven security implementations to enhance resilience. These technologies will streamline the deployment, configuration and management of security tools, improving efficiency and enabling rapid detection and response capabilities. ISG expects service providers to:

- Emphasize the integration and interoperability of security tools to provide a unified and resilient security ecosystem.
- Incorporate proactive threat hunting and continuous vulnerability management as central components of technical security service offerings, focusing on identifying and mitigating weaknesses before they can be exploited.
- Specialize in securing emerging technologies, such as IoT and OT environments, to meet the high demand for building resilient security controls in these complex areas as organizations expand their digital footprint.
- Extend their focus to CTEM, where technical services continuously identify, assess and mitigate risks across the attack surface, transitioning from periodic assessments to proactive, real-time risk management.

**The evolving landscape of Strategic Security Services (2025):**

In 2025, Strategic Security Services will be increasingly focused on enhancing business resilience in the face of evolving cyberthreats and accelerating digital transformation initiatives, particularly those involving AI. ISG anticipates a strong emphasis on:

- Integrating cybersecurity into the overall business strategy, with a focus on comprehensive cyber risk management and governance frameworks.
- Providing proactive, threat-informed advisory services, leveraging real-time intelligence to guide organizations in building resilient security strategies aligned with their specific risk profiles.
- Integrating security into digital transformation initiatives, especially those involving AI, ensuring that resilience is built into new technologies and business models from the outset.
- Prioritizing business resilience and continuity planning as core components of strategic security services, helping organizations develop robust plans to respond and recover from cyber incidents, ensuring minimal disruption to business operations.

**The evolving landscape of Next-Generation SOC/MDR services (2025):**

Next-generation SOC/MDR offerings in 2025 will be defined by significant advancements in threat intelligence, analytics and automation to enhance organizational resilience. These services will leverage enhanced threat intelligence, incorporating AI and ML for accurate and rapid threat detection and response. ISG anticipates traction with the following:

- Proactive threat hunting becoming a standard feature, with SOC analysts actively seeking out hidden threats using advanced techniques.
- Integrating deeper business context into SOC/MDR operations to enable the prioritization of threats based on their potential impact on critical assets and business operations, thereby supporting business resilience.
- Implementing automation and orchestration, powered by advanced analytics platforms, as essential components for rapid incident response, enabling quick containment and remediation of security incidents while minimizing disruption to business continuity.
- Shifting from reactive alert processing to assuming proactive security responsibility by leveraging AI to augment human analyst capabilities and improve overall security posture.

**Future outlook for 2025**

The U.S. cybersecurity market continues to present significant and evolving challenges for enterprises and service providers, demanding a strong focus on building resilience. The growing adoption of advanced solutions such as cloud security, MDR, zero trust, analytics and automation, AI for cybersecurity, and CTEM reflects a mature understanding of these challenges and a strategic shift toward enhancing cyber and business resilience.

In 2025, the emphasis on digital transformation, particularly AI initiatives, will further shape the cybersecurity landscape. To navigate this evolving landscape effectively, U.S. enterprises must prioritize building a resilient security posture that integrates people, processes and technology. Boards and executives should recognize AI-related risk, governance and compliance as cybersecurity imperatives and invest strategically in security to safeguard their AI and broad digital investments. Leveraging the expertise of cybersecurity service providers will be crucial for augmenting internal teams, accessing specialized skills and ensuring compliance.

Continuous learning, adaptation and a proactive security mindset focused on resilience will be paramount for mitigating risks and ensuring business continuity amid an ever-changing cyberthreat environment. Service providers must continue to innovate and adapt their offerings to meet the increasingly sophisticated needs of enterprises, delivering cutting-edge solutions and expertise to help them build and maintain resilience against sophisticated threats.

> Service providers are becoming imperative partners in quantifying cyber risks in business terms, aligning security investments with core business objectives and industry-specific contexts. Their expertise facilitates clear ROI demonstration from protecting digital transformation investments and assets, ultimately enhancing overall business risk management.

*Report Author:*
*Bhuvaneshwari Mohan (Global - IAM)*

**AI-driven capabilities, zero trust and seamless UX are integral to IAM**

The need for robust identity and access management (IAM) has become critical due to escalating cyberthreats, the expansion of hybrid work models and the widespread adoption of cloud technologies. IAM provides the foundation for secure operations, enabling organizations to innovate while meeting rigorous regulatory requirements.

**Strategic importance of IAM for enterprises:** IAM is foundational to building a resilient security posture that adapts to evolving threats and business demands and significantly strengthens security by reducing the risks of unauthorized access and data breaches. Key security measures such as adaptive and context-aware access controls, continuous identity risk assessments and zero trust architectures form the backbone of these efforts. Adaptive access controls leverage real-time analytics to identify and address unusual behavior effectively. Adopting zero trust frameworks within IAM systems is becoming a standard for securing access, regardless of the user's location or device. The cornerstone of zero trust is rigorous identity verification and access control; therefore, enterprises need robust authentication mechanisms.

In addition to enhancing security, IAM facilitates compliance with regulatory standards such as GDPR, HIPAA, CCPA, SOX and PCI DSS through real-time audit trails and automated user access provisioning. These capabilities prevent unauthorized access by providing visibility into user activity and safeguarding sensitive data. IAM also simplifies the adherence to complex regulations, allowing enterprises to focus on their core operations.

The IAM landscape is transforming significantly, driven by the need for secure, seamless identity solutions and evolving organizational needs. Below are the key IAM-related trends that ISG observed:

> As an identity-centric approach taking **centre stage**, IAM has become a **strategic necessity**.

**Emergence of decentralized identities:** One of the most promising developments is the rise of decentralized identity models, which leverage blockchain technology to empower users to control their digital identities, enabling consent-driven authentication and privacy. Both verifiable credentials and decentralized identifiers are essential standards for decentralized identities. Customer identity and access management (CIAM) is gaining increased relevance with the rise of decentralized identities due to the evolving focus on privacy, security and user-centric control over personal data.

**Growth of identity as a service (IDaaS):** The rapid growth of IDaaS underscores the broad enterprise shift toward cloud-first architectures. IAM vendors are enhancing their IDaaS platforms to integrate seamlessly with SaaS applications and multicloud and hybrid cloud infrastructures. This trend enables organizations to achieve greater agility, scalability and security while adapting quickly to dynamic business and workforce demands.

**Market consolidation and strategic acquisitions:** The ongoing consolidation in the IAM market reflects a strategic effort by vendors to integrate advanced technologies and expand their product capabilities. For instance, Microsoft's sustained investments in this space reshape the competitive landscape. While these developments drive innovation, they also increase dependency on a few dominant players.

**Adoption of biometric authentication and passwordless access:** Enterprises are increasingly adopting biometric authentication and passwordless access to enhance security and UX. These methods, including facial recognition, fingerprint scanning and FIDO2-based keys, reduce dependency on passwords, mitigate phishing risks and align with zero trust principles for strong identity assurance.

**Industry-specific IAM solutions:** The unique requirements of different industries necessitate tailored IAM solutions. Healthcare organizations must comply with HIPAA while securing electronic health records (EHRs), utilizing granular access controls and secure telemedicine platforms. Financial services need to adhere to SOX and PCI DSS standards by implementing robust measures, such as behavioral analytics and multifactor authentication (MFA), to prevent fraud and ensure data integrity. Retailers require scalable IAM solutions to protect customer data and manage workforce access efficiently during peak periods.

**Technological advancements and product innovations:** The IAM market continues to evolve, with innovations such as AI-driven identity analytics, context-aware authentication and deep integrations with cloud platforms. AI and ML play a vital role in IAM solutions, analyzing and detecting unusual user behavior and automatically adjusting access controls based on real-time information. These advancements enhance the ability of IAM systems to detect anomalies, adjust access decisions dynamically, and support hybrid cloud and multicloud environments. Identity and threat detection and response (ITDR) solutions are emerging as an important aspect of IAM as they focus on proactive threat detection, real-time monitoring and anomaly detection to address identity-centric attacks effectively.

### Challenges in implementing IAM

Integration complexities often arise when organizations attempt to align IAM with legacy systems, cloud platforms and third-party applications. These technical hurdles frequently demand specialized expertise and extended implementation timelines. The rapidly evolving threat landscape and the need for enhanced UX without compromising security further complicate IAM implementation.

Enterprises must thoroughly evaluate criteria such as the ability to provide seamless integration, enhanced end UX, product effectiveness, and improved cost and licensing models to ensure the selected IAM vendor aligns with their security needs, business goals and compliance requirements.

As AI is increasingly incorporated into identity security, it also poses many threats, such as AI model poisoning, model theft and synthetic identities. Therefore, AI-enhanced IAM systems should consider following zero trust principles, strengthening IAM configurations, regularly auditing and testing AI models, and maintaining a hybrid approach using AI for assistance while maintaining human oversight in decision-making.

The IAM market is set for growth driven by rising cyberthreats, regulatory pressures and digital transformation. Investment in decentralized identity models, IDaaS and AI-driven solutions will likely accelerate. Opportunities lie in developing industry-specific solutions that address unique regulatory and operational requirements. Evolving real-time adaptive security measures, identity governance and compliance management will prioritize UX.

IAM serves as a strategic enabler that supports compliance, drives innovation and enhances UX. As the digital landscape evolves, investment in advanced IAM solutions will be crucial for organizations aiming to secure their operations and grow in an interconnected world.

This report examines the strategic significance of IAM for organizations across all sizes, highlights key IAM vendors and their capabilities from a global perspective and offers a detailed overview of the market landscape.

Identity solutions of hyperscalers such as AWS and Google Cloud are excluded from this assessment as they are designed primarily for securing their own cloud ecosystems and are not sold as standalone offerings.

> At the core of zero trust lies rigorous identity verification and strict access control, emphasizing continuous, risk-based authentication. Enterprises must go beyond traditional methods by adopting passwordless solutions, biometric authentication and behavioral analytics. Real-time, context-aware risk assessments ensure dynamic access, making identity security proactive rather than reactive, which is critical in today’s evolving threat landscape.

*Report Author: Gowtham Sampath (Global - XDR)*

### XDR addresses complex IT environments and talent shortages with enhanced visibility and automation

The extended detection and response (XDR) market is rapidly maturing, driven by enterprise demand for consolidated, intelligence-led security operations. In response to the increasing sophistication of cyberthreats, organizations are shifting from siloed detection tools to unified platforms that deliver comprehensive visibility, automation and contextual analytics across endpoints, networks, cloud workloads and identities. XDR has evolved from a niche extension of endpoint detection and response (EDR) into a core component of modern security operations center strategies, enabling proactive threat hunting, rapid containment and coordinated response across the attack surface.

At the core of this transformation is the pervasive adoption of AI, ML and behavioral analytics, which now power many detection, correlation and prioritization engines within XDR platforms. These technologies reduce false positives and allow for early-stage anomaly detection and advanced threat modeling. The growing integration of cloud-native security and zero trust frameworks reflects the market's recognition that security perimeters are dynamic and identity-driven. XDR platforms increasingly align with MITRE ATT&CK and support Continuous Threat Exposure Management (CTEM) and automation-first response models.

Key trends and developments

- **Emergence of agentic AI:** The integration of agentic AI (autonomous, goal-driven systems) is revolutionizing XDR platforms. These AI agents can independently detect, investigate and respond to threats, reducing reliance on human intervention and enhancing response times.
- **Shift toward open and modular architectures:** Organizations are demanding XDR solutions that offer open architectures, allowing seamless integration with existing

XDR's evolution **unifies defenses**, driving **proactive, intelligent** cyber **resilience**.

security tools and third-party applications. This modular approach enhances flexibility and ensures comprehensive threat visibility across diverse environments.

- **Integration of behavioral analytics for insider threat detection:** Advanced behavioral analytics are being employed to detect insider threats by monitoring deviations from typical user behavior. This proactive approach enables early identification of potential security breaches originating from within the organization.
- **Adoption of CTEM:** XDR platforms are incorporating CTEM to provide real-time assessments of an organization's security posture. Organizations can prioritize remediation efforts by evaluating vulnerabilities and potential attack vectors.
- **Expansion into operational technology (OT):** XDR solutions are extending their capabilities to secure OT environments, addressing the unique challenges of industrial systems and critical infrastructure. This expansion ensures comprehensive protection across both IT and OT domains.
- **Integration of knowledge graphs:** XDR platforms are leveraging knowledge graphs to map relationships between various entities within an organization. This integration provides context-rich threat intelligence, improving the accuracy of threat detection and response strategies.
- **AI-driven insider risk management (IRM):** Advanced IRM systems powered by AI are being integrated into XDR platforms to proactively identify and mitigate insider threats. These systems utilize adaptive scoring and real-time policy enforcement to enhance organizational security.
- **Focus on proactive defense mechanisms:** The XDR market is experiencing a shift from reactive to proactive defense strategies. By anticipating potential threats and vulnerabilities, organizations can implement measures to prevent security incidents before they occur.

These trends underscore the dynamic evolution of the XDR landscape, highlighting the importance of adaptability, integration and proactive strategies in modern cybersecurity frameworks.

Looking forward, in the second half of 2025, vendors in the XDR market are expected to deepen their focus on open architectures, third-party integrations and AI-assisted analyst augmentation. Future-ready XDR platforms will detect and respond to known threats and act as decision-support engines capable of autonomous investigation, real-time risk scoring and adaptive policy enforcement. As cyberattacks become increasingly dynamic and multistage, XDR is poised to become the operational nerve center of enterprise cybersecurity.

XDR is fundamentally transforming cyber defense by shifting from reactive to proactive security. This profound evolution is powered by advanced AI and ML, enabling predictive capabilities to anticipate and block attacks before they escalate. XDR moves beyond mere detection to prevent breaches by integrating identity data and comprehensive threat intelligence.

*Report Author: Yash Jethani (Global - SSE)*

## Zero trust SSE architecture uses AI to evolve, with continuous authentication and strict access controls

### Why you need zero trust principles

In today's digital landscape, traditional security perimeters are obsolete. Zero trust architecture provides continuous authentication and strict access controls essential for secure remote work and cloud environments. Verifying every user and device before granting access, organizations can significantly reduce breach risks and protect sensitive data from external attackers and insider threats.

Zero trust architecture operates on the *never trust, always verify* principle, requiring continuous authentication regardless of location. Modern cybersecurity measures strengthen this approach by:

- **AI and ML:** Enhances zero trust by continuously monitoring user behavior patterns and automatically identifying anomalies that suggest compromised credentials
- **Ransomware defense:** Supports zero trust by isolating potential threats and preventing lateral movement within networks, limiting damage scope
- **Cloud security:** Extends zero trust principles to distributed environments through CASB tools that enforce consistent access policies across all applications
- **IoT protection:** Applies zero trust microsegmentation to connected devices, preventing compromised devices from accessing critical systems
- **Critical infrastructure security:** Implements zero trust measures to create secure operational zones with strict verification for accessing control systems
- **Data privacy:** Aligns with zero trust's least-privilege access controls to ensure regulatory compliance and protect sensitive information

Providers are aligning SSE with enterprise needs for **agility, integration** and **a unified SASE**.

- **Emerging technologies:** Strengthens zero trust authentication through quantum-resistant encryption and blockchain-verified identity management.

A robust cybersecurity strategy integrates these elements within a zero trust framework, creating multiple verification layers that protect against sophisticated threats.

Security service edge (SSE) is a fundamental component that enables zero trust principles in modern network environments. SSE delivers cloud-based security functions that enforce zero trust by:

- **Identity-based access control:** SSE validates user identity before granting access to applications, aligning with zero trust's *never trust, always verify* principle.
- **Continuous verification:** SSE continuously monitors sessions after initial authentication, detecting behavioral anomalies that might indicate a security compromise.
- **Policy enforcement point:** SSE serves as a cloud-delivered control point where zero trust policies are consistently applied across all users, locations and devices. Legacy VPN replacement reduces the attack surface with a more secure remote access solution.
- **Application-level controls:** Rather than securing network segments, SSE secures access to specific applications, supporting zero trust's focus on protecting resources rather than networks. ZTNA provides zero trust access to private applications, replacing VPNs while CASB secures connectivity to SaaS apps, preventing data loss and cyberattacks, and secure collaboration enables the safe sharing of confidential information.
- **Inspection and threat prevention:** SSE provides deep inspection of encrypted traffic, detecting and blocking threats that might exploit trusted connections. Secure web gateway (SWG) enables secure internet access with advanced threat prevention while DEM monitors device, application and network performance for rapid issue resolution.
- **Data protection integration:** SSE incorporates data loss prevention (DLP) and cloud access security broker (CASB) capabilities to prevent sensitive data exfiltration, supporting zero trust data security requirements. GenAI DLP prevents sensitive data sharing with GenAI, while AI-enabled DLP uses intelligent policies to control and protect sensitive data.
- **Sensitive information management:** SSE discovers, assesses and protects sensitive data in real time, while continuous zero trust access consistently authorizes user and device access.

SSE provides the cloud-delivered security stack to implement zero trust principles at scale across distributed environments. It replaces traditional perimeter security with a flexible, identity-centric approach to secure remote work, cloud adoption and mobile access scenarios without sacrificing protection or visibility.

SSE serves a diverse range of customers, including end enterprises, cloud service providers (CSPs) delivering cloud services, network service providers (NSPs) offering network connectivity, and managed service providers (MSPs) providing outsourced IT and security. Large enterprises, characterized by extensive IT teams and infrastructure and small and midsize businesses (SMBs), often constrained by resources, also represent key customer segments. Understanding these distinct profiles is crucial for SSE vendors and organizations alike in tailoring solutions and adoption strategies.

**Components and functions of SSE, SLA compliance expansion and road map for 2025 and 2026:**

**SSE components can be broken into four major buckets:**

- CNAPP: Combines cloud security tools (CSPM, CIEM, CWP) for streamlined, scalable cloud protection — a key part of SSE
- Digital ecosystem exposure management: Identifies and mitigates risks across interconnected digital assets (cloud, IoT, BYOD), which is crucial for expanding digital footprints and being a differentiator for SSE vendors

## 2025 SLAs

Enhanced AI-driven monitoring tools for **predictive analytics** in SLA compliance

Expansion of SLA KPIs to include **IoT-specific metrics** as edge computing adoption grows

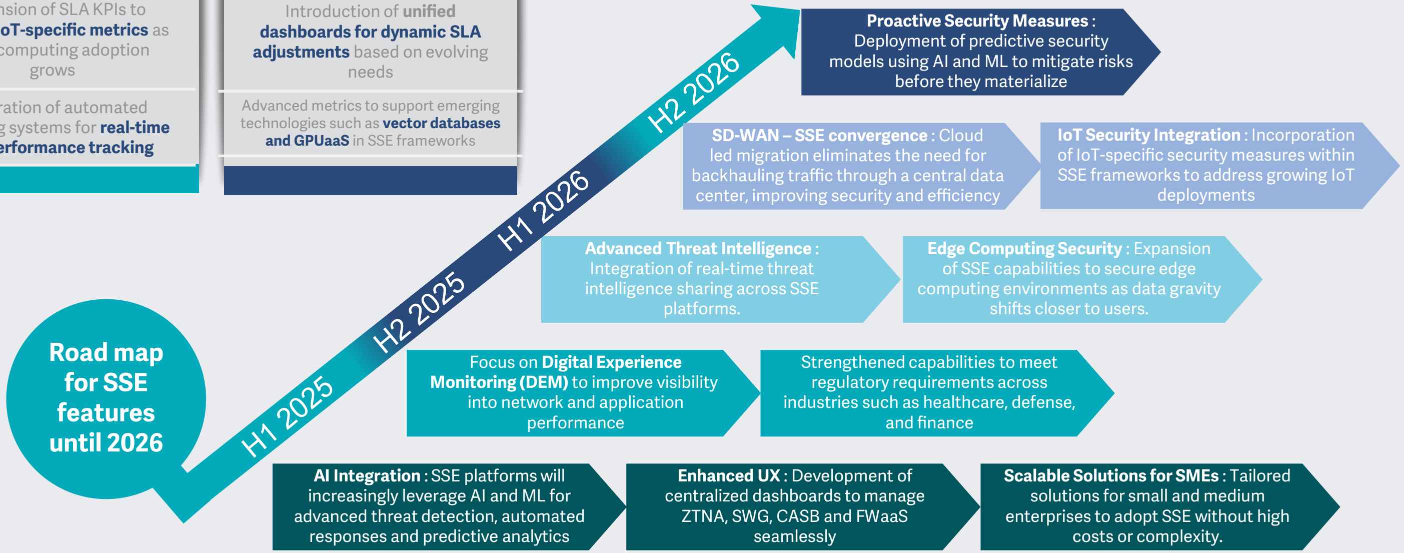
Integration of automated reporting systems for **real-time SLA performance tracking**

## 2026 SLAs

Development of **proactive SLA** models using AI and ML to predict potential service disruptions

Introduction of **unified dashboards for dynamic SLA adjustments** based on evolving needs

Advanced metrics to support emerging technologies such as **vector databases and GPUaaS** in SSE frameworks



**Road map for SSE features until 2026**

**AI Integration** : SSE platforms will increasingly leverage AI and ML for advanced threat detection, automated responses and predictive analytics

**Enhanced UX** : Development of centralized dashboards to manage ZTNA, SWG, CASB and FWaaS seamlessly

**Scalable Solutions for SMEs** : Tailored solutions for small and medium enterprises to adopt SSE without high costs or complexity.

Focus on **Digital Experience Monitoring (DEM)** to improve visibility into network and application performance

Strengthened capabilities to meet regulatory requirements across industries such as healthcare, defense, and finance

**Advanced Threat Intelligence** : Integration of real-time threat intelligence sharing across SSE platforms.

**Edge Computing Security** : Expansion of SSE capabilities to secure edge computing environments as data gravity shifts closer to users.

**SD-WAN – SSE convergence** : Cloud led migration eliminates the need for backhauling traffic through a central data center, improving security and efficiency

**IoT Security Integration** : Incorporation of IoT-specific security measures within SSE frameworks to address growing IoT deployments

**Proactive Security Measures** : Deployment of predictive security models using AI and ML to mitigate risks before they materialize

Source: ISG, 2025

- Next-generation deep packet inspection (DPI): Uses advanced techniques such as ML to analyze encrypted traffic and detect sophisticated threats in cloud environments, enhancing visibility for CASB, SWG and ZTNA within SSE
- UEBA: Employs analytics and ML to detect abnormal user and entity behavior indicative of insider threats or attacks, increasingly integrated into SSE for advanced threat detection

Increasingly, SSE vendors offer platforms that integrate multiple functions and components. This platform offers comprehensive cloud-native security through a single architecture. It provides the ability to inspect encrypted traffic at scale and features an inline proxy for cloud and web traffic. Core security functions include a full-port firewall with intrusion protection (FWaaS), API-based data security for cloud services (CASB) and continuous security assessment for public cloud infrastructure (CSPM). Advanced data loss protection is usually included for data in transit and at rest, alongside advanced threat protection (ATP) leveraging AI and ML, UEBA and sandboxing. The platform integrates threat intelligence with other security tools (EPP/EDR, SIEM, SOAR), provides data loss from GenAI systems and offers zero trust network access (ZTNA) to replace legacy VPNs and finally enables secure collaboration via email and collaboration tools. It can also feature a software-defined perimeter with zero trust access (SD-WAN/SDP) and a global, scalable network infrastructure with optimizations for SaaS performance.

By 2026, as per the figure above, ISG expects the SSE components and functions to evolve to include IoT security, proactive edge healing and solutions tailored for SMEs.

**Technology trends in SSE:**

- SSE solutions increasingly adopt zero trust principles, moving away from VPN-based remote access to identity-driven security. ZTNA remains foundational to SSE, ensuring that only authorized users and devices access resources, driven by the need to secure remote work and cloud environments.
- Providers and product vendors are embedding ML and AI-driven threat detection for anomaly detection, automated remediation and real-time policy enforcement.
- As enterprises prefer cloud-native SSE over legacy appliance-based security, full cloud-native architecture now supports distributed workforces and multicloud adoption. Cloud-native SSE platforms are scaling to handle massive traffic volumes, supporting digital transformation with flexible, scalable security for hybrid IT environments.
- SSE solutions prioritize low latency and minimal downtime to match consumer-grade application experiences, addressing the demands of a distributed workforce without compromising security.
- SSE platforms are deeply integrated with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) for better threat visibility and response. On the other hand, Autonomous Digital Experience Management/Monitoring (ADEM) is being integrated into SSE to monitor end-user performance and security, using AI for predictive analytics and troubleshooting.
- DLP, encryption and adaptive access controls are becoming standard features that address increasing compliance needs.
- Integration with IAM and SSE (SSO/MFA) is now seen as commonplace to enforce stronger authentication policies.

**Business trends in SSE:**

- Many enterprises adopt SSE first and integrate SD-WAN later for a complete SASE deployment. However, this is likely a two-way trend as many enterprises adopt networking solutions and then migrate to SASE by layering on SSE features. Hence, the line between SSE and secure access service edge (SASE) continues to blur as providers offer unified platforms combining networking (SD-WAN) and security (ZTNA, SWG, CASB, FWaaS) features, catering to hybrid and distributed workforces.

- With VPN limitations, SSE is replacing traditional remote access solutions as remote and hybrid work drives SSE demand. Enterprises are increasingly adopting secure browsers as a critical first line of defense against browser-based threats, driven by the shift to cloud-based work and remote access. Given the growing reliance on web applications, this is seen as a necessity.
- SSE platforms are leveraging AI and ML for real-time threat detection, behavioral monitoring and automated responses, reducing manual intervention and enhancing proactive security.
- Enterprises are moving toward OpEx models instead of traditional CapEx-heavy hardware investments, thus favoring a shift to subscription-based security (Security-as-a-service).
- Enterprises prefer fewer providers that provide end-to-end SSE solutions instead of managing multiple security tools. This drives the consolidation of the vendor landscape, favoring single-vendor strategies, particularly for small and midsize enterprises.
- Industries such as finance, healthcare and government are embracing SSE to meet strict data protection and access control regulations.

**Recent acquisitions in the zero trust or SSE space:**

- **Cloudflare:** In February 2025, Cloudfare acquired BastionZero to enhance its zero trust infrastructure access controls, expanding the capabilities of Cloudflare One, its SASE platform. It also acquired Area 1 Security in 2022, enhancing email security within its SSE offering.
- **Zscaler:** In October 2024, Zscaler acquired network segmentation startup Airgap Networks to strengthen its zero trust security offerings. In March 2024, it purchased Israeli data security startup Avalor to enhance its AI-driven data protection capabilities. In February 2024, Zscaler acquired another Israeli application security company Canonic Security, to bolster its defenses against SaaS-based threats. In May 2021, it had acquired Smokescreen to add deception technology and enhance threat detection.
- **Hewlett Packard Enterprise (HPE):** In March 2023, HPE acquired Axis Security, a cloud-native SSE vendor. This acquisition bolstered HPE's edge-to-cloud security capabilities by integrating Axis Security into its Aruba networking platform, creating a unified SASE solution.
- **Netskope:** In June 2022, Netskope acquired WootCloud, an innovator in applying zero trust principles to IoT security, extending its zero trust capabilities to enterprise IoT. It also acquired Infiot in 2022, strengthening its zero trust and SD-WAN capabilities.
- **Palo Alto Networks:** The company acquired CloudGenix in 2020, integrating SD-WAN and SSE to create a full SASE stack. The move highlights the trend among enterprises toward single-vendor SSE/SASE platforms, which simplify deployment and management while avoiding the complexities associated with multivendor setups.
- **Check Point:** In September 2023, it completed its acquisition of Perimeter 81 to strengthen its SASE capabilities. Managed through a user-friendly cloud console, Perimeter 81's capabilities ensure reliable connectivity via a global backbone network, while its SWG protects against web-borne threats.
- **SonicWall:** In January 2024, SonicWall acquired Banyan Security, a cloud platform focused on identity-centric SSE, to extend its security capabilities to cloud and hybrid environments, remote workers and BYOD scenarios. Banyan Security's framework assessed device posture to guarantee secure access and included a SWG to defend against internet-based threats. Additionally, it offered VPN as a service (VPNaaS) for modern, secure network access.

SSE provides cloud-based security services such as SWG and ZTNA, making it easier for distributed workforces to interact securely from a distance. Enterprises must also adhere to changing legal standards, which calls for strong security measures to protect corporate and personal data. Various industries are adopting SSE solutions because they facilitate compliance efforts through centralized security policies, real-time threat monitoring and data loss prevention. The blurred lines between

SSE and Secure Access Service Edge (SASE) indicate a compelling trend where enterprises can seamlessly adopt comprehensive security and networking solutions tailored for hybrid and distributed workforces. As organizations continue to navigate a landscape shaped by remote operations and stringent compliance requirements, the SSE market is poised for growth, becoming an essential component of organizational strategy and operational resilience in the digital era.

For effective SSE deployment, organizations should adopt several key strategies. This includes minimizing reliance on legacy security hardware by leveraging SSE's integrated features and implementing zero trust principles through ZTNA for robust access control. Consolidating disparate security tools onto a unified SSE platform streamlines management while embracing hybrid and cloud-ready SSE architectures ensures flexibility. A phased rollout, starting with critical areas such as ZTNA, allows for gradual and strategic adoption. Furthermore, prioritizing the security of remote work environments and ensuring a positive UX with DEM is vital. Ultimately, strategic budget allocation toward SSE investments that address key risks will drive the most impactful security outcomes, and the CIOs and line of business heads need to converge on their own security budgets.

> Enterprises seek scalable, high-performance solutions with seamless integration, unified management and a clear path to full SASE for future-ready security. While providers indicate a shift toward agile, unified and performance-oriented security frameworks, the ultimate aim is to deliver a truly frictionless and comprehensive security experience across any user, device, and location.

## Provider Positioning

**Page 1 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Accenture | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Aryaka | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Atos | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Avertium | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger |
| Beta Systems | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| BeyondTrust | Rising Star ★ | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Bitdefender | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| BlackBerry (Arctic Wolf) | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| BlueVoyant | Not In | Not In | Not In | Not In | Contender | Not In | Product Challenger | Not In | Product Challenger |

# Provider Positioning

Page 2 of 13

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Broadcom | Leader | Leader | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| BT | Not In | Not In | Not In | Product Challenger | Not In | Contender | Not In | Contender | Not In |
| Capgemini | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Cato Networks | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| CDW | Not In | Not In | Not In | Market Challenger | Not In | Market Challenger | Not In | Market Challenger | Not In |
| CGI | Not In | Not In | Not In | Market Challenger | Not In | Market Challenger | Not In | Market Challenger | Not In |
| Check Point Software | Not In | Product Challenger | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Cisco | Not In | Market Challenger | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Cloudflare | Not In | Not In | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In |

# Provider Positioning

Page 3 of 13

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Cognizant | Not In | Not In | Not In | Contender | Not In | Product Challenger | Not In | Product Challenger | Not In |
| Computacenter | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Contender | Not In |
| Critical Start | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Leader |
| Cross Identity | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| CrowdStrike | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| CyberArk | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Cybereason | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| CyberProof | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| CyberSecOp | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger | Not In | Contender |

# Provider Positioning

**Page 4 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Cyderes | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Leader |
| Deloitte | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| DXC Technology | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| Entrust | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Ericom Software | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| ESET | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Evidian IAM (Eviden) | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| EY | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Fischer Identity | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

# Provider Positioning

Page 5 of 13

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Forcepoint | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Fortinet | Market Challenger | Leader | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Fortra | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Fujitsu | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Contender | Not In |
| FusionAuth | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Globant | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Contender | Not In |
| Gopher Security | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| GTT | Not In | Not In | Not In | Not In | Market Challenger | Not In | Market Challenger | Not In | Market Challenger |
| Happiest Minds | Not In | Not In | Not In | Not In | Product Challenger | Not In | Contender | Not In | Contender |

# Provider Positioning

**Page 6 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| HCLTech | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| HPE (Aruba) | Not In | Not In | Rising Star ★ | Not In | Not In | Not In | Not In | Not In | Not In |
| IBM | Leader | Leader | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| iboss | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Imprivata | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Infosys | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Innova Solutions | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In | Product Challenger |
| Inspira | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Contender |
| JumpCloud | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

## Provider Positioning

Page 7 of 13

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Kaspersky | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| KPMG | Not In | Not In | Not In | Product Challenger | Not In | Leader | Not In | Product Challenger | Not In |
| Kroll | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Leader | Not In |
| Kudelski Security | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| Kyndryl | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| LMNTRIX | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Lookout | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| LTIMindtree | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| Lumen Technologies | Not In | Not In | Not In | Market Challenger | Not In | Contender | Not In | Contender | Not In |

# Provider Positioning

**Page 8 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| ManageEngine | Leader | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Menlo Security | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Microland | Not In | Not In | Not In | Not In | Leader | Not In | Rising Star ★ | Not In | Leader |
| Microsoft | Leader | Leader | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Mphasis | Not In | Not In | Not In | Not In | Rising Star ★ | Not In | Leader | Not In | Product Challenger |
| NCC Group | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| Netskope | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| NTT DATA | Not In | Not In | Not In | Rising Star ★ | Not In | Rising Star ★ | Not In | Rising Star ★ | Not In |
| Okta | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

## Provider Positioning

**Page 9 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| One Identity (OneLogin) | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Open Systems | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| OpenText | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Optiv | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| Orange Cyberdefense | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| Palo Alto Networks | Not In | Leader | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Persistent Systems | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Rising Star ★ |
| Ping Identity | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Presidio | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger |

# Provider Positioning

Page 10 of 13

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Proficio | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Leader |
| Proofpoint | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| PurpleSec | Not In | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Product Challenger |
| PwC | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Rackspace Technology | Not In | Not In | Not In | Product Challenger | Leader | Product Challenger | Leader | Product Challenger | Leader |
| Rapid7 | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| RSA | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| SailPoint | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Saviynt | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

## Provider Positioning

**Page 11 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| SecureAuth | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Secureworks | Not In | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In |
| SecurityHQ | Not In | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Product Challenger |
| SenseOn | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| SentinelOne | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Seqrite | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Sequretek | Contender | Contender | Not In | Not In | Not In | Not In | Contender | Not In | Contender |
| Skyhigh Security | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| SLK Software | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger |

# Provider Positioning

**Page 12 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| SonicWall (Banyan Security) | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Sophos | Not In | Rising Star ★ | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Stefanini | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Contender |
| Syntax | Not In | Not In | Not In | Not In | Contender | Not In | Contender | Not In | Not In |
| TCS | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Tech Mahindra | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| TEHTRIS | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Thales | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Trellix | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

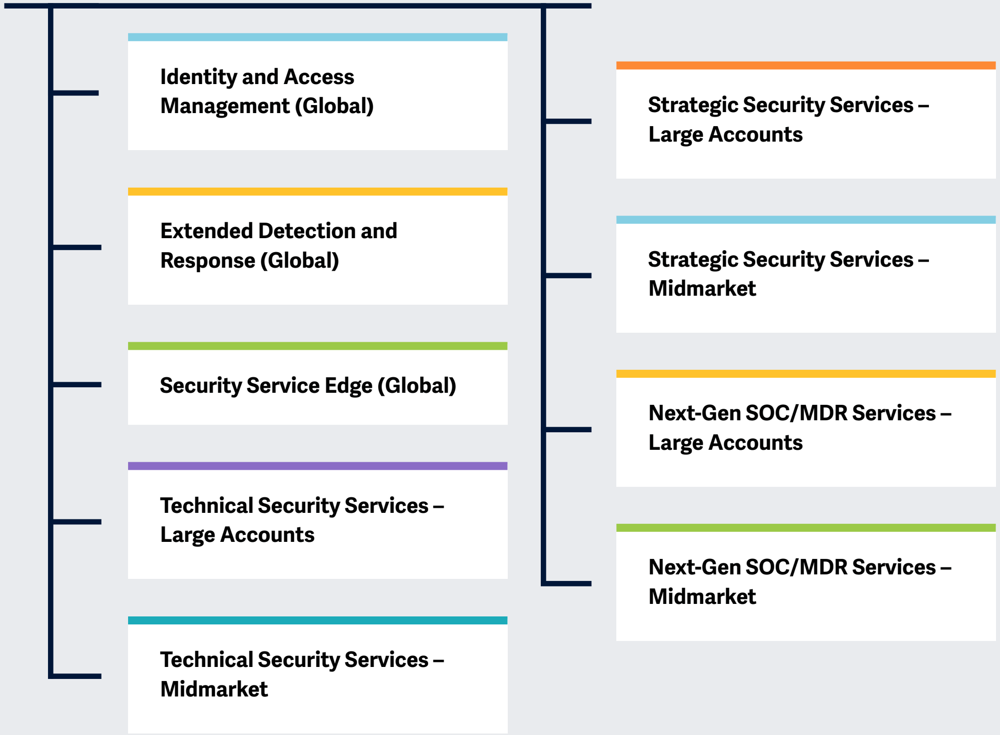
## Provider Positioning

**Page 13 of 13**

| | Identity and Access Management (Global) | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services – Large Accounts | Technical Security Services – Midmarket | Strategic Security Services – Large Accounts | Strategic Security Services – Midmarket | Next-Gen SOC/ MDR Services – Large Accounts | Next-Gen SOC/ MDR Services – Midmarket |
|---|---|---|---|---|---|---|---|---|---|
| Trend Micro | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Trustwave | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| Unisys | Not In | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader |
| Verizon Business | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger | Not In |
| Versa Networks | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Wipro | Not In | Not In | Not In | Leader | Not In | Leader | Not In | Leader | Not In |
| Zensar Technologies | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Not In | Product Challenger |
| Zscaler | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |

# Key focus areas for Cybersecurity – Services and Solutions 2025.

Simplified Illustration Source: ISG 2025



Identity and Access Management (Global)

Extended Detection and Response (Global)

Security Service Edge (Global)

Technical Security Services – Large Accounts

Technical Security Services – Midmarket

Strategic Security Services – Large Accounts

Strategic Security Services – Midmarket

Next-Gen SOC/MDR Services – Large Accounts

Next-Gen SOC/MDR Services – Midmarket

## Definition

In the era of rapid technological advancements and AI integration into daily operations, the cybersecurity landscape has become increasingly complex and multifaceted. Regulatory requirements such as the Network and Information Security (NIS) 2 Directive in the European Union are elevating the demand for robust cybersecurity measures, compelling organizations to reassess their security frameworks amidst emerging threats. Simultaneously, the commoditization of hacking tools has significantly reduced entry barriers for malicious actors, resulting in a surge of cybercriminal activities and a corresponding escalation of risks.

The proliferation of technology has expanded the attack surface, posing critical challenges for organizations as they navigate between OT and IT. The scarcity of skilled cybersecurity personnel has amplified this complexity, spurring accelerated demand for managed security services as companies seek external expertise to fortify their defenses.

Continued AI development presents risks and opportunities in the cybersecurity space. Security service providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats and understanding the transformative impact of new technologies such as quantum computing. In response to these challenges, businesses are increasingly investing in solutions such as identity and access management (IAM), data loss prevention (DLP), extended detection and response (XDR), and security service edge (SSE), combining advanced tools and human expertise with behavioral and contextual intelligence to enhance their security posture.

## Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following nine quadrants: Identity and Access Management (Global), Extended Detection and Response (Global), Security Service Edge (Global), Technical Security Services – Large Accounts, Technical Security Services – Midmarket, Strategic Security Services – Large Accounts, Strategic Security Services – Midmarket, Next-Gen SOC/MDR Services – Large Accounts and Next-Gen SOC/MDR Services – Midmarket.

This ISG Provider Lens™ study offers IT decision-makers:

- Transparency on the strengths and weaknesses of relevant providers/software vendors
- A differentiated positioning of providers by segments (quadrants)
- Focus on the regional market

This ISG Provider Lens™ study offers IT-decision makers: Our study serves as the basis for important decision-making in terms of positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing provider.

## Provider Classifications

The provider position reflects the suitability of providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the service requirements from enterprise customers differ and the spectrum of providers operating in the local market is sufficiently wide, a further differentiation of the providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).

## Provider Classifications: Quadrant Key

**Product Challengers** offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

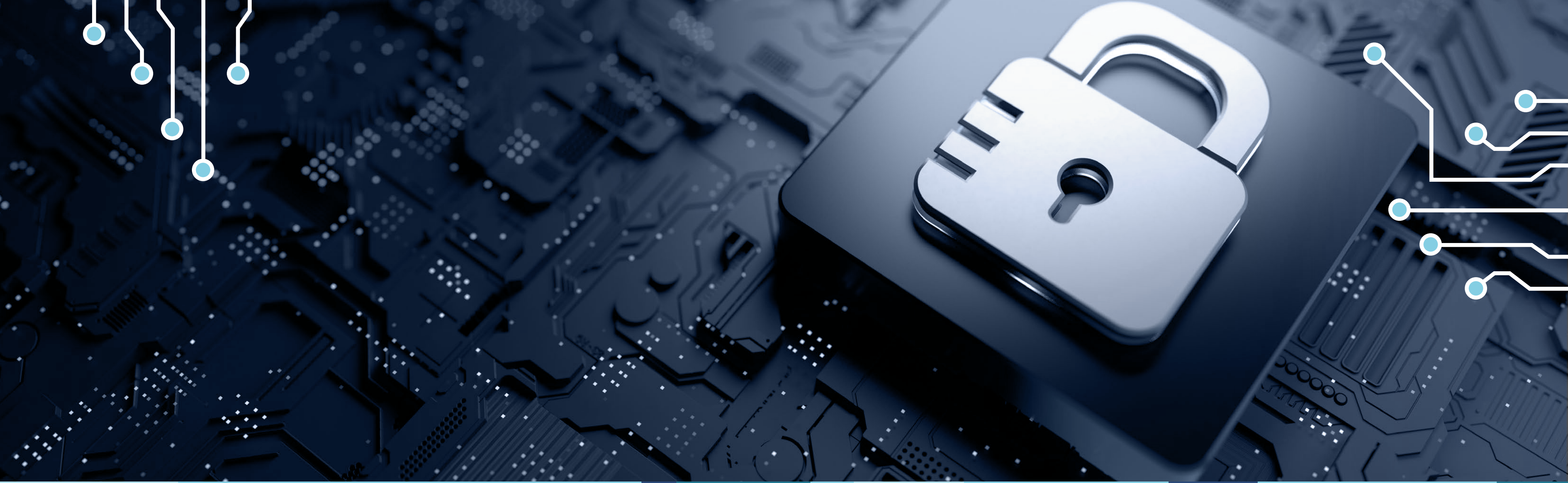
**Leaders** have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

**Contenders** offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/ services and follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

**Market Challengers** have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

**Not in** means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.



# Identity and Access Management (Global)

## Who Should Read This Section

This report is valuable for vendors offering **identity and access management (IAM)** solutions **globally** to understand their market position and for enterprises looking to evaluate these vendors. In this quadrant, ISG highlights the current market positioning of these vendors based on the depth of their capabilities and market presence. The report outlines the key IAM challenges, including securing identities in hybrid IT environments, enabling seamless access and combating advanced threats, emphasizing the need for adaptive authentication, zero trust and unified identity solutions for agility.

### Technology professionals

Should read this report to understand vendors' integration capabilities to reduce threat impact, where they use advanced technologies to transform legacy systems.

### Security and data professionals

Should read this report to gain insights into the way vendors comply with security and data protection regulations and stay updated with market trends.

### Business professionals

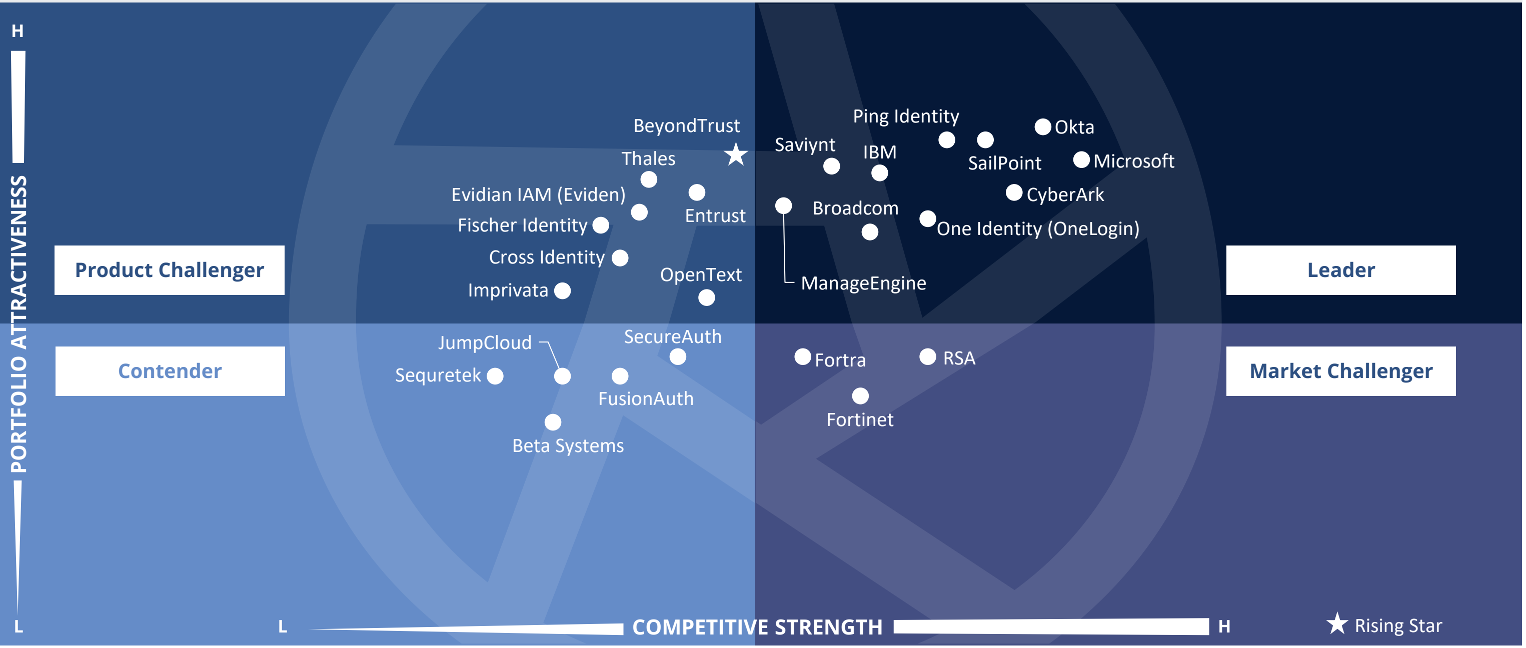
Should read this report to balance data security, CX and privacy in the current business environment, which prioritizes digital transformation.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Identity and Access Management

Global 2025



The quadrant examines IAM vendors that excel in deploying **adaptive identity solutions**. Essential features include **real-time access controls** for **zero trust security**, along with a **user-friendly interface** and compliance with **regulatory requirements**.

*Bhuvaneshwari Mohan*

### Definition

IAM solution providers assessed in this quadrant are distinguished by their proprietary software, including SaaS, and services for managing enterprise user identities. It excludes pure service providers that do not offer an IAM product, either on-premises or cloud-based, developed with proprietary software. Depending on organizational needs, these solutions can be deployed on-premises, in customer-managed clouds, as as-a-service models or as a combination of these options.

IAM solutions focus on managing user identities and access rights, including specialized access through privileged access management (PAM) governed by defined policies. IAM suites integrate secure mechanisms, frameworks and automation for real-time user and attack profiling to meet evolving application needs. Providers are also expected to include social media and mobile access functionalities, addressing security needs beyond traditional web rights management. This quadrant also encompasses machine identity management.

### Eligibility Criteria

1. Offer solutions that can be **deployed on-premises**, in the **cloud**, as **identity-as-a-service** (IDaaS) or through a managed third-party model
2. Deliver solutions that can **support authentication** as a combination of **single sign-on (SSO), multifactor authentication (MFA)**, and risk-based and context-based models
3. Offer solutions that can **support role-based access** and PAM
4. Provide **access management** to address multiple enterprise needs such as **cloud, endpoint, mobile devices, APIs and web applications**
5. Propose solutions that can **support one or more legacy and new IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIMOffer a portfolio with one or more of the following solutions — **directory, dashboard or self-service management** and lifecycle management (migration, sync and replication) — to support secure access

## Observations

In 2025, the IAM market will evolve rapidly, driven by AI-powered security, passwordless authentication and compliance needs. Vendors focus on identity-centric security, automation and UX to support enterprises in managing the digital identities of both human and non-human identities across dynamic and complex environments.

Identity threat detection and response (ITDR) has gained significant attention over the last 12-18 months. Vendors are integrating AI and ML for identity threat detection, automating governance and enforcing risk-based authentication. Security teams increasingly leverage intelligent identity analytics to detect and respond to threats in real time, minimizing the attack surface. Passwordless authentication, including passkeys, biometrics and FIDO2, is becoming standard, reducing phishing risks while ensuring seamless user access.

Zero trust models continue to shape IAM, as it is essential for robust identity management. Real-time capabilities such as dynamic access management are becoming critical to ensure better alignment with zero trust principles. Most IAM platforms are steadily evolving toward semi-autonomous access control by integrating predictive AI to enhance policy decisions and context-aware responses while maintaining operational oversight.

Cloud adoption accelerates IAM's shift toward scalable, interoperable IDaaS solutions, ensuring seamless authentication across hybrid and multicloud environments. Decentralized identity is also emerging, allowing users greater control over personal data. The demand for CIAM solutions is rising as businesses seek to provide secure, personalized and seamless digital experiences for their customers while ensuring robust fraud prevention and privacy protection.

From the 61 companies assessed for this study, 26 qualified for this quadrant, with ten being Leaders and one Rising Star.

### Broadcom

**Broadcom** empowers enterprises to shift from fragmented IAM to a fully orchestrated one by combining technology, scale and domain expertise and identity-centric security model — ready for hybrid cloud, zero trust architectures and regulatory agility.

### CyberArk

**CyberArk** is transforming into a full-scale identity security powerhouse, addressing modern attack surfaces while maintaining its PAM leadership augmented by its adaptive and zero trust-driven approach.

### IBM.

**IBM's** Security Verify enables enterprises to ensure frictionless and secure access control across on-premises, cloud and hybrid cloud environments. Its identity fabric and orchestration capabilities allow for highly customizable workflows.

### ManageEngine

**ManageEngine** offers cost-effective, modular IAM tailored for Microsoft environments. Enterprises benefit from robust on-premises AD lifecycle automation, MFA and auditing without needing full cloud migration.

### Microsoft

**Microsoft** Entra delivers a unified identity platform with deep integration across Microsoft 365, Azure and third-party applications. It is ideal for enterprises seeking scalable, cloud-native identity with native zero trust and conditional access controls.

### Okta

**Okta's** cloud-native architecture ensures high availability and scalability, making it ideal for enterprises of all sizes. Its multicloud compatibility allows seamless integration with AWS, Google Cloud and Azure.

## One Identity

**One Identity** unifies identity governance and administration (IGA) with PAM on a single platform, which is ideal for enterprises modernizing legacy IAM while controlling privileged access. Its deep AD/LDAP integration and robust governance automation simplify hybrid deployments.

**Ping Identity** excels with its flexible, hybrid-ready IAM platform, blending AI-driven risk analysis, no-code orchestration via DaVinci and deep standards support to empower secure, adaptive access across complex enterprise environments.

## SailPoint

**SailPoint** is solidifying its position as a leader in identity security with cutting-edge AI-powered solutions and cloud-first innovation. Strategic acquisitions, including PAM, third-party risk management and healthcare-focused IGA, are broadening its capabilities, driving secure, scalable identity management for enterprises.

## Saviynt

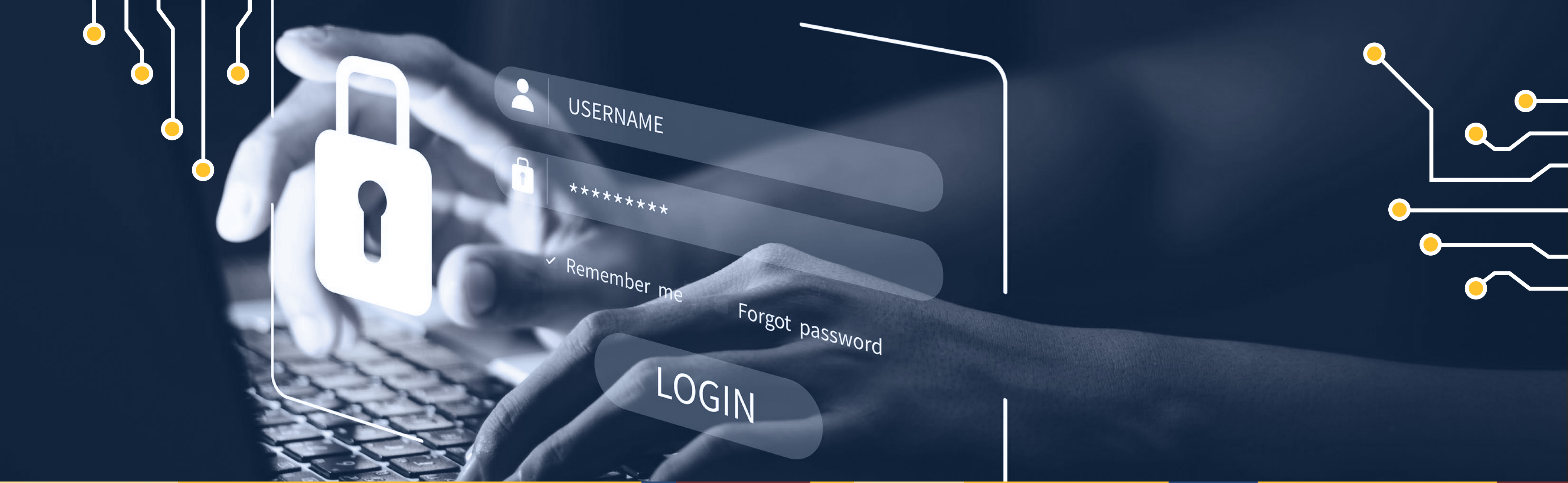
**Saviynt** empowers enterprises with cloud-native identity governance, unifying IGA, PAM and access to insights in a single platform. Its fine-grained entitlement management and risk-aware automation support complex compliance-driven environments.

**BeyondTrust** (Rising Star) stands out with enterprise-grade privileged access management, offering adaptive risk-based controls, session monitoring and endpoint privilege security, which are critical for minimizing attack surfaces across hybrid infrastructure.

## Hidden Champions:

**Entrust** is recognised as a hidden champion for its strong capabilities in IAM, particularly in digital identity, PKI and authentication. Its offerings are well-suited to enterprises addressing hybrid work models, zero trust adoption and regulatory compliance requirements. Its ability to deliver scalable, secure and compliance-ready IAM solutions makes Entrust a valuable enabler of resilient access control and trust assurance, especially for financial and government clients.

**Fischer Identity** is recognised as a hidden champion for its policy-driven IGA automation, seamless Identity as a Service (IDaaS) delivery model, and purpose-built support for regulated sectors such as education and public sector. It excels in delivering configurable lifecycle governance, centralized identity data management, and compliance-aligned access controls. Its streamlined architecture reduces complexity and offers a strong value proposition for mid-sized enterprises needing rapid deployment.



# Extended Detection and Response (Global)

## Who Should Read This Section

This report is valuable for providers offering **extended detection and response (XDR)** services **globally** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. It evaluates global XDR service providers for their enhanced visibility and unified threat detection capabilities that aid enterprises having limited resources with data-driven insights and integration.

### Security professionals

Should read this report for a broad outlook on security trends and discern providers' capabilities in helping enterprises devise robust security strategies.

### Technology professionals

Should read this report to gain insights into the emerging trends in the security landscape and providers' abilities to develop tailored security platforms.

### Strategy professionals

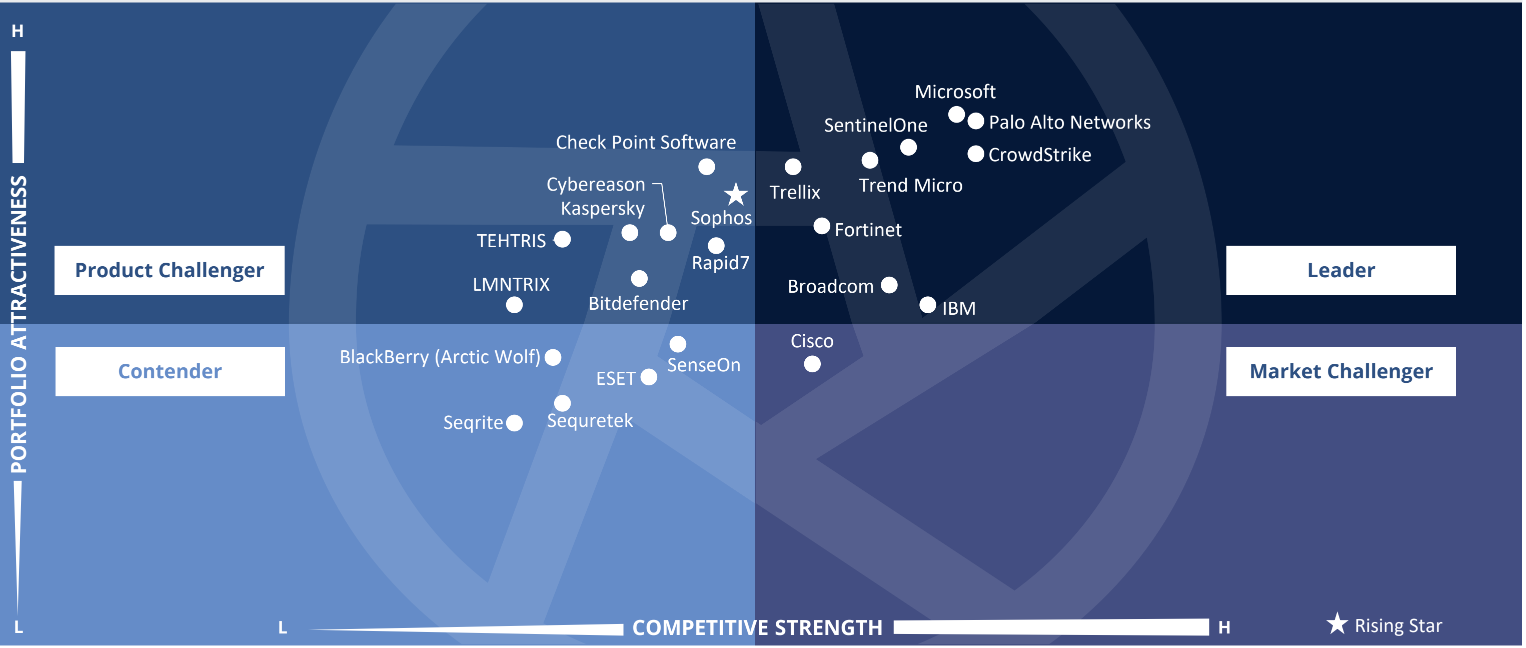
Should read this report to understand service providers' relative positioning and also capabilities in supporting decision-making on partnerships and cost-reduction initiatives.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Extended Detection and Response

Global 2025



This quadrant assesses XDR vendors' and their platforms' ability to provide **integrated threat detection, investigation and response capabilities that enhance visibility and threat context across multiple endpoints, networks and cloud** environments.

*Gowtham Sampath*

## Definition

XDR solution providers assessed in this quadrant are distinguished by their platforms that integrate, correlate and contextualize data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-based technology integrating multiple security solutions and using analytics to improve detection accuracy. It consolidates security products to enhance visibility and threat context across enterprise workspaces, networks and workloads.

XDR solutions use telemetry and contextual data for detection and response, integrating multiple products into a unified interface. They feature high automation and prioritize alerts based on severity to determine the needed tailored responses. This quadrant excludes pure service providers that do not offer an XDR solution based on proprietary software. XDR solutions aim to reduce product sprawl alert fatigue and address integration challenges. They help security operations teams manage or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

## Eligibility Criteria

1. Offer XDR solutions based on **proprietary software** and not on third-party software
2. Ensure that an XDR solution has two primary components: **XDR front end and XDR back end**
3. Offer front end with **three or more solutions or sensors**, including, but not limited to, **endpoint detection and response, endpoint protection platforms**, network protection (firewalls and IDPS), **network detection and response**, identity management, email security, mobile threat detection, cloud workload protection and deception identification
4. Provide solutions with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solutions capable of **blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware
6. Provide solutions using **threat intelligence** and **real-time insights on threats** emanating across endpoints
7. Deliver solutions with **automated response features**

### Observations

The XDR market is undergoing rapid evolution, shaped by increasing enterprise demand for integrated threat detection, response automation and advanced analytics across endpoints, networks, cloud environments and identities. Vendors are aggressively embedding AI and ML across their platforms to reduce dwell times, accelerate threat triage and enable more predictive, behavior-based detection models. This has elevated XDR from a reactive tool into a proactive defense layer, particularly as threat actors become sophisticated and targeted in their approaches.

Native- and third-party solution integration continues to be a critical differentiator, with XDR platforms expanding telemetry ingestion capabilities to include third-party SIEMs, SOAR tools, threat intelligence feeds and adjacent security technologies. Many solutions now offer unified analyst workbenches, curated detections and automated playbooks designed to support lean security operations center (SOC) teams. This enhances visibility and enables faster correlation and contextualization of alerts, reducing false positives and analyst fatigue.

Vendors are actively acquiring competitors, accelerating innovation to enhance threat detection capabilities, expand into new customer segments, or embed managed detection and response (MDR) expertise.

As enterprises seek outcomes over tooling, XDR platforms are evolving to offer modular, cloud-delivered architectures with flexible deployment models. Vendors also focus on modular deployment options that cater to hybrid and multicloud environments, enabling organizations to extend security coverage without increasing complexity.

From the 61 companies assessed for this study, 23 qualified for this quadrant, with nine being Leaders and one Rising Star.

### Broadcom

**Broadcom's** Symantec XDR solution delivers unified threat detection and response, integrating telemetry across multiple domains. The focus is on reducing alert fatigue through correlation, prioritization and automation within a broad ecosystem of Symantec solutions.

### CrowdStrike

**CrowdStrike's** Falcon Insight XDR platform builds on its well-known EDR foundation and cloud-native architecture to deliver a scalable, high-performance detection and response solution that combines threat intelligence, AI and behavioral analytics.

### Fortinet

**Fortinet's** FortiXDR delivers extended detection and response by tightly integrating across its native security fabric, including network, endpoint, email and cloud. The platform emphasizes automation-first response, AI-driven analytics and deep telemetry correlation.

### IBM

**IBM's** XDR strategy is centered around QRadar Suite, combining threat detection, investigation, and response capabilities across hybrid environments. The platform emphasizes open integration, AI-driven automation and deep threat intelligence via IBM X-Force.

### Microsoft

**Microsoft** Defender XDR's 100 percent protection in the MITRE Engenuity ATT&CK® Evaluations shows full visibility and defense across all attack stages, including Windows and Linux underscoring its robust multiplatform support.

### Palo Alto Networks

**Palo Alto Networks** has completed its acquisition of IBM's QRadar SaaS assets. The company aims to provide its customers with advanced security solutions powered by next-gen security SOCs and AI.

### SentinelOne

**SentinelOne** will retire its legacy deception product to focus on higher-growth segments and prioritize investments in AI-powered security and data. It is authorized to sell AI-powered security tools to the most security-conscious federal agencies.

## Trellix

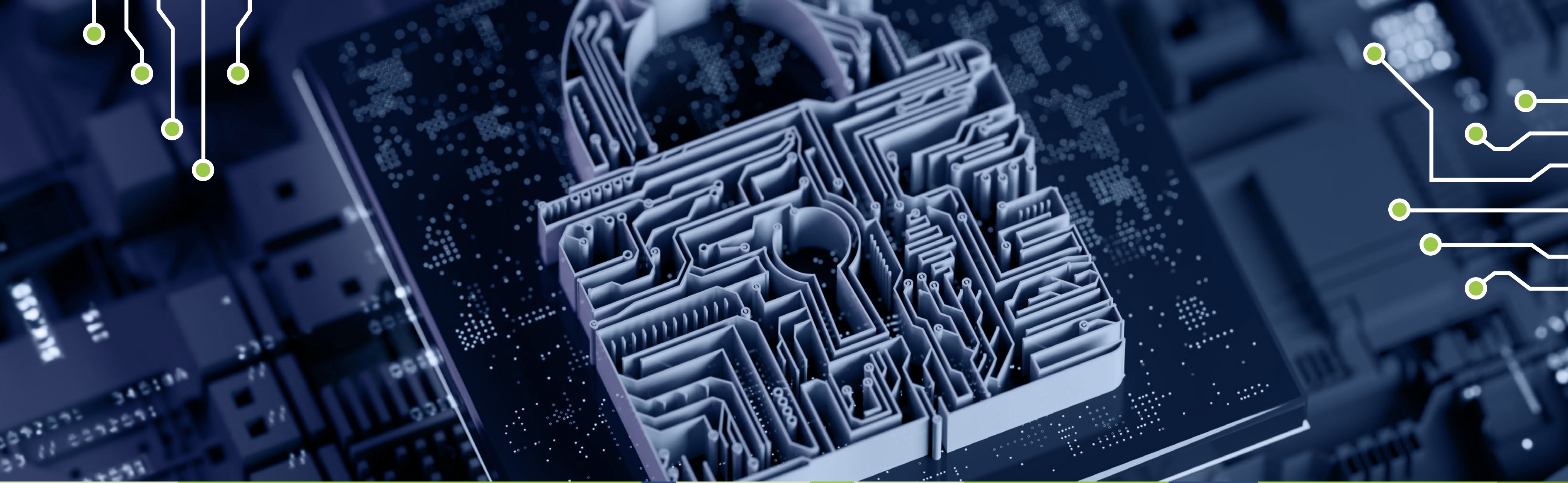
**Trellix** delivers an open and adaptive XDR platform to support dynamic defense strategies. Its emphasis is on integration, threat intelligence and ML to enable faster detection and autonomous response across enterprise environments.

## Trend Micro

**Trend Micro** launched Trend Cybertron, a specialized cybersecurity large language model (LLM) integrated with its Trend Vision One platform. This innovative AI-powered cybersecurity agent is designed to shift enterprises toward a proactive security model.

## Sophos

**Sophos'** (Rising Star) recent acquisition of SecureWorks' MDR business is expected to significantly expand Sophos' threat detection capabilities, service-led offerings and Intercept X platform with improved visibility and automation.



# Security Service Edge (Global)

## Who Should Read This Section

This report is valuable for providers offering services related to **security service edge (SSE) globally** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. Enterprises should read this report for insights on security service edge (SSE) service providers, which is crucial for ensuring security across hybrid and multicloud environments.

### Data management professionals

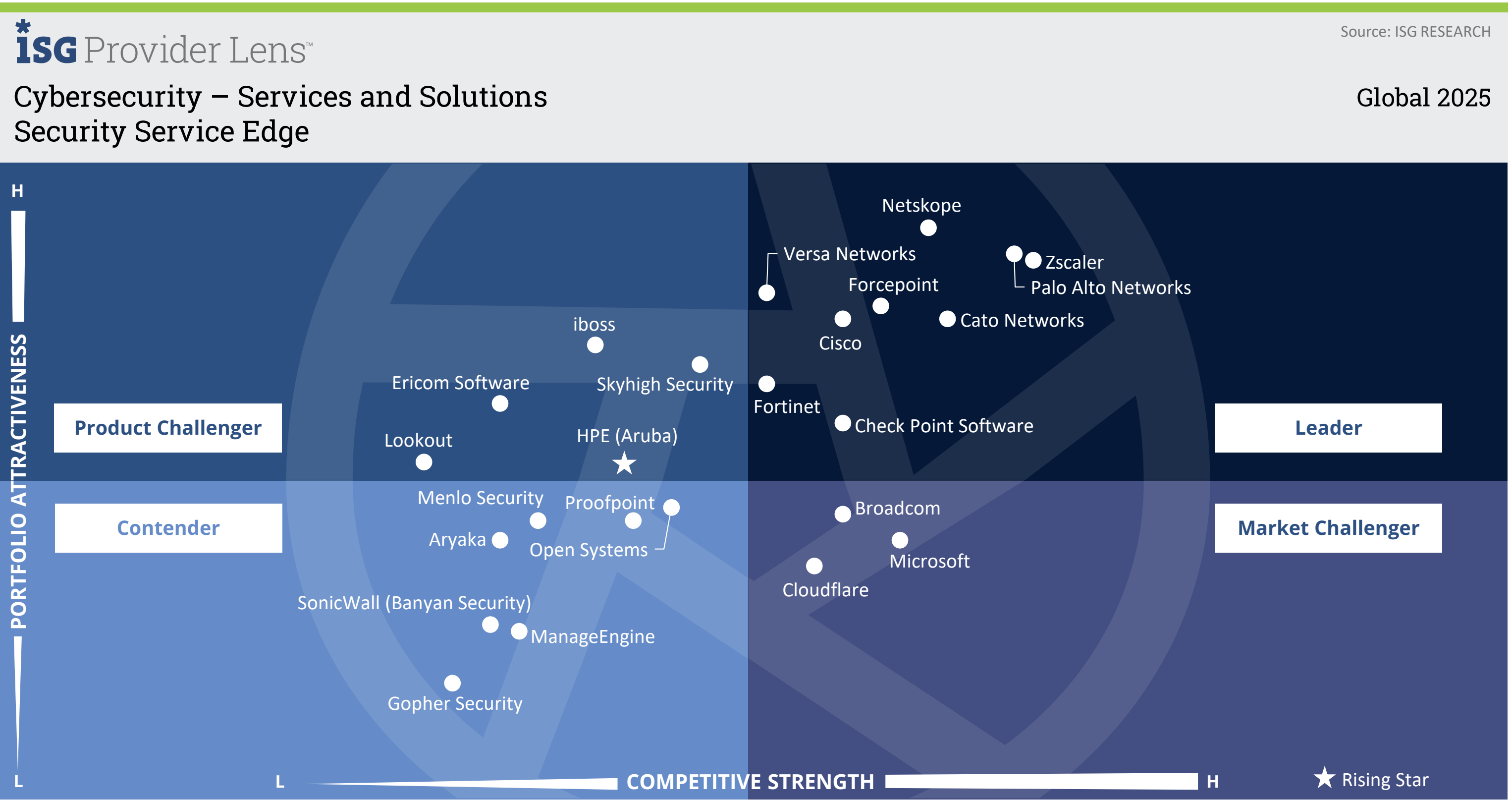
Should read this report to understand how SSE providers help enterprises overcome challenges related to data regulation mandates with enhanced policy controls and reporting.

### Technology professionals

Should read this report to understand how SSE providers assist with adopting enterprisewide zero trust frameworks to improve their security posture.

### Strategy professionals

Should read this report for insights on SSE providers' critical capabilities and their focus on user-centricity to deliver security at the edge or for devices through the cloud.



This quadrant, emphasizing UX, evaluates SSE vendors that deliver **cloud-centric solutions**, integrating various offerings to enable safe access to cloud, **SaaS, web services and private applications**.

*Yash Jethani*

## Definition

SSE solution providers assessed in this quadrant offer cloud-centric solutions, combining proprietary software or hardware and associated services, enabling secure access to the cloud, SaaS, web services and private applications. Providers offer SSE solutions as an integrated security service through globally positioned points of presence with support for local data storage that combines individual solutions such as zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS). SSE can also include other security solutions such as DLP, browser isolation and next-generation firewall (NGFW) to secure access to cloud and on-premises applications.

Providers showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients. This quadrant excludes the network components of secure access service edge (SASE), such as SD-WAN, which will be covered in the ISG Provider Lens™ Network – Software Defined Solutions and Services 2025 study.

## Eligibility Criteria

1. Provide SSE as an **integrated solution** with **ZTNA, CASB, SWG and FWaaS** components
2. Offer solutions **predominantly based on proprietary** software; these solutions may **partially rely on partner solutions** while avoiding **complete dependency on third-party** software
3. Maintain **globally located points of presence** to deliver solutions
4. Deliver **SSE functionalities to cloud and on-premises** environments (including hybrid environments)
5. Undertake **contextual and behavioral evaluations and analysis (user entity and behavior analytics [UEBA])** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **availability of solutions globally**

### Observations

Most companies prioritize SASE or SSE architectures with integrated security and networking. There is a growing shift toward cloud-native services for scalability and resilience, with AI increasingly enhancing threat defense and data protection. Zero trust is commonly emphasized for securing application and data access. Many providers are expanding globally and strengthening offerings through partnerships, with most focusing on cybersecurity, data protection and threat mitigation.

However, differentiated features of top providers include contextual policy enforcement, future-proof security and strategic growth partnerships. Many providers highlight advanced threat defense and data protection as core strengths, providing integrated or cloud-native solutions across diverse environments. Innovation in AI-driven security, intelligent service delivery for targeted markets, and foresight into emerging technologies such as secure browsers and quantum and AI applications stand out as differentiators.

Besides, the convergence of networking and security for high-performance environments necessitates providers to constantly adapt and expand their capabilities to address the complexities of modern security. UX and cloud-native scalability are key priorities, especially for HPE (Aruba) and Fortinet via global PoPs and partnerships. Single-vendor solutions from Versa and Netskope streamline deployment, while Palo Alto's Prisma SASE targets digital experience monitoring (DEM). Market growth is projected to be driven by a threefold to fivefold increase in AI applications set to reshape security.

From the 61 companies assessed for this study, 24 qualified for this quadrant, with nine being Leaders and one Rising Star.

### Cato Networks

**Cato Networks** delivers the scalable, resilient Cato Single Pass Cloud Engine (Cato SPACE) architecture that powers a global cloud service with comprehensive contextual policy enforcement based on network, device, identity, application and data attributes.

### Checkpoint

**Checkpoint** emphasizes Quantum SASE and Harmony Connect, focusing on cloud security and ZTNA. Partnerships, including Tata Communications, enhance its global reach and drive regional growth through industry recognition, consulting expertise, global R&D and AI-driven security innovations.

### Cisco

**Cisco** highlighted its threat defense during the Mobile World Congress 2025, with AI assistant integrations announced for 2025.

### Forcepoint

**Forcepoint** establishes itself as a leader in data protection and AI with its Forcepoint ONE™ platform, offering a comprehensive cloud-native SSE solution for cloud, web, private apps and endpoints.

### Fortinet

**Fortinet's** FortiSASE leverages partnerships and FortiGuard AI services, targeting hybrid environments with a licensing model. Fortinet focuses on unified SASE enhancements, hybrid mesh firewall evolution, and OT security integration.

### Netskope

**Netskope** promotes its intelligent SSE and NewEdge cloud, with a midmarket SASE launch in January 2024 tailored for MSPs, emphasizing zero trust telemetry.

### Palo Alto Networks

**Palo Alto Networks** expects threefold to a fivefold growth in AI apps – providing a boost to adoption of its secure browser adoption – integrating AI into Prisma SASE while excelling in SSE with strong Zero Trust and threat prevention capabilities.

### Versa Networks

**Versa Networks** highlights over 100 Gbps unified SASE gateways, focusing on consolidating networking and security for large enterprises via a robust partner ecosystem.

### zscaler™

**Zscaler** emphasizes its zero trust SASE with new SD-WAN capabilities launched in January 2024, focusing on seamless UX and AI-driven security enhancements.

### HPE (Aruba)

**HPE (Aruba)** (Rising Star) has integrated its SSE with SD-WAN following the acquisition of Axis Security in 2023. With the addition of AI enhancements and plans for acquiring Juniper Networks (pending for 2025), HPE (Aruba) is poised to expand its capabilities further.

# Technical Security Services – Large Accounts

## Who Should Read This Section

This report is valuable for service providers offering **technical security services (TSS)** in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. The report evaluates providers specializing in enterprise security transformations, focusing on those designing and managing multilayered architectures using SASE, IAM and OT security to counter threats and ensure compliance globally.

### Technology professionals

Should read this report to gain insights into provider compliance, market trends and integration for innovation, scalability and threat reduction using advanced technologies.

### Security and data professionals

Should read this report to gain insights into provider compliance, market trends and integration of vendor-neutral solutions in large-scale architecture transformations.

### Business professionals

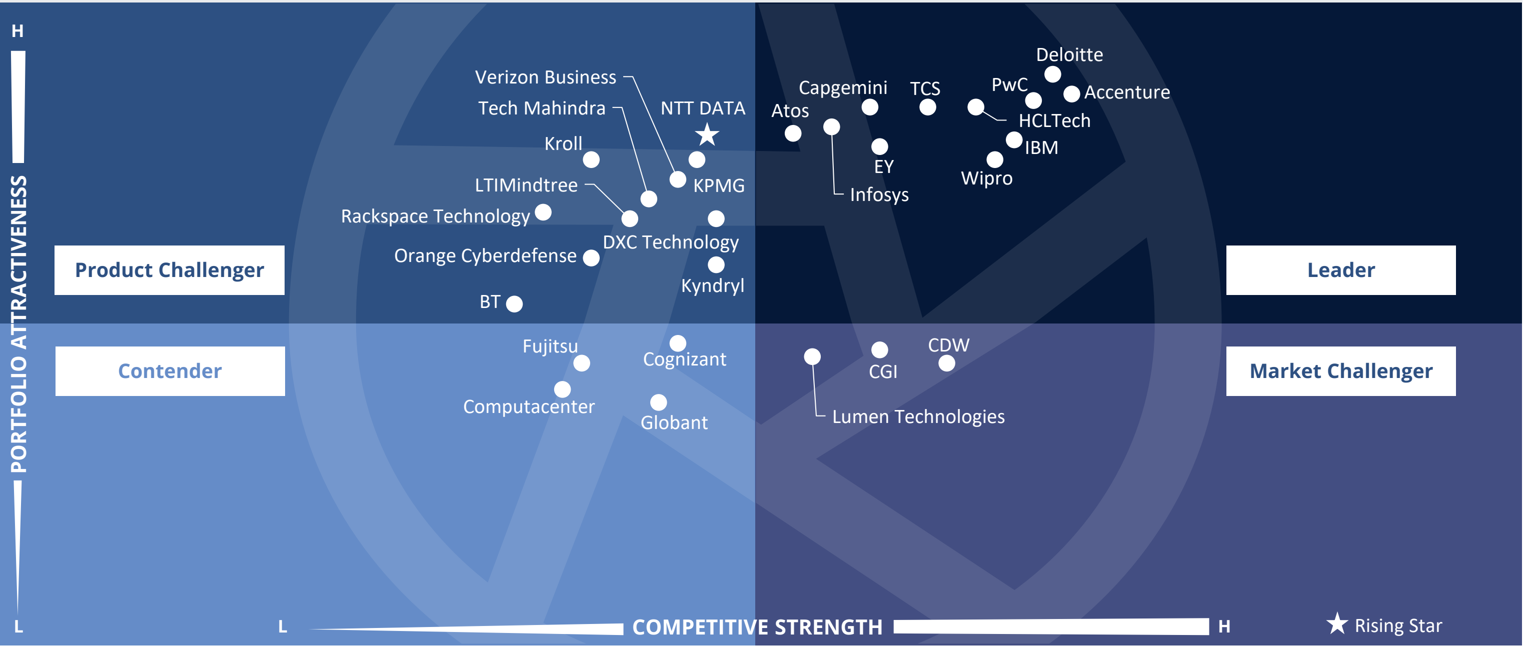
Should read this report to balance data security, customer experience and privacy amid the digital transformation at the forefront of businesses today.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Technical Security Services – Large Accounts

U.S. 2025



The quadrant assesses providers delivering **modular and scalable** technical services by combining **industry-specific** frameworks, **advanced threat detection, cloud, IT/OT** and **identity** expertise to **modernize** enterprise security and drive **risk reduction.**

*Gowtham Sampath*

### Definition

TSS providers assessed in this quadrant cover integration, maintenance and support for IT and OT security products or solutions. TSS encompasses a wide range of security products, including cloud and data center security, IAM, DLP, network security, endpoint security, OT security, SASE and others.

These providers offer playbooks and road maps to enhance security using best-of-breed tools, improving posture and reducing threats. Their portfolios support complete or individual security architecture transformations, alongside product or solution identification, assessment, design and implementation. They invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio.

This quadrant also includes classic managed security services provided without a security operations center. It examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other solution vendors and service providers.

### Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Obtain **authorization from security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies
4. **Do not focus exclusively on proprietary products** or solutions
5. Present **case studies** that demonstrate successful design, deployment and management of cybersecurity solutions for companies within the target country

**Observations**

In the rapidly evolving cybersecurity landscape, large service providers are increasingly aligning their offerings with critical challenges and market demands. The integration of AI and ML technologies is enhancing the efficiency of threat detection, response and mitigation. Service providers are leveraging these innovations to automate security operations, improve real-time insights and create predictive models that strengthen security postures.

A key trend among these providers is the focus on hybrid security architectures, combining traditional on-premises systems with cloud-based solutions to address the complexities of modern enterprises. This integration of IT and OT systems is becoming increasingly critical, particularly in industries such as manufacturing, energy and healthcare, where OT security is a priority. The alignment between IT and OT security ensures that vulnerabilities across the entire ecosystem are addressed, providing a comprehensive defense strategy.

Large providers are also driving the adoption of zero trust architectures, which are gaining traction as essential models for securing access to digital environments. These models, coupled with secure-by-design implementations, are integral to risk-aligned solutions that cater to specific industry needs.

Acquisitions play a vital role in expanding service capabilities, allowing providers to enhance their portfolios with specialized expertise, particularly in cloud security, identity management and advanced threat protection. This approach positions these service providers to offer highly effective security solutions for enterprises navigating the increasingly complex digital threat landscape.

From the 116 companies assessed for this study, 29 qualified for this quadrant, with eleven being Leaders and one Rising Star.

accenture

**Accenture** launched new services and capabilities designed to reinvent business and cyber resilience through the power of GenAI, deepfake protection and quantum-safe data security solutions to help clients across industries become cyber-resilient organizations.

Atos

**Atos** offers a mature TSS portfolio addressing IT/OT security environments with capabilities in design, integration and maintenance of advanced security solutions and blending technical depth with operational resilience to support enterprisewide transformation goals.

Capgemini

**Capgemini** delivers a comprehensive portfolio of TSS that enables enterprises to manage complex hybrid environments across IT/OT domains with an emphasis on industry partnerships, specialized certifications and vertical-specific frameworks.

Deloitte.

**Deloitte** emphasizes repeatable playbooks, threat reduction road maps and industry-specific customization, making it a strong player for organizations seeking to align their technical defenses with enterprise risk profiles and regulatory expectations.

EY

**EY** develops prescriptive road maps and playbooks designed to address evolving threat landscapes, blending technical implementation with strategic risk alignment, focusing on securing cloud-first and hybrid IT/OT environments.

HCLTech

**HCLTech** delivers a technically mature TSS portfolio anchored in secure infrastructure transformation and vendor-neutral integration relying on industrialized security delivery, bolstered by frameworks and accelerators that improve security posture and resilience.

IBM

**IBM** offers comprehensive and technically advanced TSS portfolios, underpinned by its deep security research, product innovation and integration capabilities, operationalizing security transformation at scale using vendor-agnostic methodologies.

**Infosys** provides an engineering-driven approach to TSS, combining architecture-led delivery with product implementation encompassing a wide range of security technologies across IT, cloud and OT environments and emphasizing unified integration and posture improvement.

**PwC** integrates technical cybersecurity services with business-aligned outcomes, leveraging its consulting heritage to provide deep technical implementation with strategic oversight, delivering modular security blueprints, implementation playbooks and industry context.

**TCS** delivers a robust suite of TSS centered on secure enterprise architecture with its Cyber Defense Suite and contextualized transformation frameworks, which empowers clients to improve posture and resilience through modular adoption of best-of-breed tools.

**Wipro** offers a mature and modular suite of TSS that supports large-scale enterprise security transformations through its CyberTransform, Zero Trust Engineering frameworks and significant investments in integration accelerators, playbooks and blueprints.

**NTT DATA** (Rising Star) provides a comprehensive suite of TSS built around a security-first strategy, leveraging in-house expertise and partnerships with leading security vendors, focusing on integrating, managing and transforming security architectures across industries.

# Technical Security Services – Midmarket

## Who Should Read This Section

This report is valuable for service providers offering **technical security services (TSS)** in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. This report offers actionable insights for enterprises to enhance security with scalable, cost-effective solutions, assessing providers' capability to integrate advanced, vendor-neutral tools into infrastructures.

### Technology professionals

Should read this report to gain insights into provider compliance, market trends and integration for innovation, scalability and threat reduction using advanced technologies.

### Security and data professionals

Should read this report for insights on compliance, risk management, threat detection and aligning cybersecurity with business goals.

### Business professionals

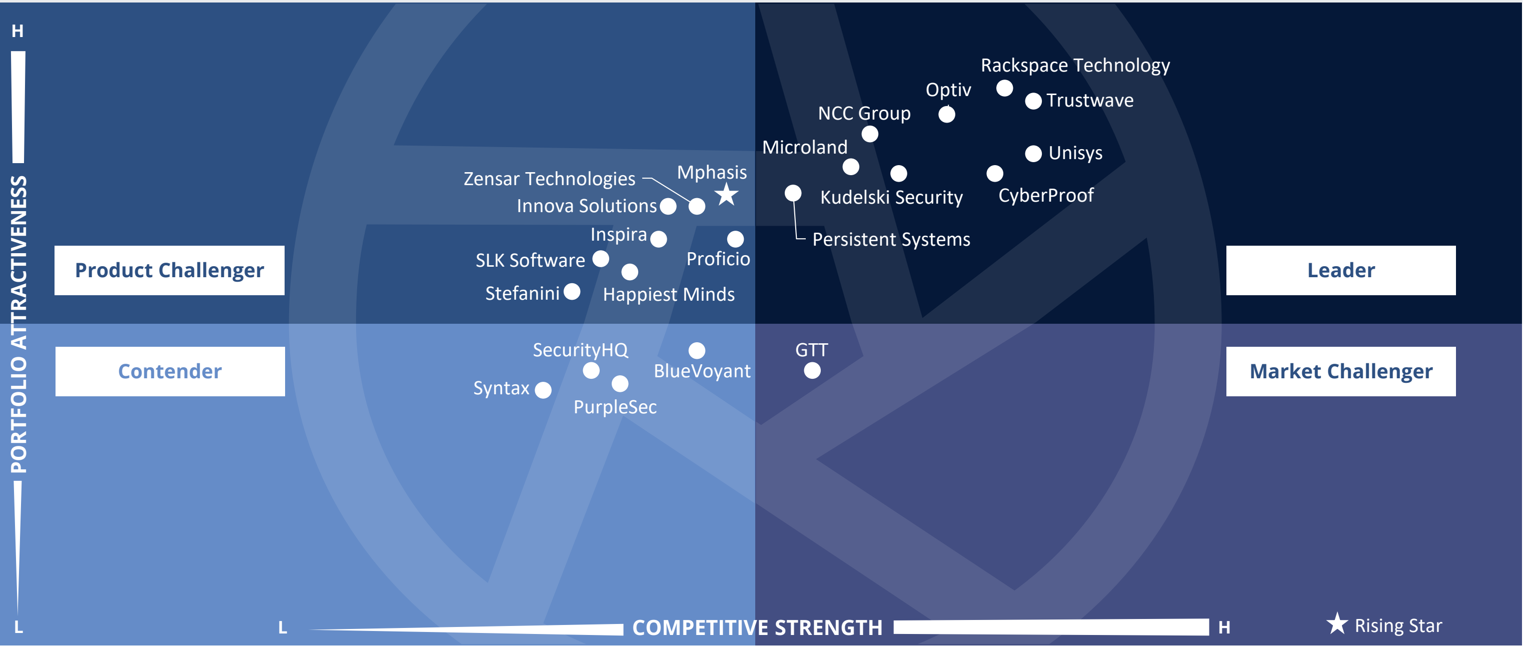
Should read this report to balance data security, customer experience and privacy amid the digital transformation at the forefront of businesses today.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services – Midmarket

U.S. 2025



The quadrant assesses providers delivering **modular and scalable** technical services by combining **industry-specific** frameworks, **advanced threat detection, cloud, IT/OT** and **identity** expertise to **modernize** enterprise security and drive **risk reduction.**

*Gowtham Sampath*

### Definition

TSS providers assessed in this quadrant cover integration, maintenance and support for IT and OT security products or solutions. TSS encompasses a wide range of security products, including cloud and data center security, IAM, DLP, network security, endpoint security, OT security, SASE and others.

These providers offer playbooks and road maps to enhance security using best-of-breed tools, improving posture and reducing threats. Their portfolios support complete or individual security architecture transformations, alongside product or solution identification, assessment, design and implementation. They invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio.

This quadrant also includes classic managed security services provided without a security operations center. It examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other solution vendors and service providers.

### Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Obtain **authorization from security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies
4. **Do not focus exclusively** on **proprietary products** or solutions
5. Present **case studies** that demonstrate successful design, deployment and management of cybersecurity solutions for companies within the target country

## Observations

Compared to large cybersecurity integrators that emphasize scale, standardization and enterprisewide platforms, midsize service providers are differentiating through agility, contextual expertise and execution-focused partnerships. These midsize providers are embedding AI and ML for broad analytics and targeted use-case engineering, such as dynamic threat modeling, adaptive detection rules and comanaged SOC enrichment that respond to each client's operational footprint.

Another differentiator is how midsize providers approach IT/OT convergence by building custom policy frameworks and modular deployment models specifically designed for hybrid infrastructures in industries such as manufacturing, utilities and public services. Their structure allows quick alignment to handle critical challenges, particularly in environments still modernizing from legacy systems.

While zero trust adoption is prevalent across the market, midsize providers excel in practical zero trust enablement, deploying incremental, risk-prioritized controls instead of enterprisewide architectural overhauls. This approach accelerates time to value, especially for mid-tier organizations that require defense-in-depth without operational disruption.

Midsize firms also emphasize industry specificity, creating TSS blueprints that reflect industry regulations, threat models and resource constraints. Strategic acquisitions among these providers focus on depth over breadth, such as bolstering red and blue team capabilities or integrating niche identity platforms, enabling them to deliver personalized, compliance-ready security outcomes.

From the 116 companies assessed for this study, 22 qualified for this quadrant, with nine being Leaders and one Rising Star.

### CyberProof

A UST Company

**CyberProof** has expanded collaboration with Google Cloud by leveraging Google Chronicle Security Operations to bolster security analytics and threat detection. This emphasizes a cloud-first approach to security, leveraging Google's robust infrastructure and capabilities.

### KUDELSKI SECURITY

**Kudelski Security** has introduced a new AI Security Service Portfolio; expanded its partnership with CrowdStrike (Next-Gen SIEM), Wiz (CSPM) and Qualys (Risk Operations) solutions to provide comprehensive threat exposure management and detection and response solutions tailored to client needs.

### MICROLAND®

**Microland** had achieved Elite Plus status with Juniper Networks to codevelop a Network-as-a-Service offering, enhancing secure AI-native networking solutions. It is partnering with Microsoft by focusing on cloud-first strategies and infrastructure modernization.

### NCC Group

**NCC Group** has launched a flagship Partner Network to enhance software resilience offerings, enabling software vendors to support customers in adopting and managing new technologies confidently.

### Optiv

**Optiv** announced its 2024 Partner of the Year Award winners, highlighting its expansive array of industry-leading technology partners with winners including CrowdStrike, SailPoint, Google Cloud and Cribl, among others.

### Persistent

**Persistent Systems'** acquisition of Arrka has significantly expanded its capabilities in data privacy, governance and AI oversight, as well as the ability to implement solutions that secure data across its lifecycle and align with frameworks such as NIST.

### rackspace technology

**Rackspace Technology** has revamped its Channel Partner Program with enhanced incentives and a long-term growth strategy, focusing on a channel-first approach. It announced Rackspace AI Business, a holistic AI-ready platform engineered to optimize enterprise AI workloads.

**Trustwave** has introduced two new accelerators, including Accelerator for Microsoft Purview and the Accelerator for Microsoft Entra ID, which are designed to help organizations quickly improve their security maturity and identify cost-saving opportunities.

**Unisys** has formed a strategic partnership with Freshworks to deliver innovative ITSM solutions by combining Freshworks' modern ITSM tools with Unisys's global reach and expertise, targeting midmarket and enterprise companies.

**Mphasis** (Rising Star) has announced a strategic security partnership with SecPod to offer vulnerability management services through SecPod's SanerNow CVEM platform that continuously scans, detects, prioritizes, normalizes and patches vulnerabilities.

# Kudelski Security

Leader

> “Kudelski Security exemplifies precision-driven implementation and tailored lifecycle support, distinguishing itself through its ability to integrate vendor-agnostic technologies into complex IT-OT environments, making it a trusted partner for enterprises.”
>
> *Gowtham Sampath*

### Overview

Kudelski Security is an innovative and independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is a division of the Kudelski Group (SIX:KUD S), which has over 1,800 employees in 20 with headquarters in Phoenix, Arizona, and in Cheseaux-sur-Lausanne, Switzerland. Kudelski Security provides next-gen MDR complemented by Advisory, Technology security services and OT/CPS security services. The company maintains close ties with global technology companies, including F5, Fortinet, Juniper, Zscaler, Microsoft, CrowdStrike Wiz, Qualys to leverage their capabilities in networking, infrastructure and security.

### Strengths

**Vendor-agnostic integration and lifecycle support:** Kudelski Security emphasizes flexibility through its vendor-agnostic approach, allowing clients to integrate the best-of-breed technologies into their existing ecosystems. Its robust lifecycle services covering assessment, implementation, tuning and long-term support ensure sustained performance and threat protection regardless of the technology stack. It also delivers converged security across verticals to manage complex threat surfaces with precision and resilience.

**High-touch support model:** Through its Cyber Fusion Centers in the U.S. and Switzerland, Kudelski Security delivers high-touch implementation and postdeployment services tailored to client risk profiles. This proximity to clients, geographically and operationally, enhances response agility and ensures continuity in security operations. The company emphasizes flexibility through its vendor-agnostic approach, allowing clients to integrate the best-of-breed technologies into their existing ecosystems.

**Engineering-driven automation and tuning:** Kudelski Security leverages its in-house engineering and R&D capabilities to automate security solution deployment and fine-tune configurations over time. This approach reduces manual overhead, increases efficiency and ensures the adaptive evolution of controls in response to emerging threats.

### Caution

While Kudelski Security offers a robust suite of security services, the complexity of implementing and integrating these solutions in highly diverse IT and OT environments could be challenging for organizations with legacy systems or those lacking internal cybersecurity expertise.

# Strategic Security Services – Large Accounts

## Who Should Read This Section

This report is valuable for service providers offering **strategic security services (SSS)** in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. This report equips enterprises with intelligence to align cybersecurity strategies with emerging technologies like AI, focusing on providers that tackle advanced threats.

### Cybersecurity professionals

Should read this report to effectively manage risks, enhance threat detection, align strategies with business goals and better understand security trends.

### Technology professionals

Should read this report to find partners embedding security in digital projects, countering threats with AI and automation, and uncovering trends in tailored security solutions.

### Strategy professionals

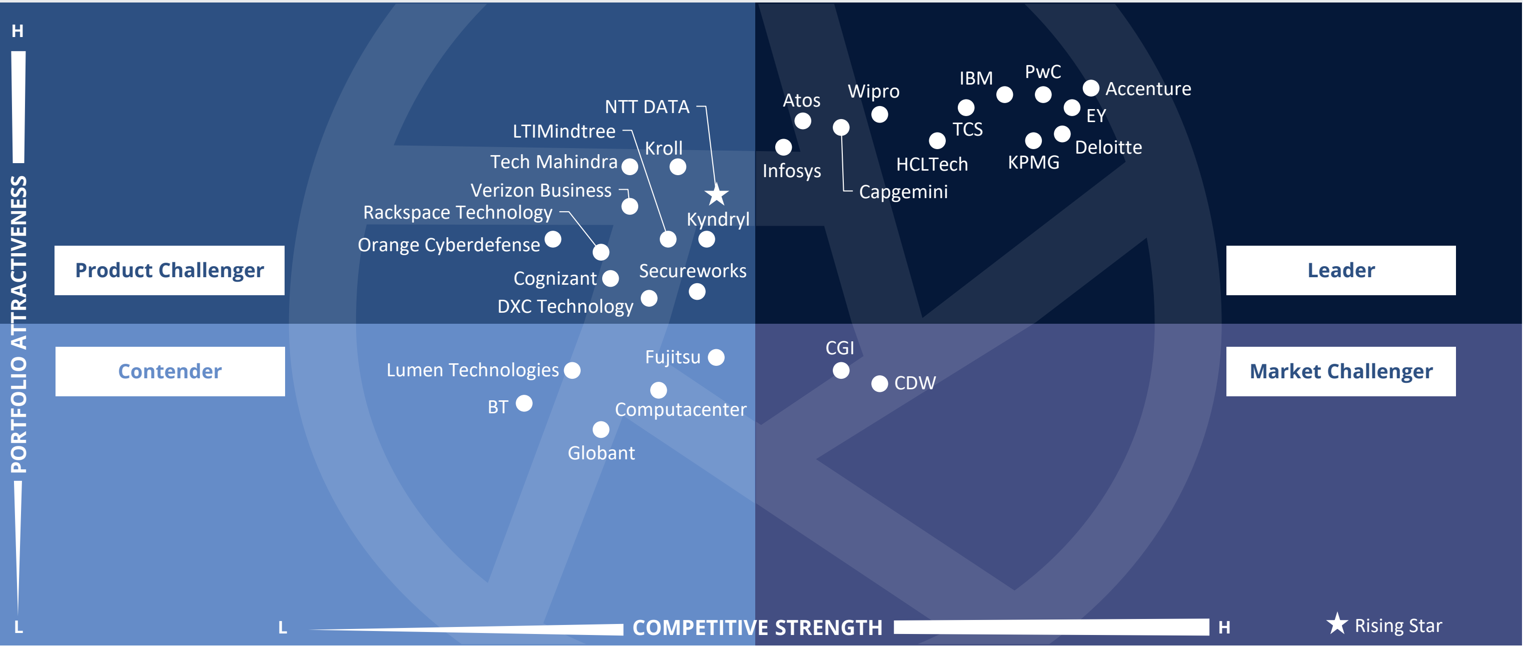
Should read this report to know providers' capabilities for partnerships and cost reduction. CFOs and CEOs should evaluate solutions for cost-effectiveness and strengthen cybersecurity.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Strategic Security Services – Large Accounts

U.S. 2025



The quadrant assesses providers delivering strategic cybersecurity services through **expert-led assessments, vCISO** offerings and security **maturity evaluations** that integrate IT/OT strategies and regulatory alignment to fortify **enterprise resilience.**

*Gowtham Sampath*

### Definition

SSS providers assessed in this quadrant offer IT and OT security consulting. Services include security audits, assessments, awareness and training. These providers also help assess security maturity and define cybersecurity strategies to meet enterprise-specific requirements.

Providers employ experienced security consultants to plan and manage end-to-end security programs for enterprises. Considering the rising demand from SMBs and talent shortages, SSS providers offer on-demand experts via virtual CISO services. They create business continuity road maps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to improve cyber literacy and response among enterprise board members and employees. They also provide guidance on selecting security technologies and suppliers, reviewing organizational structures for cybersecurity, evaluating security processes and practices, and improving them in alignment with the risks faced. This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.

### Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Display competence in the application of good practices and market security frameworks such as ISO 27000, NIST and CIS
3. **Offer at least one of the above** strategic security services in the respective countries assessed for this study
4. Provide **security consulting services using frameworks such as NIST and ISO**
5. **Do not focus exclusively on proprietary products** or solutions

### Observations

Cybersecurity strategies have evolved toward an intelligent, integrated and resilient approach, where large providers are driving transformation with a focus on AI and ML, zero trust and long-term resilience. As enterprises increasingly face advanced threats, solutions are evolving to ensure deep IT/OT integration and more robust, industry-specific defenses that align with the unique risk profiles of industries such as healthcare, finance and government.

The key trends include deploying AI-driven threat intelligence platforms that continuously learn and adapt, helping enterprises anticipate and mitigate risks before they manifest. Zero trust architectures have become foundational, ensuring that every access point, device and identity is continually verified in a fluid, dynamic environment. With security audits becoming increasingly automated and integrated with business processes, providers are offering continuous risk validation, ensuring ongoing compliance and proactive security assessments.

Furthermore, with the growing emergence of quantum computing, a significant focus on quantum-readiness has taken hold, preparing enterprises for the next frontier in cybersecurity. The ability to craft risk-aligned solutions that balance security and innovation while ensuring long-term operational resilience is quickly becoming a key differentiator. Providers are securing data and building frameworks that enable businesses to scale confidently, innovate freely and stay ahead of an increasingly complex threat landscape.

From the 116 companies assessed for this study, 30 qualified for this quadrant, with twelve being Leaders and one Rising Star.

accenture

**Accenture** has expanded its cybersecurity services by investing in QuSecure to offer comprehensive post-quantum crypto agility solutions. The company has introduced new services leveraging GenAI to enhance business and cyber resilience.

Atos

**Atos** leverages the AIsaac Cyber Mesh platform with GenAI and predictive analytics to reinforce cyber resilience. The company also focuses on digital sovereignty by offering trusted and tailored cybersecurity solutions, including post-quantum cryptography services.

Capgemini

**Capgemini** emphasizes cybersecurity as a catalyst for transformation, integrating a business-focused approach with industry-specific expertise and advanced technology. The company focuses on quantum computing, communication and security to prepare for future challenges.

Deloitte.

**Deloitte** offers Quantum Cyber Readiness services to help organizations mitigate cryptographic risks associated with quantum computing. The company provides cyber risk services, assisting clients in transforming enterprise security and preparing for the quantum era.

EY

**EY** advises organizations to prepare for quantum computing cybersecurity threats, emphasizing the importance of proactive measures to secure data. The firm also offers insights into building a simplified, secure, compliant and resilient cybersecurity posture.

HCLTech

**HCLTech** provides integrated cybersecurity solutions, including security audits, compliance, risk advisory services and security assessments. The company also explores quantum technology's impact on security and intelligence innovations.

IBM

**IBM** offers Quantum Safe services, providing technology, services and strategies needed to execute an end-to-end quantum-safe transformation and build cryptographic agility. The company also emphasizes the importance of preparing for quantum cybersecurity threats.

**Infosys** has developed Quantum Living Labs to explore quantum computing's potential in transforming business operations. The company also offers business resilience validation services to identify critical business services and minimize the impact of disruptions.

**KPMG** has developed a comprehensive quantum security framework to help organizations transition to quantum resilience and ensure compliance. The company focuses on risk, resilience and trust, emphasizing the importance of maintaining operations and mitigating future incidents.

**PwC** advises organizations to prepare for quantum computing's cybersecurity risks by transitioning to quantum-resistant encryption and aligning with evolving regulatory frameworks. It also provides strategies for transitioning to quantum-resistant systems.

**TCS** emphasizes preparing for the quantum shift by developing post-quantum cryptography algorithms to ensure cloud and online activity. The company also focuses on GenAI, cloud security and zero trust to protect enterprises from emerging threats.

**Wipro** offers the CyberTransform platform, delivering strategy-first cybersecurity advisory and implementation services. The company also provides insights into the state of cybersecurity, highlighting the importance of resilience in an age of continuous disruption.

**NTT DATA** (Rising Star) has introduced a new globally unified cybersecurity strategy to provide end-to-end support for clients confronting sophisticated cyberthreats. The company also emphasizes building strong security foundations to prepare for future challenges.

# Strategic Security Services – Midmarket

## Who Should Read This Section

This report is valuable for service providers offering **strategic security services (SSS)** in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. This report gives enterprises insights to evaluate security maturity and form custom cybersecurity strategies. It highlights providers' on-demand expertise, virtual CISO services and capabilities to enhance cyber literacy through exercises.

### Cybersecurity professionals

Should read this report to effectively manage risks, enhance threat detection, align strategies with business goals and better understand security trends.

### Technology professionals

Should read this report to find partners embedding security in digital projects, countering threats with AI and automation, and uncovering trends in tailored security solutions.

### Strategy professionals

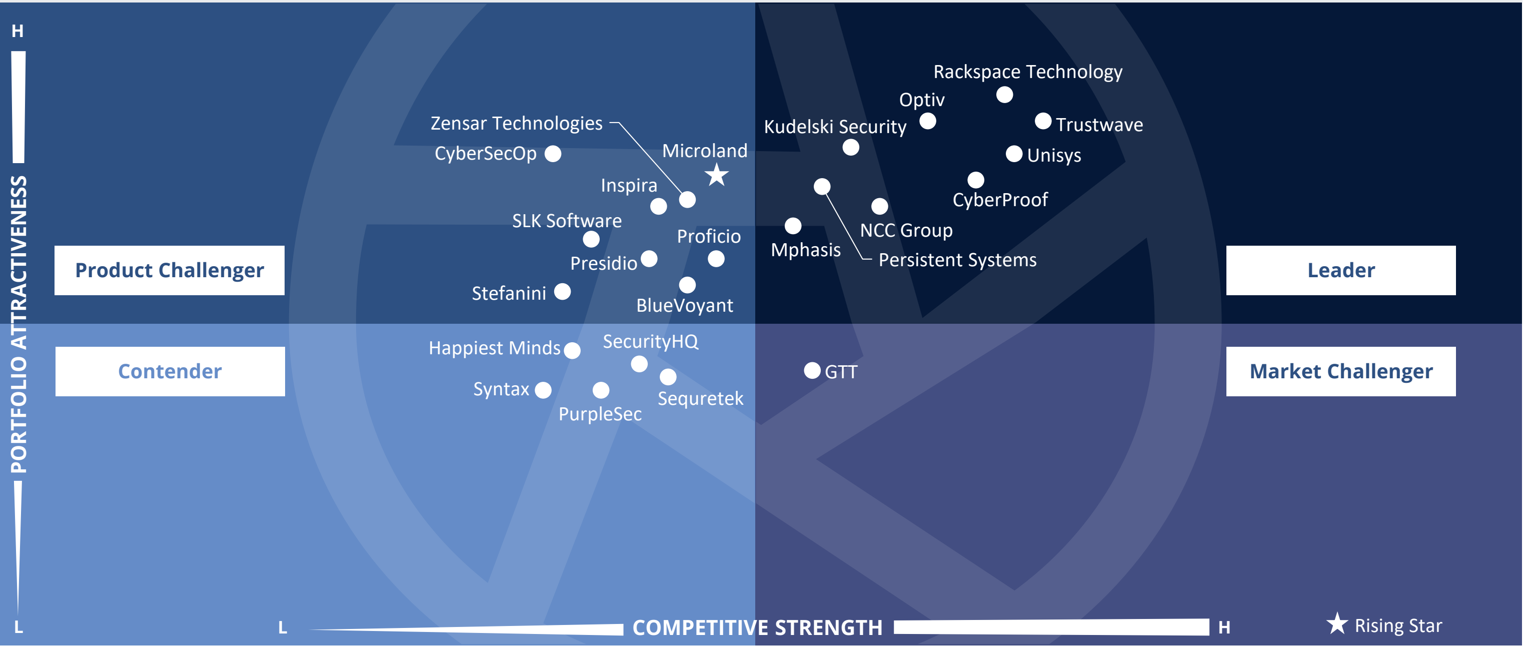
Should read this report to know providers' capabilities for partnerships and cost reduction. CFOs and CEOs should evaluate solutions for cost-effectiveness and strengthen cybersecurity.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Strategic Security Services – Midmarket

U.S. 2025



This quadrant assesses providers delivering strategic cybersecurity services through **expert-led assessments, vCISO** offerings and security **maturity evaluations** that integrate IT/OT strategies and regulatory alignment to fortify **enterprise resilience.**

*Gowtham Sampath*

## Definition

SSS providers assessed in this quadrant offer IT and OT security consulting. Services include security audits, assessments, awareness and training. These providers also help assess security maturity and define cybersecurity strategies to meet enterprise-specific requirements.

Providers employ experienced security consultants to plan and manage end-to-end security programs for enterprises. Considering the rising demand from SMBs and talent shortages, SSS providers offer on-demand experts via virtual CISO services. They create business continuity road maps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to improve cyber literacy and response among enterprise board members and employees.

They also provide guidance on selecting security technologies and suppliers, reviewing organizational structures for cybersecurity, evaluating security processes and practices, and improving them in alignment with the risks faced. This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.

## Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Display competence in the application of good practices and market security frameworks such as ISO 27000, NIST and CIS
3. **Offer at least one of the above** strategic security services in the respective countries assessed for this study
4. Provide **security consulting services using frameworks such as NIST and ISO**
5. **Do not focus exclusively** on **proprietary products** or solutions

### Observations

Midmarket cybersecurity providers are reshaping the landscape of Strategic Security Services by offering agile, high-impact solutions that prioritize contextual relevance over scale. These organizations deliver tightly aligned advisory and managed services that address specific industry risks, regulatory requirements and operational maturity levels. Their differentiation lies in combining zero trust implementation, AI-enhanced threat detection and adaptive compliance models into modular, scalable offerings that meet the needs of resource-conscious enterprises.

Unlike large providers that build extensive frameworks, midmarket firms focus on integration over orchestration, providing automation-led platforms that improve visibility, streamline threat response and support hybrid IT and OT environments. They emphasize value through modular engagement models, including comanaged services, virtual CISO capabilities and rapid security assessments tailored for agencies or midsize enterprises undergoing transformation. Their strategies prioritize outcome-driven execution and delivering tangible security improvements without burdening teams or requiring large-scale infrastructure changes.

Many providers are focused on enhancing readiness for emerging threats such as quantum risk and AI-based attack surfaces while maintaining practical priorities such as securing multicloud architectures and enabling resilient data governance. These providers have become essential partners for organizations seeking accelerated security maturity, offering clarity, precision and measurable value where agility and domain alignment are critical than global reach.

From the 116 companies assessed for this study, 24 qualified for this quadrant, with nine being Leaders and one Rising Star.

CyberProof®
A UST Company

**CyberProof's** layered approach to resilience includes advanced attack path mapping and risk-based prioritization, which enable adaptive risk mitigation. This approach emphasizes role-based visibility, allowing security leaders to co-align risk with operational objectives.

KUDELSKI SECURITY

**Kudelski Security** delivers effective programs to reduce risks and strengthen cybersecurity postures. Its CTEM services helps organizations better manage their attack surface and its AI Security Service Portfolio introduces robust guardrails for organizations adopting AI.

Mphasis
The Next Applied

**Mphasis** utilizes its Next Labs innovation engine and cyber resilience programs to address data recovery readiness, incident response maturity and secure architecture design, especially in multicloud and AI-integrated ecosystems.

NCC Group

**NCC Group** partnered with Dragos to deliver OT resilience through its Facility Due Diligence service, focusing on safeguarding OT environments against cyberthreats. The company joined Auto-ISAC as a strategic partner to enhance cybersecurity in the automotive industry.

Optiv

**Optiv** introduced the Optiv Market System (OMS) in October 2024, a unified cybersecurity reference architecture, aligning industry standards such as NIST and MITRE with Optiv's services and partner technologies, enabling enterprises to assess and optimize security investments.

Persistent

**Persistent Systems** acquired select assets from SoHo Dragon to strengthen and enhance its cybersecurity capabilities in the finance sector. The company offers a Cybersecurity Platform that helps enterprises meet security and compliance requirements.

rackspace
technology

**Rackspace Technology** formed a strategic partnership with Rubrik to launch the Rackspace Cyber Recovery Cloud, a fully managed isolated recovery service designed to enhance cyber resilience and ensure business continuity.

Trustwave

**Trustwave** has expanded its tabletop simulation and incident response planning services, ensuring enterprises are prepared for ransomware attacks, regulatory audits and business continuity scenarios.

unisys

**Unisys** emphasizes future-proof resilience through offerings such as post-quantum cryptography (PQC) services and continuous security validation, enabling risk-informed decision-making at both the system and organizational levels.

MICROLAND

**Microland** (Rising Star) enhanced its cybersecurity services portfolio with an analytics-led approach to cyber defense management. The company also announced a strategic partnership with Serco AsPac to drive digital transformation, leveraging cloud for business agility and resilience.

# Kudelski Security

Leader

> "Kudelski Security blends strategy with operational depth and offers a security advisory model that balances governance oversight with pragmatic execution, aligning cybersecurity initiatives with business goals and focusing on resilience and trust."
>
> *Gowtham Sampath*

### Overview

Kudelski Security is an innovative and independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is a division of the Kudelski Group which has a dual headquarters in Phoenix, Arizona, and in Cheseaux-sur-Lausanne, Switzerland, operating in 20 countries with over 1,800 employees. The company's team of consultants is highly experienced, with a strong background in managing end-to-end security programs with cybersecurity strategies tailored to specific business needs, focusing on enterprise-specific risk profiles, and compliance requirements.

### Strengths

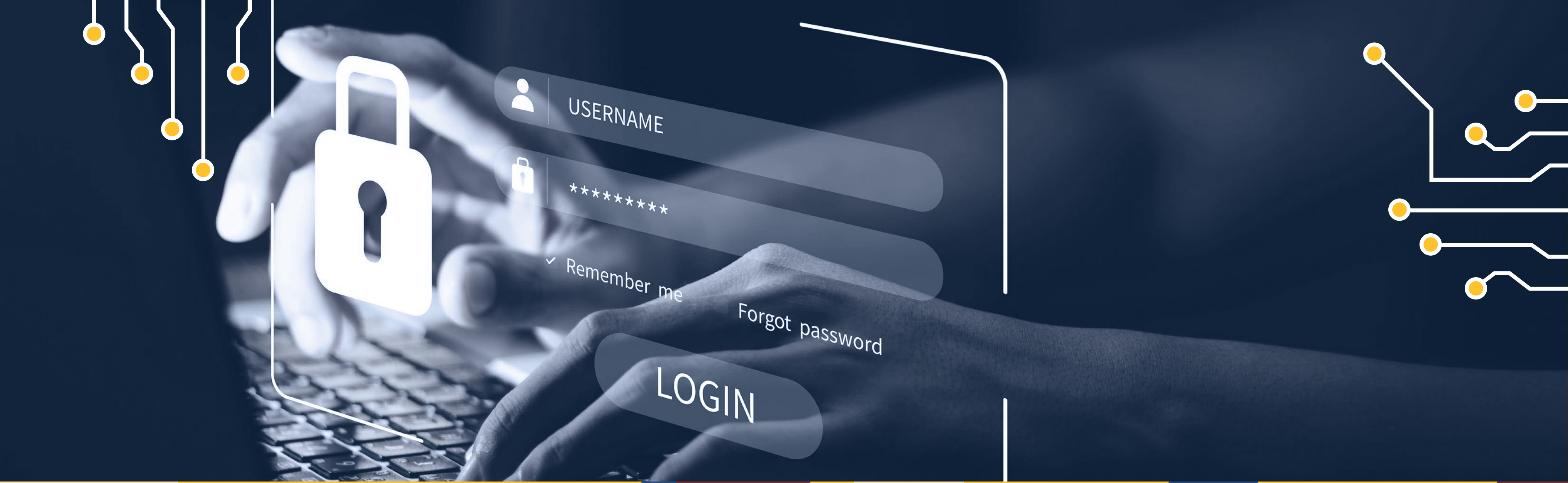
**Comprehensive offerings:** Kudelski Security offers a full range of cybersecurity services for IT & OT/CPS, including risk & security assessments, vulnerability management, Continuous Threat Exposure Management (CTEM), offensive security services, incident response and managed security services (MSS). Its holistic approach ensures that organizations receive a well-rounded security program, from planning and consulting to active monitoring and real-time threat detection.

**Integrated incident readiness and response:** Kudelski Security's strategic advisory services include a proactive approach to incident readiness through tabletop exercises, threat modeling and crisis simulation workshops. These services are closely integrated with its global incident response, MDR and CTEM capabilities, ensuring that strategies are rooted in operational reality with seamless support for post-breach actions, threat mitigation and remediation programs.

**Customized security consulting:** Kudelski's security consulting services are tailored to meet the specific needs of each enterprise, considering the company's risk profile, industry challenges and security maturity. Its consultants work closely with clients to design cybersecurity strategies that align with business goals and compliance requirements, ensuring security investments are directly tied to organizational priorities.

### Caution

Although Kudelski Security has strong advisory and trust-led engagements, it may face challenges scaling its presence in highly competitive global markets dominated by larger consultancies. Expanding brand awareness and investment in platform-driven advisory delivery could further enhance its strategic positioning.



# Next-Gen SOC/MDR Services – Large Accounts

## Who Should Read This Section

This report is valuable for service providers offering **Next-Gen SOC Services** in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. This report analyzes providers for enterprises, highlighting those integrating AI-driven threat hunting and forensics with traditional security services to manage diverse environments and mitigate threats.

### Cybersecurity professionals

Should read this report to gain insights on providers aligning SOC services with compliance and helping devise robust security strategies while mitigating transformational risks.

### Technology professionals

Should read this report to know security trends and providers' tailored platforms. Compliance leaders can find SOC-aligned providers, and IT leaders can access vendor-neutral expertise.

### Business professionals

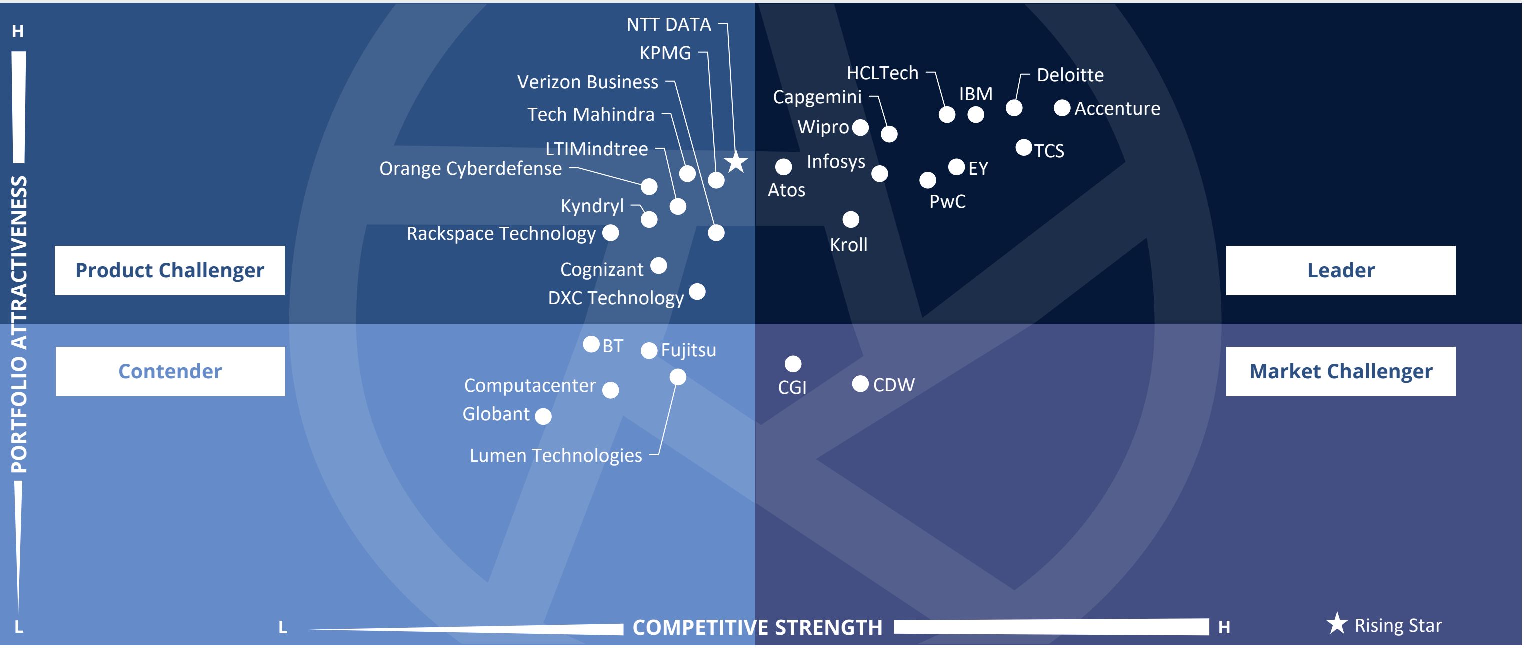
Must read this report to gain valuable insights into simplifying security operations. It offers practical solutions to reduce complexity and enhance efficiency.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Next-Gen SOC/MDR Services – Large Accounts

U.S. 2025



The quadrant evaluates providers integrating **advanced MDR** capabilities with **AI-driven analytics, automated response** and **real-time threat intelligence** to deliver **unified**, proactive **security operations** across **hybrid IT and OT** environments.

*Gowtham Sampath*

## Definition

Providers assessed in this quadrant offer services related to the continuous monitoring of IT and OT infrastructures by a security operations center (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle from identification to response and remediation.

Next-Gen SOC providers are in demand to strengthen enterprises' security posture and improve the effectiveness of security programs. They blend traditional managed security services with innovation to deliver integrated cyber defense and managed detection and response (MDR) services. These providers also invest in threat detection and hunting, threat intelligence, modeling and forensics, incident management and advanced technologies, such as automation, big data, AI and ML, to offer a holistic approach to proactive threat mitigation and advanced security.

## Eligibility Criteria

1. Offer standard services, including **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services, to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, security information and event management (SIEM) services**, security advisors and auditing support, either remotely or at clients' site
3. MDR-specific capabilities, including **advanced threat intelligence and behavior-based and human**-led threat hunting, delivering **offensive and defensive** security capabilities with a unified view for reporting and metrics
4. Possess **accreditations** from security tools vendors
5. **Manage own SOCs**
6. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
7. Offer a variety of tiered pricing models

### Observations

The Next-Gen SOC and MDR Services delivered by large providers reflect a strategic shift toward intelligent, risk-aligned and industry-specific cybersecurity models. Providers in this space are integrating AI and ML across detection, threat hunting and response workflows, enabling rapid decision-making and predictive threat mitigation. Increasingly, SOCs are built to easily manage complex IT and OT environments, offering integrated visibility and response across enterprise and operational systems.

Proactive defense is becoming the de-facto norm, with continuous threat intelligence enrichment, automation-driven detection and precision-guided response actions. Service providers are aligning SOC and MDR offerings with zero trust principles, ensuring identity-centric controls, adaptive trust models and granular policy enforcement. In addition, emphasis on verticalized solutions is deepening, with providers offering industry-specific threat intelligence, compliance alignment and tailored use cases to address unique sectoral risks.

A critical differentiator of modern SOCs is the blend of expert human analysis and automated decision engines, where human expertise sharpens machine-driven insights for higher fidelity and contextualized responses. Providers are engineering SOC platforms that automate detection and response and strengthen long-term cyber resilience through risk-based prioritization, continuous posture improvement and integrated incident management frameworks. Large providers are evolving their SOC models to deliver sustainable, business-aligned protection strategies that adapt dynamically to an organization's risk profile and operational needs.

From the 116 companies assessed for this study, 29 qualified for this quadrant, with twelve being Leaders and one Rising Star.

accenture

**Accenture** has expanded its cybersecurity capabilities through strategic partnerships and service launches with Google. Accenture and CrowdStrike have collaborated to drive cybersecurity transformation, helping clients navigate innovation and growth.

Atos

**Atos** has launched AI-powered managed detection and response (MDR) services, offering round-the-clock protection and response to cyberthreats. The company opened a new SOC in Mexico to provide advanced cybersecurity services across North and South America.

Capgemini

**Capgemini's** next-generation SOC aims to enhance cybersecurity defenses by leveraging AI and GenAI to improve threat detection, reporting and response. This includes integrating AI to reduce analyst fatigue, guide investigations and provide real-time threat response.

Deloitte.

**Deloitte's** Managed Extended Detection and Response (MXDR) service combines leading technology and service innovation to provide 24/7 prevention, detection and response capabilities, helping reduce cyberattacks on critical networks and assets.

EY

**EY** announced a strategic alliance with BlueVoyant to help enterprises deploy and effectively run Microsoft 365 E5 advanced security tools. EY offers 24/7 threat monitoring, detection and response capability to rapidly detect security incidents and minimize their impact.

HCLTech

**HCLTech** has collaborated with Google Cloud Security to provide AI-driven MDR solutions, empowering enterprises with comprehensive security coverage to respond to cyberthreats. HCLTech and AWS have entered a strategic collaboration to accelerate GenAI adoption.

**IBM** has introduced new advancements to its managed detection and response (MDR) service offerings, incorporating agentic AI and automation capabilities designed to support autonomous security operations and predictive threat intelligence for clients.

**Infosys**' SOCs are built around modular, scalable platforms that integrate seamlessly with client-owned or third-party tools, offering comanaged or fully managed models tailored to enterprise and public sector needs.

Kroll

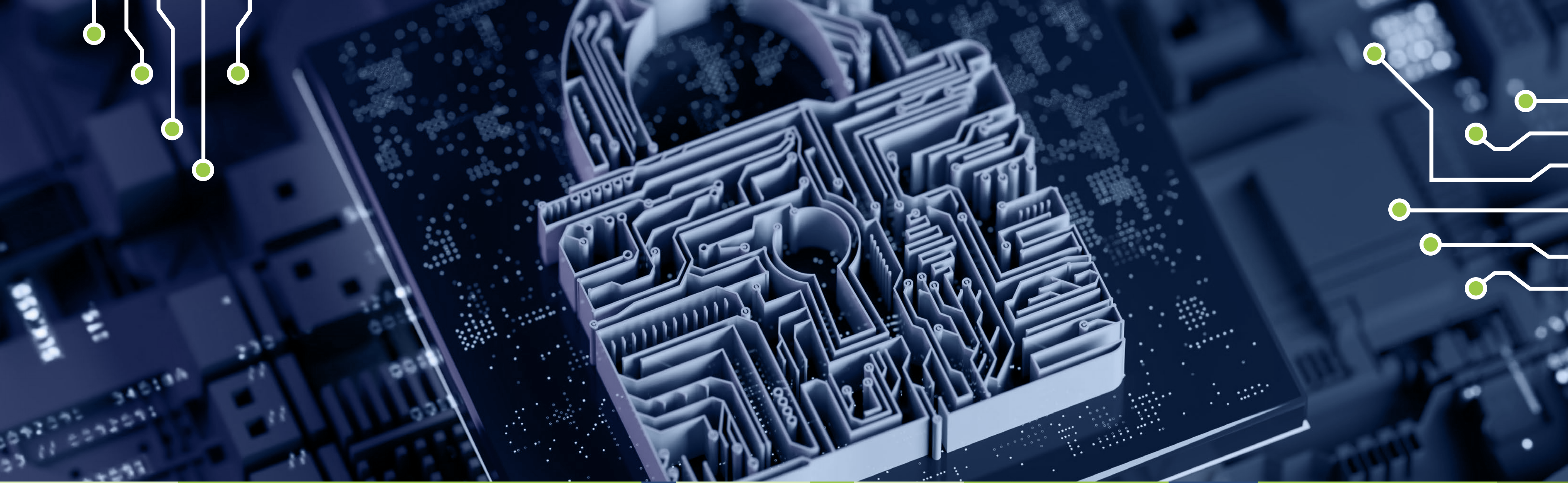
**Kroll** offers Responder managed detection and response (MDR) service, providing extended security monitoring round the clock, earlier insight into targeted threats and complete response to contain and eradicate threats across digital estates.

**PwC** has announced two new service offerings: the launch of its Threat and Vulnerability Managed Service and the expansion of its Third-Party Risk Management service. PwC and Cynalytica announced a partnership to define the next frontier in industrial cybersecurity.

**TCS** has partnered with Google Cloud to launch AI-powered cybersecurity solutions, including an MDR solution and a Secure Cloud Foundation solution. These solutions aim to enhance businesses' threat detection and response capabilities, even in non-cloud environments.

**Wipro** has partnered with CrowdStrike to modernize enterprise security operations with a new integration, the Falcon Next-Gen SIEM. Wipro's AI-MDR services, powered by Palo Alto Networks' Cortex XSIAM Autonomous SecOps platform, offer a unified view of security operations.

**NTT DATA** (Rising Star) has partnered with Palo Alto Networks to deliver AI-driven, cloud-to-edge cybersecurity solutions, introducing its Managed Extended Detection and Response (MXDR) service powered by Cortex XSIAM.



# Next-Gen SOC/MDR Services – Midmarket

## Who Should Read This Section

This report is valuable for service providers offering **Managed Detection and Response (MDR)** Services in the **U.S.** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence. This report guides enterprises in selecting **Managed Detection and Response (MDR)** providers that enhance security through scalable, innovative managed services using AI, ML and automation for cost-effective defense.

### Cybersecurity professionals

Should read this report to understand SOC compliance and strategy, and IT managers can identify incident management and MDR providers that enhance detection and respond efficiently.

### Technology professionals

Should read this report to know security trends and providers' tailored platforms. Compliance leaders can find SOC-aligned providers, and IT leaders can access vendor-neutral expertise.

### Business professionals

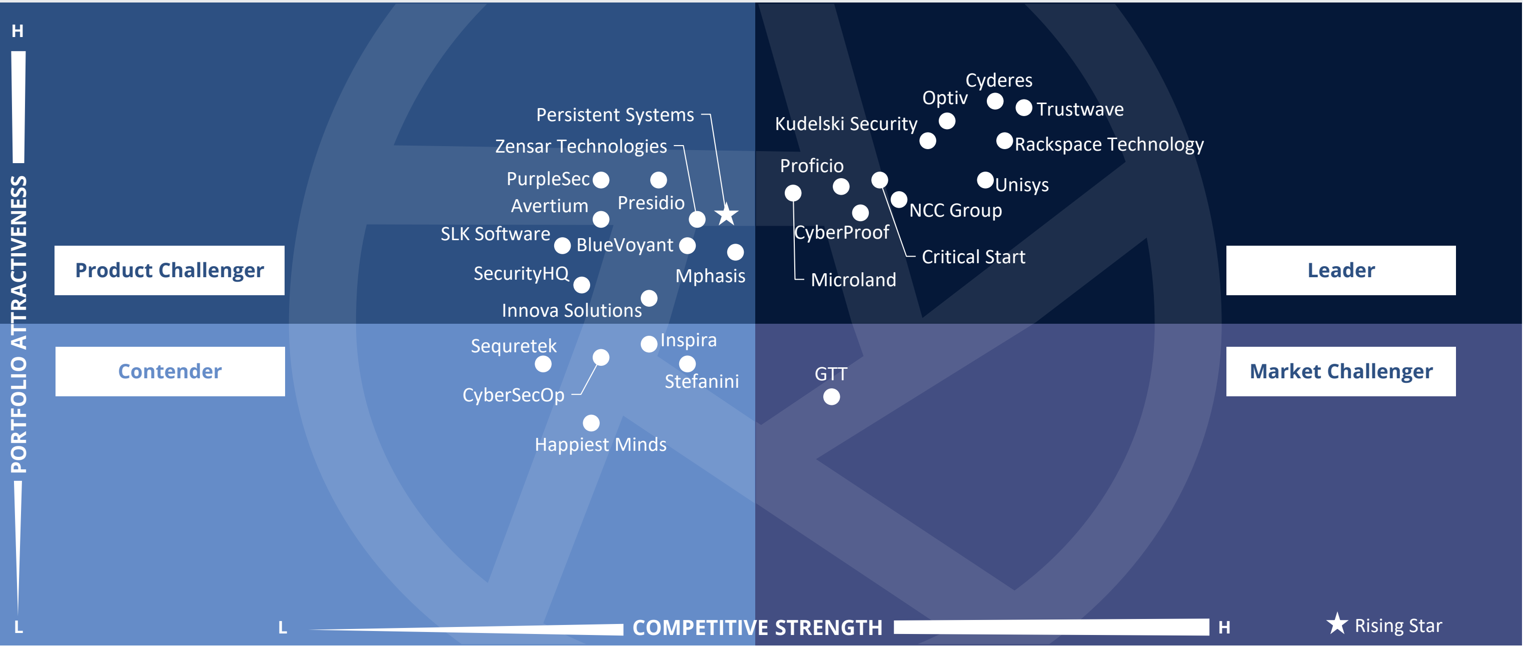
Must read this report to gain valuable insights into simplifying security operations. It offers practical solutions to reduce complexity and enhance efficiency.

ISG Provider Lens™

Source: ISG RESEARCH

## Cybersecurity – Services and Solutions
## Next-Gen SOC/MDR Services – Midmarket

U.S. 2025



This quadrant evaluates providers integrating **advanced MDR** capabilities with **AI-driven analytics, automated response** and **real-time threat intelligence** to deliver **unified**, proactive **security operations** across **hybrid IT and OT** environments.

*Gowtham Sampath*

### Definition

Providers assessed in this quadrant offer services related to the continuous monitoring of IT and OT infrastructures by a security operations center (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle from identification to response and remediation.

Next-Gen SOC providers are in demand to strengthen enterprises' security posture and improve the effectiveness of security programs. They blend traditional managed security services with innovation to deliver integrated cyber defense and managed detection and response (MDR) services. These providers also invest in threat detection and hunting, threat intelligence, modeling and forensics, incident management and advanced technologies, such as automation, big data, AI and ML, to offer a holistic approach to proactive threat mitigation and advanced security.

### Eligibility Criteria

1. Offer standard **services, including security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services, to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, security information and event management (SIEM) services**, security advisors and auditing support, either remotely or at clients' site
3. MDR-specific capabilities, including **advanced threat intelligence** and **behavior-based and human-led threat hunting**, delivering **offensive and defensive** security capabilities with a **unified view** for reporting and metrics
4. Possess **accreditations** from security tools vendors
5. **Manage own SOCs**
6. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
7. Offer a variety of tiered pricing models

### Observations

Midmarket cybersecurity providers are differentiating in the Next-Gen SOC/MDR Services landscape by offering agility, tailored services and context-aware security operations that rival the scale-driven models of larger players. These providers focus on blending automation, AI and ML with expert-led analysis to create SOCs that are efficient and contextually intelligent. Another key characteristic is their commitment to risk-aligned protection, especially in industries such as healthcare, manufacturing and financial services, where regulatory compliance and operational uptime are critical.

Compared to large providers that emphasize the breadth of portfolio, midmarket providers are prioritizing threat detection use cases aligned to MITRE ATT&CK®, reducing mean time to respond (MTTR) through real-time orchestration and investing in specialized capabilities such as cloud-native SOC, OT security integration and behavior-based insider threat detection. Their ability to integrate with client-owned tools across SIEM, SOAR, EDR and IAM stacks also delivers cost efficiency and quick onboarding.

These providers are also innovating through modular service delivery, offering comanaged SOCs, compliance-driven dashboards and digital threat playbooks tailored to regional and industry-specific threats. Using shared threat intelligence networks and collective defense models ensures that clients benefit from the early detection of zero-day threats without compromising operational autonomy. The competitive edge of midmarket providers lies in focus, flexibility and speed of execution.

From the 116 companies assessed for this study, 27 qualified for this quadrant, with eleven being Leaders and one Rising Star.

### Critical Start

**Critical Start's** Cyber Range offers clients an immersive environment to simulate real-world attack scenarios aligned with MITRE ATT&CK®. Offering the Cyber Range as part of its innovative platform accelerates onboarding and strengthens customer engagement.

### CyberProof®
A UST Company

**CyberProof** expanded its partnership with Google Cloud to enhance its Managed XDR services. This collaboration leverages Google Chronicle Security Operations and other Google Cloud Security solutions to deliver advanced threat detection and response capabilities.

### Cyderes

**Cyderes**' acquisition of Outpost Security marks a significant evolution in its managed cybersecurity services, prioritizing risk-based alerting (RBA) and Splunk-centric threat detection to combat modern cyberthreats and deliver quick, precise threat detection and response.

### KUDELSKI SECURITY

**Kudelski Security** integrates leading platforms such as Microsoft, Crowdstrike, Splunk, Google Secops and Claroty into its proprietary FusionDetect™platform. The company's services provide 24/7 threat detection and response, helping clients reduce exposure, risk and build cyber resilience.

### MICROLAND®

**Microland** has partnered with Securonix to elevate its managed SOC offerings. This strategic partnership aims to provide enterprises with advanced AI-based solutions for threat detection and mitigation.

### NCC Group

**NCC Group** Managed Extended Detection and Response (MXDR) enhances Microsoft Sentinel by tailoring integrations, automating enrichment and accelerating threat detection aligned to organizations' specific risk profiles.

### Optiv

**Optiv** launched its MDR service on the Google Security Operations platform, utilizing Google AI to analyze extensive log data for accelerated threat detection and response. It announced Optiv Market System, a single reference architecture for the cybersecurity industry.

Proficio

**Proficio** introduced an AI Assistant Module integrated into its ProSOC MDR platform, enhancing visibility and providing actionable response recommendations. The AI Assistant helps analysts search across multiple logs but lacks expertise in specific SIEM query languages.

rackspace technology

**Rackspace Technology** signed a multi-year strategic collaboration agreement with AWS to deliver accelerated digital transformation for customers. The company also joined the AWS Generative AI Partner Innovation Alliance, aiming to enhance its cybersecurity offerings.

Trustwave

**Trustwave** has a strategic and extensive partnership with Microsoft, being early adopters of security products such as Microsoft Sentinel and Microsoft Copilot. The company has tailored its offerings to align with Microsoft's innovations and investment in cybersecurity.

unisys

**Unisys** is advancing its next-generation SOC capabilities by embedding AI and analytics at the core of its MXDR framework. The company's investment in GenAI and automation is driving transformation across its managed security services portfolio.

Persistent

**Persistent Systems'** (Rising Star) SOC Copilot enhances SOC efficiency through features such as Malware Information Sharing Platform (MISP) integration, Knowledge Graphs for Configuration Management Databases (CMDB), automated reporting and unified threat intelligence.

# Kudelski Security

Leader

> “Kudelski Security integrates advanced AI-driven technologies with human expertise to offer proactive threat detection and rapid response capabilities. By providing tailored solutions for regulated industries, the firm ensures a holistic approach to security.”
>
> *Gowtham Sampath*

## Overview

Kudelski Security is an innovative and independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is a division of the Kudelski Group which has a dual headquarters in Phoenix, Arizona, and in Cheseaux-sur-Lausanne, Switzerland, operating in 20 countries with over 1,800 employees. The company offers AI-augmented, risk-based Detection & response capabilities, Proactive Threat Hunting and CTEM services operating from its 4 Cyber Fusion Centers (Switzerland, Spain, USA) and proprietary FusionDetect™ Platform.

## Strengths

**Proactive threat detection with AI and automation:** Kudelski Security employs a sophisticated mix of AI and ML technologies, proven methodologies and rich security expertise to enhance threat detection capabilities. Its use of automation across its MDR platform improves response time and ensures the detection and swift mitigation of known threats. Kudelski Security constantly analyzes the dynamic threat landscape, applies advanced algorithms to identify anomalous behaviors, enhancing its ability to detect zero-day threats and advanced persistent threats (APTs) early, minimizing the potential impact on clients.

**Human-led threat hunting and forensics expertise:** Beyond automation, Kudelski Security integrates skilled cybersecurity experts into its threat detection process. Its human-led threat hunting capabilities allow for deep insights into complex security incidents, using contextual awareness to identify vulnerabilities that automated systems may overlook.

**Holistic cyber defense:** Kudelski Security incorporates various layers of protection for IT & OT environments, including CTEM, threat detection, proactive threat hunting, response, recovery, policy management and posture improvement. Its comprehensive threat management ensures that businesses can detect and address threats in real-time while continuously improving their security posture.

## Caution

Kudelski Security’s robust solutions and reliance on advanced security technologies require organizations to have a certain level of security maturity and infrastructure. Enterprises with less developed security programs may face challenges in fully leveraging these capabilities without additional support or investment.

# Appendix

# Methodology & Team

The ISG Provider Lens™ 2025 – Cybersecurity – Services and Solutions study analyzes the relevant software vendors/service providers in the U.S. market, based on a multiphased research and analysis process, and positions these providers based on the ISG Research methodology.

**Study Sponsor:**
Heiko Henkes

**Lead Author:**
Gowtham Sampath (U.S., Global - XDR), Bhuvaneshwari Mohan (Global - IAM), and Yash Jethani (Global - SSE)

**Editors:**
Esha Pal and Radhika Venkatachalam

**Research Analyst:**
Sandya Kattimani

**Data Analyst:**
Rajesh Chillappagari and Laxmi Kadve

**Consultant Advisors:**
Doug Saylors and David Gordon

**Project Manager:**
Shreemadhu Rai B

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this study will include data from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. ISG recognizes the time lapse and possible market developments between research and publishing, in terms of mergers and acquisitions, and acknowledges that those changes will not reflect in the reports for this study.

All revenue references are in U.S. dollars ($US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Services and Solutions market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
   - Strategy & vision
   - Tech Innovation
   - Brand awareness and presence in the market
   - Sales and partner landscape
   - Breadth and depth of portfolio of services offered
   - CX and Recommendation

*Author (U.S.and Global - XDR)*

## Gowtham Sampath

**Assistant Director and Principal Analyst, ISG Provider Lens™**

Gowtham Sampath is a Prinicipal Analyst with ISG Research, responsible for authoring ISG Provider LensTM quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices.

In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries. He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

*Author (Global - IAM)*

## Bhuvaneshwari Mohan

**Author and Research Analyst**

Bhuvaneshwari is a Senior Research Analyst at ISG and is responsible for driving and co-authoring ISG Provider Lens™ studies on Digital Business Enablement, Supply Chain, ESG Services and Cybersecurity. She contributes to the research process with necessary data and market analysis, develops content from an enterprise perspective, and authors Global Summary reports. She comes with 8 years of hands-on experience and has delivered insightful custom reports across verticals.

She is a versatile research professional having experience in Competitive Benchmarking, Social Media Analytics, and Talent Intelligence. Prior to ISG, she honed her research expertise in Sales Enablement roles with IT & Digital Services Providers and was predominantly part of Sales Enablement teams.

*Author (Global - SSE)*

## Yash Jethani

**Senior Manager and Principal Analyst**

Yash has over 14 years of professional experience, primarily in the technology, media and telecom (TMT) vertical. He has contributed to thought leadership, market and competitive research, consulting, business development, and due diligence as well as account management cutting across corporate marketing, risk, strategy, and sales functions.

Prior to ISG, Yash worked with KPMG in India supporting their national TMT practice in advisory, thought leadership as well as strategic pursuits. While at IDC, he was responsible for delivering custom as well as syndicated research for Telco & IoT Asia Pacific clients.

He has also had stints with CGI and TCS in supporting their corporate and account marketing initiatives with a focus on next-gen IT delivery within Telco/ Comms verticals. He currently contributes to ISG Provider Lens global research studies as a lead analyst for software defined networks, managed network services as well as telecom and media managed services studies across regions.

Yash holds a PGDM in Telecom & IT supported by an engineering degree in computers. He is also TM Forum certified and actively contributes as a member to the Bangalore Software Process Improvement Network, a non-profit.

*Research Analyst*

## Sandya Kattimani

**Senior Research Analyst**

Sandya Kattimani is a senior research analyst at ISG and is responsible for supporting and co-authoring ISG Provider Lens™ studies on Contact Center, Life Sciences, Mainframes. Sandya has over 6 years of experience in the technology research industry and in her prior role, she carried out research delivery for both primary and secondary research capabilities. Her area of expertise lies in Competitive Intelligence, Customer Journey Analysis, Battle Cards, Market analysis and digital transformation. She is responsible for authoring the enterprise content and the global summary report, highlighting regional as well as global market trends and insights. Prior to this role she has worked as technology research analyst, where she was responsible for project work which includes detail technology scouting, competitive intelligence, company analysis, technologies study and other Ad hoc business research assignments.

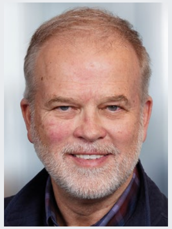
*Study Sponsor*

## Heiko Henkes

**Director & Principal Analyst, Global IPL Content Lead**

Heiko Henkes serves as Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens™ (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as a strategic program manager and thought leader for IPL lead analysts.

Henkes heads Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice. His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation, IT competencies, sustainable business strategies and change management in a cloud-AI-driven business landscape. Henkes is known for his contributions as a keynote speaker on digital innovation, sharing insights on using technology for business growth and transformation.



*IPL Product Owner*

## Jan Erik Aase

**Partner and Global Head – ISG Provider Lens™**

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

## ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens™ research, please visit this webpage.

## ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

## ISG

ISG (Nasdaq: III) is a global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth.

The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.

For more information, visit isg-one.com.

ISG Provider Lens™

JULY 2025

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS