ISG Provider Lens™

Cybersecurity – Services and Solutions

Strategic Security Services – Large Accounts

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

Customized report courtesy of:

HCLTech

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

Table of Contents

Executive Summary 03

Provider Positioning 20

Introduction

Definition 33
Scope of Report 35
Provider Classifications 36

Appendix

Methodology & Team 45
Author & Editor Biographies 46
About Our Company & Research 49

Strategic Security Services – Large Accounts 37 – 43

Who Should Read This Section 38
Quadrant 39
Definition & Eligibility Criteria 40
Observations 41
Provider Profile 43

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- **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.

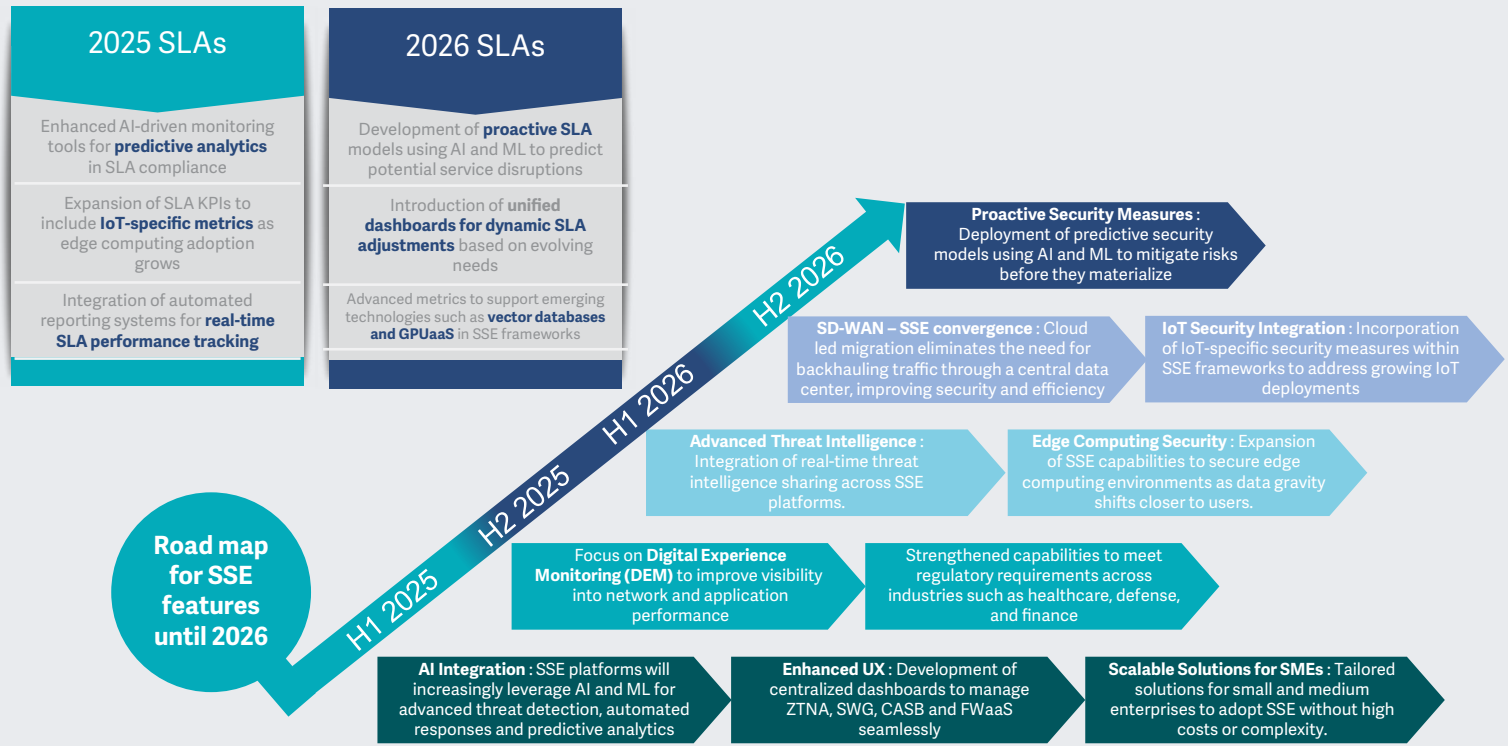
SSE serves a diverse range of customers, including end enterprises, cloud service providers (CSPs) delivering cloud services, network service providers (NSPs) offering network connectivity, and managed service providers (MSPs) providing outsourced IT and security. Large enterprises, characterized by 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 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.



Source: ISG, 2025

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- 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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- 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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

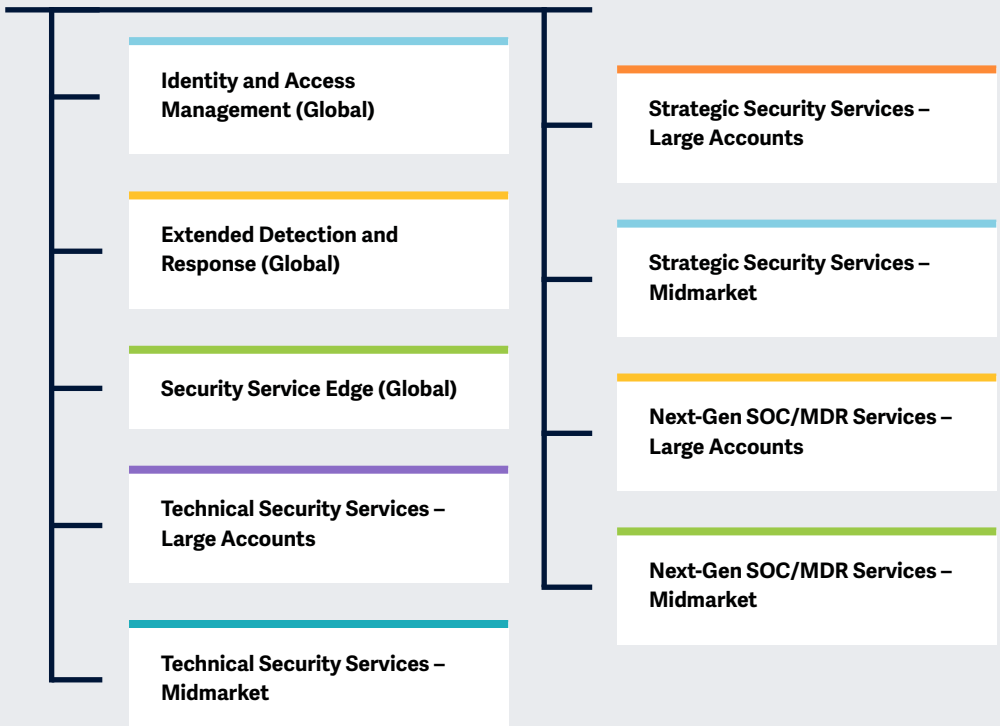
Provider Positioning

	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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Key focus areas for Cybersecurity – Services and Solutions 2025.

Simplified Illustration Source: ISG 2025



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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Introduction

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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).

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

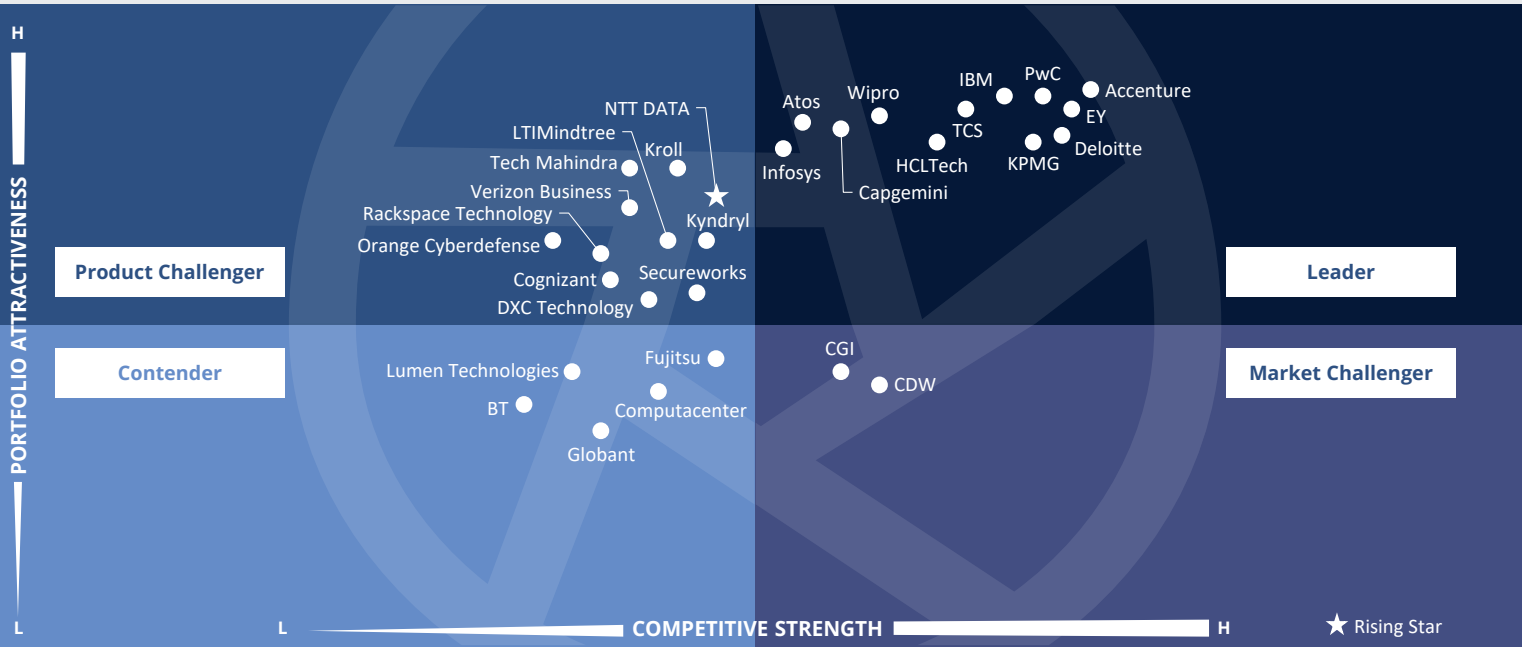
© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Leader

"HCLTech is repositioning cybersecurity as a digital business enabler through a pragmatic mix of advisory expertise, technical implementation and operational maturity with customized strategies to address emerging IT and OT convergence risks."

Gowtham Sampath

HCLTech

Overview

HCLTech is headquartered in Noida, India. It has more than 223,420 employees across over 220 delivery centers worldwide. In FY25, the company generated $13.8 billion in revenue, with IT and Business Services as its largest segment. It has employed approximately 7,500 cybersecurity professionals globally and has over 800 active customers across all major industries, with six cybersecurity fusion centers (CSFCs) and more than 210 global delivery centers. These resources provide consulting coverage across seven dedicated CoEs, with the aim of helping customers accelerate their security journey.

Strengths

Integrated IT-OT security advisory: HCLTech's inclusion of OT within its broad cybersecurity strategy ensures comprehensive protection across industrial and digital domains, bridging the IT-OT gap. Its advisory model incorporates platform-based governance, risk and compliance (GRC) services covering third-party risk management, compliance tracking and operational oversight. This model ensures unified risk visibility and improved response capabilities across enterprise and industrial assets.

AI governance and oversight: HCLTech is actively embedding AI governance and data security into its cybersecurity advisory services, reinforcing its commitment to ethical and secure AI deployment. Its proprietary frameworks such as TRiBE for responsible AI oversight and E.L.E.V.A.T.E. for data-centric security management address AI model integrity, data lineage, privacy risks and algorithmic accountability.

Sector-tailored architecture: HCLTech is expanding its strategic security advisory through industry-specific consulting and security architecture design. It is developing verticalized cybersecurity solutions for various industry verticals. These solutions incorporate domain-aware threat modeling, regulatory alignment and business continuity features that match sectoral operating realities.

Caution

While HCLTech has made strides in strategic advisory, its visibility and brand recall in high-stakes boardroom strategy consulting are perceived as weaker than traditional consulting providers. In-depth focus on quantum risk modeling and secure digital identity could enhance its positioning in emerging threat landscapes.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Study Sponsor

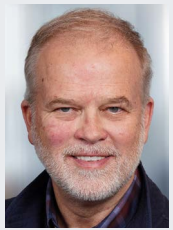
Heiko Henkes

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

JULY, 2025

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS

© 2025 Information Services Group, Inc.
All Rights Reserved