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:

Capgemini

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

Table of Contents

Executive Summary 03

Provider Positioning 18

Introduction

Definition 32
Scope of Report 34
Provider Classifications 35

Appendix

Methodology & Team 44
Author & Editor Biographies 45
About Our Company & Research 49

Strategic Security Services – Large Accounts 36 – 42

Who Should Read This Section 37
Quadrant 38
Definition & Eligibility Criteria 39
Observations 40
Provider Profile 42

Report Author: Bhuvaneshwari Mohan

Resilience, regulation and readiness define the cybersecurity priorities for the UK enterprises in 2025

The UK cybersecurity landscape in 2025 marks a pivotal transition, with cybersecurity evolving beyond a traditional protective function to become a foundational element of national resilience. In 2024, the cybersecurity sector demonstrated strong momentum, achieving a 12 percent annual revenue growth and an 11 percent employment growth, as reported in the UK Cyber Security Sectoral Analysis 2025 published by the Department for Science, Innovation and Technology (DSIT). This growth reflects its economic resilience and expanding role in addressing national and enterprise-level security demands.

The UK government, through its National Cyber Security Centre (NCSC), is orchestrating a new national agenda in which cybersecurity becomes a shared societal responsibility, codified in regulation and enforced through cross-sectoral accountability. Driven by the increasing frequency and severity of cyber incidents, the proliferation of AI-enabled attack vectors, and state-linked actors targeting the UK's democratic, health and economic institutions, the UK government's cybersecurity initiatives have transitioned from fostering innovation to ensuring regulatory maturity, integrating cybersecurity into core strategies for digital transformation, national resilience and supply chain integrity.

The U.K. government has recently implemented various initiatives and continues to amend the regulations to keep up with the fast-changing threat landscape and bolster national cybersecurity:

- **Cyber Security and Resilience Bill:** Announced in July 2024, this forthcoming legislation aims to enhance the UK's cyber defences and protect essential public services by mandating broader protections for digital services and supply chains.
- **Designation of data centres as Critical National Infrastructure (CNI):** In September 2024, the UK government classified data

UK firms now perceive **cyber resilience** as critical to their **reputation, trust and competitive edge.**

centres as CNI to strengthen protections against cyberattacks and IT outages. This move ensures that data centres receive additional government support and priority access to security agencies and emergency services.

- **Establishment of the Laboratory for AI Security Research (LASR):** In October 2024, the UK government announced the creation of a new AI security research lab with £8 million in funding. This initiative aims to bolster the UK's defence against increasing risks associated with cyber warfare, particularly those amplified by AI technologies.
- **Cybersecurity network to enhance national resilience:** In November 2024, UK Research and Innovation (UKRI) launched a new network to strengthen cybersecurity, harness emerging technologies, including quantum, AI, biology, engineering and semiconductors, and better prepare society against future cyber threats.
- **NCSC annual review 2024:** This comprehensive annual review outlines the UK's approach to remaining digitally confident, capable and resilient. It emphasises adapting, innovating and investing to protect and promote national interests in cyberspace. The report highlights the need for businesses in the UK to develop *secure by design* products and emphasises the need to raise cybersecurity standards in all aspects of AI design, development and deployment.

The NCSC reports that the UK faces its most significant nation-state-sponsored cybersecurity threats from countries such as China, Russia, Iran and North Korea. In 2024, the top sectors affected by ransomware activity were academia, manufacturing, IT, legal, charities and construction. The NCSC works closely with industry leaders, government agencies, academic institutions and international partners to promote a unified approach to cybersecurity.

The government's forward trajectory suggests increasing investments in AI risk governance, post-quantum cryptography standards, protective DNS services at scale and the hardening of digital supply chains. These initiatives reflect the UK's commitment to enhancing cybersecurity across various sectors, ensuring the protection of critical infrastructure and staying ahead of evolving cyber threats.

Evolving enterprise challenges

Enterprises across the UK are navigating an increasingly complex cyber landscape characterised by regulatory pressure, fragmented technology ecosystems and a persistent shortage of skilled professionals. Some of the most pressing cybersecurity challenges currently faced by organisations in the UK are:

Mandatory security baselines: Regulatory obligations are extending beyond traditional critical infrastructure sectors to encompass financial services, digital service providers and even advanced manufacturing. Enterprises must move beyond annual audits and invest in continuous assurance to maintain compliance and resilience. As regulations such as NIS2, DORA and the NHS DSP Toolkit mature, organisations face overlapping compliance regimes without harmonised implementation pathways. This situation drives up audit fatigue, increases complexity in governance workflows and raises the demand for continuous assurance rather than static compliance. Non-compliance may increasingly affect access to insurance, public tenders or investor confidence.

AI arms race: Technological acceleration, particularly the proliferation of GenAI, is amplifying the scale and sophistication of cyber threats. Attackers are outpacing defenders in leveraging AI, resulting in a widening gap between threat evolution and defence readiness. The pace at which AI is industrialising cybercrime (e.g., automated phishing, deepfake social engineering) suggests that defenders must shift from reactive guidance to proactive AI-enabled threat hunting and simulation. Board-level awareness must include the risk of AI model exploitation, especially for firms using GenAI tools internally or in customer-facing services.

Convergence of physical and digital threats: The targeting of the NHS, water utilities and energy grids shows that cyber-physical integration is the new norm. Incidents such as the Synnovis ransomware attack underscore the real-world consequences of cyber disruption and show how systems are vulnerable to operational sabotage.

Security tools sprawl: Many organisations have invested in multiple-point solutions that do not interoperate. The legacy of fragmented security tools and siloed data results in diminished visibility, alert fatigue and suboptimal response capability. CISOs now recognise that technical debt in cybersecurity is becoming an enterprise risk in itself.

Talent shortage: Enterprises are finding it increasingly challenging to manage security internally. The shortage is no longer limited to high-end technical skills; it now includes governance, compliance interpretation and third-party risk management, particularly in mid-senior roles that require regulatory or sector-specific knowledge. Without a workforce strategy that addresses diversity, early STEM engagement and sectoral mobility, the UK risks ceding its long-term defensive capabilities to adversaries investing in state-supported cyber education pipelines.

Supply chain and third-party risks: For enterprises, resilience now requires a full-spectrum view of third-party digital dependencies to comprehensively understand their digital exposure. State actors and ransomware groups are exploiting supply chains to reach more secure targets, and small and midsize enterprises are increasingly becoming the frontline vulnerabilities in larger ecosystems.

Market trends redefining security service expectations

Several defining trends are reshaping how enterprises in the UK procure cybersecurity services:

1. Compliance-led procurement: Security services are increasingly procured through a compliance lens. The ability to map services to sector-specific frameworks is a baseline expectation. Providers that productise compliance into operationally simple offerings will gain traction. Enterprises seek partners that can streamline compliance as an embedded, ongoing service rather than a point-in-time project.

2. Converged and integrated services: Organisations are increasingly moving away from fragmented security stacks and demanding unified, interoperable solutions that provide end-to-end visibility and control. The modern enterprise expects providers to deliver integrated platforms that combine MDR, XDR, IAM and security posture management through a centralised operational lens. Point solutions are losing favour to platforms that offer comprehensive coverage and integrated insights. Clients are seeking unified detection, identity protection, data monitoring and threat response and are gravitating towards providers that offer full-spectrum services with seamless interoperability and centralised visibility.

3. Sector-specific expertise: Beyond technical capability, UK enterprises now expect providers to demonstrate in-depth contextual understanding of sector-specific requirements. In the public sector, this means delivering architectures that are compliant with NCSC and GovAssure guidelines. In healthcare, providers must be able to align services with NHS Digital standards, DSPT expectations and ransomware containment protocols. For energy providers, familiarity with NIS2 directives and OT security is essential. Enterprises are increasingly rejecting generic offerings in favour of those tailored to their regulatory, operational and cultural environments.

4. AI-enhanced security with operational value: While AI and automation are expected in modern security offerings, enterprises are becoming more discerning. Organisations demand demonstrable outcomes. Providers must show how AI enhances triage accuracy, enables contextual threat detection and improves operational decision-making. Increasingly, the transparency and explainability of AI models are being viewed as key differentiators, particularly in regulated environments. Enterprises are also looking for providers that can integrate AI-driven security with broader AI governance frameworks to ensure ethical and controlled deployment across the business.

5. Sovereignty and localisation of cyber operations: With geopolitical tensions and regulatory scrutiny on the rise, enterprises in the UK are placing heightened emphasis on data sovereignty, operational localisation and trust. There is growing demand for UK-based SOCs, locally staffed incident response teams and data residency assurances that meet sector-specific compliance requirements. This demand is especially pronounced in the government, defence, healthcare and legal sectors, where offshore processing or third-party dependencies raise significant concerns. Providers that invest in UK-specific infrastructure, talent and regulatory alignment are well positioned to secure high-trust and high-compliance contracts and to strengthen long-term client relationships.

Enterprises are opting for trusted, stable partners that offer both scale and agility. This trend favours providers capable of balancing tailored consulting with repeatable, automation-enhanced services, particularly in regulated sectors. Clients increasingly expect evidence-based security metrics that align with enterprise risk frameworks, rather than generic SLAs. Providers must deliver continuous control validation, attack simulation and posture benchmarking as part of standard operations.

The sector is shifting toward high-value services, particularly in AI-driven threat intelligence, SaaS security and automation, where providers are optimising productivity, reflecting increased technological sophistication and operational efficiency.

Redefining the cyber value proposition

Enterprises today require a fundamentally different security mindset — one that supports digital innovation and operational agility without compromising governance or control. As the demands of digital transformation intensify, the divide between compliance-oriented security and security that enables business growth is becoming increasingly pronounced. Cybersecurity is no longer viewed solely as a technical concern; it has become a core enterprise risk issue, shaping decisions around M&As, supply chain relationships, ESG performance and digital investment strategies. In this context, organisations are actively seeking partners that can bridge this widening gap by aligning security with strategic business objectives.

To meet these expectations, service providers must reengineer their portfolios around resilience-driven outcomes. Reengineering in this context means moving beyond isolated, tactical solutions and offering integrated, end-to-end capabilities, from continuous attack surface monitoring and threat detection to incident response, crisis management and regulatory reporting. Crucially, providers must equip clients to communicate their security posture to regulators, customers, investors and executive leadership. Achieving this requires building practical, provable, auditable and transparent services that demonstrate cyber maturity and operational readiness.

UK enterprises require a more integrated approach where security is embedded across operations, rather than being siloed as a standalone function. The shift must move from *prevent and insure* to *absorb and recover*, underpinned by tested playbooks, defined recovery SLAs and resilient third-party ecosystems that ensure continuity in the face of disruption.

Report Author:
Bhuvaneshwari Mohan (Global - IAM)

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

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

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

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

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

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

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

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

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

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

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

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

Challenges in implementing IAM

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

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

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

assistance while maintaining human oversight in decision-making.

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

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

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

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

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

Report Author: Gowtham Sampath (Global - XDR)

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

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

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

Key trends and developments

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

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

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

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

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

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

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

Report Author: Yash Jethani (Global - SSE)

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

Why you need zero trust principles

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

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

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

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

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

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

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

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

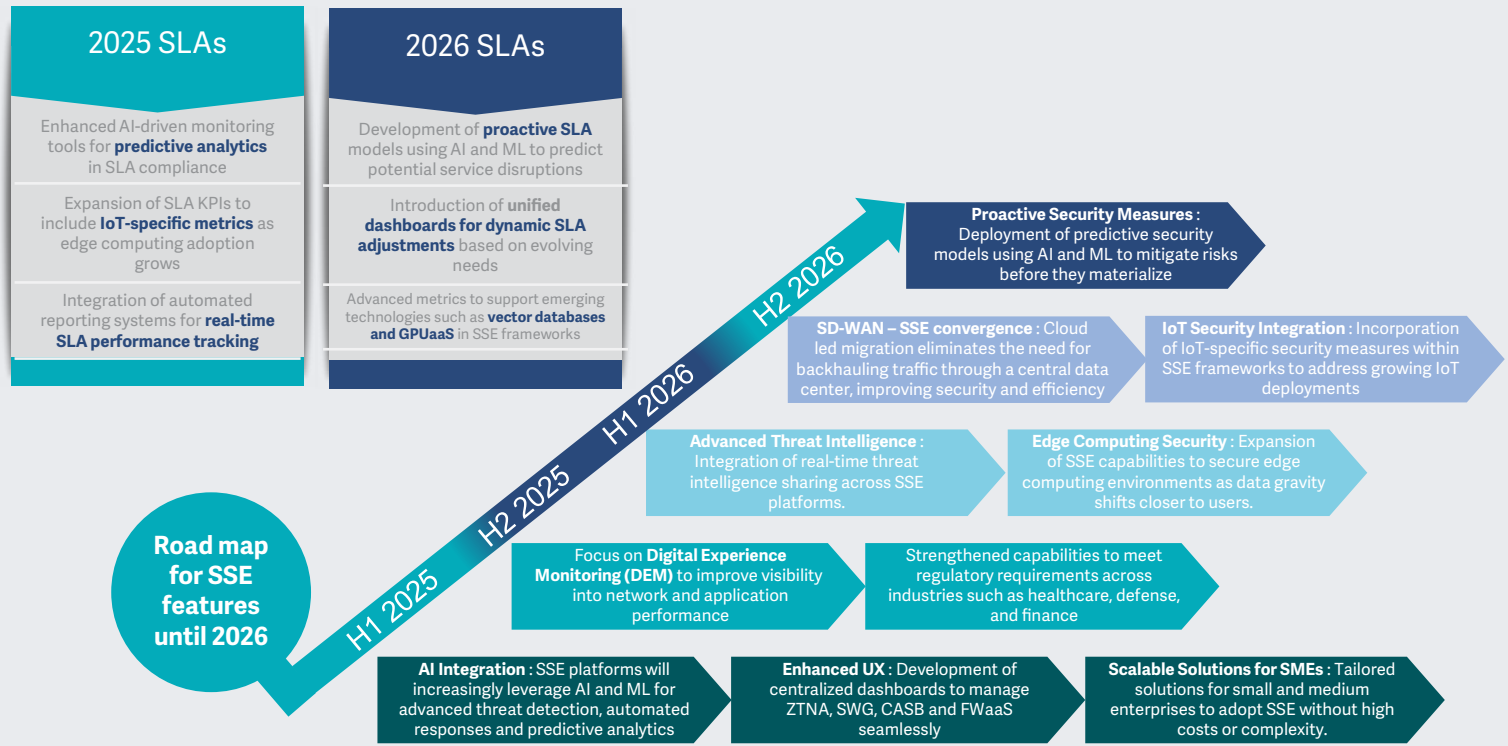
SSE provides the cloud-delivered security stack to implement zero trust principles at scale across distributed environments. It replaces traditional perimeter security with a flexible, identity-centric approach to secure remote work, cloud adoption and mobile access scenarios without sacrificing protection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

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

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

SSE components can be broken into four major buckets:

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



Source: ISG, 2025

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

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

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

Technology trends in SSE:

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

Business trends in SSE:

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

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

Recent acquisitions in the zero trust or SSE space:

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

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

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

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

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

Provider Positioning

Page 1 of 14

	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
Adarma	Not In	Not In	Not In	Not In	Contender	Not In	Leader	Not In	Contender
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
Bechtle	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	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

Provider Positioning

Page 2 of 14

	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
Bridewell	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader
Broadcom	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
Capgemini	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
Capita	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Contender	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	Not In	Contender	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Contender	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

Provider Positioning

Page 3 of 14

	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
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Cognizant	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In	Product Challenger	Not In
Computacenter	Not In	Not In	Not In	Leader	Not In	Product Challenger	Not In	Contender	Not In
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

Provider Positioning

Page 4 of 14

	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
CyberProof	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
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

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
Fischer Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
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	Product Challenger	Not In	Contender	Not In	Market Challenger	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Getronics	Not In	Not In	Not In	Not In	Leader	Not In	Contender	Not In	Contender
Globant	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Gopher Security	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 6 of 14

	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	Rising Star ★	Not In	Rising Star ★	Not In	Leader	Not In
Insight	Not In	Not In	Not In	Market Challenger	Leader	Not In	Contender	Not In	Not In
Integrity360	Not In	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Leader
ITC Secure	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender

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
JumpCloud	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
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	Not In	Not In	Product Challenger	Not In	Not In	Not In
Kroll	Not In	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Kudelski Security	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger
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
Logicalis	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Lookout	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 8 of 14

	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
LRQA Nettitude	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
LTIMindtree	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
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	Rising Star ★	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	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
NCC Group	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader	Not In	Leader
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 9 of 14

	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
NTT DATA	Not In	Not In	Not In	Product Challenger	Not In	Leader	Not In	Product Challenger	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
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
Orange Cyberdefense	Not In	Not In	Not In	Leader	Not In	Product Challenger	Not In	Rising Star ★	Leader
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Performanta	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Persistent Systems	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger

Provider Positioning

Page 10 of 14

	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
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
Quorum Cyber	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Contender
Rackspace Technology	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 11 of 14

	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	Contender	Not In	Not In	Not In
SecurityHQ	Not In	Not In	Not In	Not In	Product Challenger	Not In	Leader	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	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Smarttech247	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger

Provider Positioning

Page 12 of 14

	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
Softcat PLC	Not In	Not In	Not In	Market Challenger	Market Challenger	Contender	Not In	Not In	Not In
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
Sopra Steria	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In
Talion	Not In	Not In	Not In	Not In	Contender	Contender	Contender	Contender	Not In
Tata Communications	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★
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	Leader
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 13 of 14

	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
Telefonica Tech	Not In	Not In	Not In	Not In	Contender	Not In	Market Challenger	Not In	Market Challenger
Telstra	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Thales	Product Challenger	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Trellix	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
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	Product Challenger	Not In	Product Challenger	Not In	Rising Star ★
Unisys	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Verizon Business	Not In	Not In	Not In	Not In	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

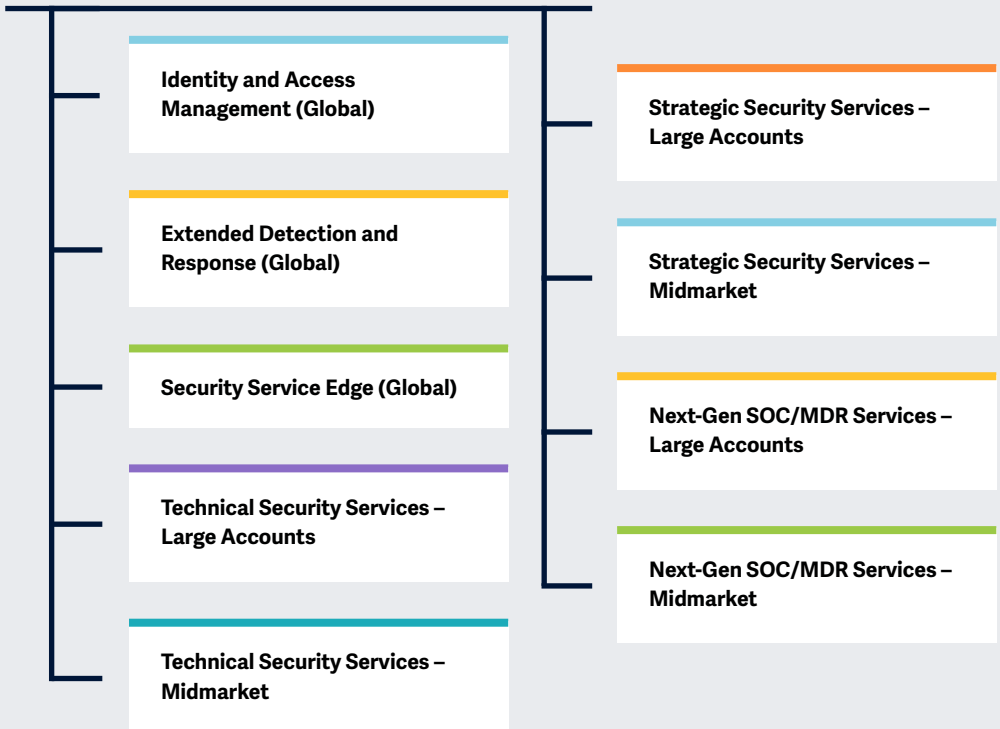
Provider Positioning

Page 14 of 14

	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
Wavestone	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
WWT	Not In	Not In	Not In	Contender	Market Challenger	Not In	Not In	Not In	Not In
Zensar Technologies	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In

Key focus areas for
Cybersecurity – Services and Solutions 2025.

Simplified Illustration Source: ISG 2025



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 organisations to reassess their security frameworks amidst emerging threats. Simultaneously, the commoditisation 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 organisations as they navigate between operational technology (OT) and IT. The scarcity of skilled cybersecurity personnel has amplified this complexity, spurring accelerated demand for managed security services (MSS) as companies seek external expertise to fortify their defences.

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 behavioural and contextual intelligence to enhance their security posture.

Scope of the Report

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

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

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

Our study serves as the basis for important decision-making by covering providers' positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing vendor relationships and potential engagements.

Provider Classifications

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

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

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

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

Provider Classifications: Quadrant Key

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

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

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

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

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

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

Strategic Security Services – Large Accounts

Who Should Read This Section

This report is valuable for service providers offering **strategic security services (SSS)** in the **UK** to understand their market position and for large enterprises looking to evaluate these providers. Strategic security services, including frameworks, assessments, architecture consulting, and governance, are vital in developing cohesive cybersecurity strategies. The report highlights addressing key enterprise challenges, aligning security strategies with emerging threats and technologies and fostering resilience, compliance and proactive management for a robust cybersecurity approach.

Cybersecurity professionals

Should read this report for insights into security trends and the critical role of consulting services in driving business continuity and resilience strategies.

Procurement professionals

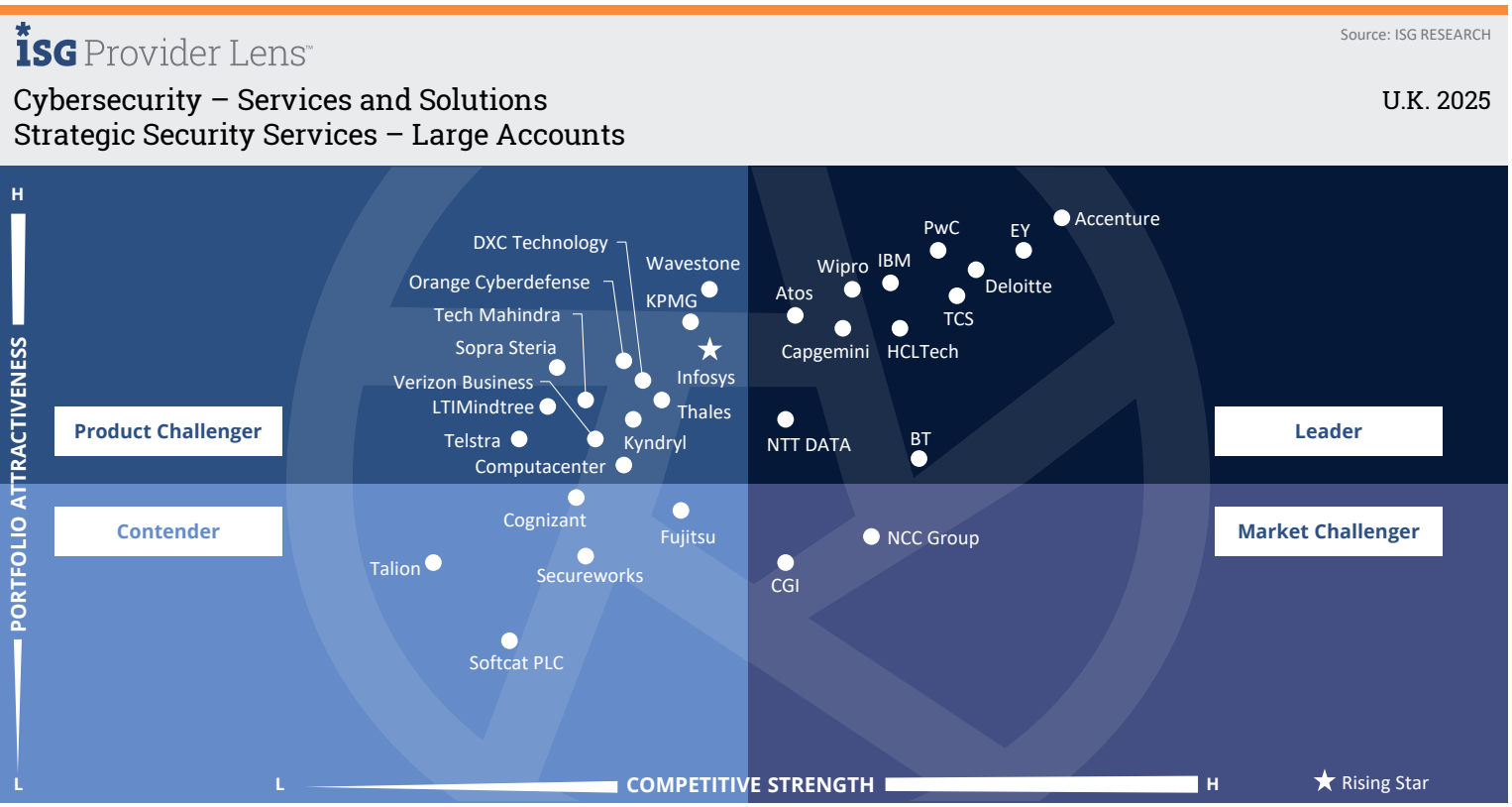
Should read this report to identify potential providers with robust partnerships and certifications and make informed sourcing decisions.

Risk management professionals

Involved in risk management, compliance and governance should read the report to understand the providers' risk-based approaches and risk assessment services.

Data management professionals

Including security and privacy officers, should read this report to understand the ever-evolving data protection standards and regulations in the UK and EU.



This quadrant analyses providers offering **in-depth security advisory, risk-driven frameworks** and **board-level security strategies** to **large enterprises** navigating **regulatory complexity, zero trust** and **cyber maturity journeys.**

Bhuvaneshwari Mohan

Definition

SSS providers assessed in this quadrant offer IT and OT security consulting. Services include security audits, assessments, and 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 roadmaps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to improve cyber literacy and response among enterprise board members and employees.

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

Eligibility Criteria

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

Observations

Strategic security service providers must transition to business-aligned, outcome-driven advisory services focussed on operational resilience and regulatory assurance. This transition requires moving beyond traditional risk assessments to support continuity planning, board-level risk governance and compliance with mandates such as DORA, NIS2, CAF and FCA resilience frameworks.

Regulatory advisory must extend into horizon scanning, scenario-based planning and change management. Providers should enable cross-functional integration across CISOs, risk officers, compliance leads and boards, embedding cybersecurity into enterprise governance rather than treating it as a technical silo.

AI risk governance is now a core advisory pillar. Providers must support the secure and compliant use of GenAI and automation through model risk assessments, AI red teaming, privacy oversight and alignment with NCSC guidance. Transparency, explainability and ethical deployment must be embedded in all AI security engagements.

Third-party and supply chain risk services are also critical. Providers should deliver continuous vendor risk assessments and integrate supplier risk management into GRC frameworks.

Board enablement is becoming a strategic imperative. Providers must quantify cybersecurity ROI, link cyber risk to financial exposure and translate threat scenarios into actionable business terms.

Lastly, delivery models must combine global scale with a strong UK presence. Firms with UK-based consultants, regulatory fluency and access to NCSC programmes will have a clear advantage. To lead, providers must offer sector-specific resilience road maps, integrated advisory and UK-grounded cyber risk governance.

From the 122 companies assessed for this study, 32 qualified for this quadrant, with 12 being Leaders and one Rising Star.

accenture

Accenture is recognised for embedding cybersecurity into enterprise transformation, M&A and sustainability programmes. Its presence in the UK is enhanced by regulatory expertise and the strategic integration of cyber into CXO and board-level priorities.

Atos

Atos brings niche strengths in industrial and OT cybersecurity strategy. Its integration of threat intelligence with critical infrastructure resilience planning makes it a strong fit for manufacturing and energy verticals with high operational risk.

BT

BT's strategic services benefit from its national presence and critical infrastructure alignment, offering a practical cyber strategy rooted in operational realities. Its advisory depth in securing converged networks and OT environments supports high-assurance sectors in the UK.

Capgemini

Capgemini combines cybersecurity strategy with business reinvention, using risk-based frameworks to integrate security in digital transformation. Its strength lies in orchestrating enterprisewide governance across hybrid estates, especially in regulated industries.

Deloitte.

Deloitte leads with board-level cybersecurity influence, offering enterprisewide strategy informed by deep risk, regulatory and M&A experience. Its ability to map geopolitical risk into cybersecurity programmes makes it uniquely equipped for complex global organisations.

EY

EY combines advanced technologies, a holistic security approach and strong client relationships to address evolving cyber threats. Strategic partnerships, global reach, thought leadership and industry-specific insights make EY a trusted advisor in cybersecurity.

HCLTech

HCLTech approaches strategy through automation-led governance and cyber resilience modelling. Its differentiator lies in combining technical visibility with board-level narratives, helping organisations move from reactive controls to sustainable cyber postures.

IBM merges extensive R&D capabilities with strategic cyber advisory, offering AI-led risk modelling and threat-informed strategy. Its global X-Force threat data fuels forward-looking cybersecurity programmes for enterprises navigating digital transformation in the UK.

NTT DATA provides a robust cybersecurity services suite that emphasises a zero trust approach to business resilience. Its focus on strengthening partner collaborations and expanding capabilities showcases its value proposition for clients.

PwC's strategic cyber services are well known for board-level engagement and regulatory foresight. Its ability to embed security into transformation, ESG and governance agendas makes it a trusted advisor across the regulated sectors in the UK.

TCS delivers strategic cyber advisory with a strong technology-embedded focus, aligning security with large-scale IT modernisation. Its emphasis on secure-by-design principles supports transformation agendas in financial and public sector ecosystems in the UK.

Wipro's strategic services leverage its global delivery model to build scalable, risk-aligned cybersecurity programmes. Its focus on converging digital, cloud and identity strategies supports enterprise resilience across the UK's hybrid infrastructure landscape.

Infosys (Rising Star) strategically embeds cybersecurity into enterprise agility programmes, particularly via its Cobalt cloud ecosystem. Its focus on control maturity, transformation assurance and regulatory alignment supports global firms navigating cloud-first strategies.

Leader

"Capgemini provides comprehensive risk assessments, tailored security strategies, proactive threat detection and continuous monitoring to help organisations maintain robust cybersecurity and compliance."

Bhuvaneshwari Mohan

Capgemini

Overview

Capgemini is headquartered in Paris, France. It has more than 341,100 employees worldwide. In FY24, the company generated €22.1 billion in revenue, with Applications and Technology as its largest segment. Capgemini provides strategic security services in the UK, assisting organisations in developing and executing long-term cybersecurity strategies. These services encompass risk management, policy framework development and aligning security initiatives with business objectives to ensure strong protection and resilience against cyber threats. Capgemini works closely with CxOs to modernise target operating models through comprehensive cybersecurity transformation strategies.

Strengths

Broad range of services: Capgemini offers comprehensive strategic and operational security services, which include audits, assessments, maturity evaluations, cybersecurity architecture, business continuity and disaster recovery. These services help enterprises with tailored solutions that meet their specific needs, ensuring robustness and flexibility. Capgemini offers strategy, design and implementation services for post-quantum cryptography transformations tailored to global banks and Fortune 2000 companies.

Integration of advanced technologies: Capgemini enhances the effectiveness and efficiency of its security measures by integrating advanced technologies, including security information and event management (SIEM), threat intelligence and GenAI for automation. Advanced data analysis capabilities are employed to provide detailed insights and proactive threat detection. This technological integration ensures that Capgemini's security solutions are advanced and highly adaptive to emerging challenges and threats, providing clients with robust and dynamic protection.

Expertise and scale: With a Cybersecurity Business Unit comprising over 6,200 specialists, Capgemini combines in-depth expertise in cybersecurity, data privacy, regulatory knowledge and transformation processes. This scale allows for extensive support across various sectors.

Caution

Capgemini should continue to invest in proprietary IP-led frameworks, highlighting its advisory capabilities and strengthening its strategic security consulting presence in the UK. This approach would enhance differentiation and reinforce its position as a trusted partner in complex security transformations.

Appendix

Methodology & Team

The ISG Provider Lens 2025 – Cybersecurity – Services and Solutions analyzes the relevant software vendors/service providers in the U.K., global markets based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Authors:
Bhuvaneshwari Mohan (U.K., Global - IAM), Monica K (U.K.), Gowtham Sampath (Global - XDR), and Yash Jethani (Global - SSE)

Editor:
Ananya Mukherjee

Research Analyst:
Bhuvaneshwari Mohan and Sandya Kattimani (Global)

Data Analysts:
Rajesh Chillappagari and Laxmi Kadve

Consultant Advisor:
Anas Barmo

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. The data collected for this report represent information that ISG believes to be current as of May 2025 for providers that actively participated and for providers that did not. ISG recognizes that many mergers and acquisitions may have occurred since then, but this report does not reflect these changes.

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

The study was divided into the following steps:

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

Author (U.K and 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.

Co-author (U.K)

Monica K

Co-author and Lead Research Specialist

Monica K is an Assistant Manager and Lead Research Specialist at ISG, where she also serves as a digital expert. She co-authors Provider Lens™ studies, the global summary report, and the enterprise perspective for the cybersecurity, ESG, and sustainability markets. Her responsibilities include managing comprehensive research projects and collaborating with internal stakeholders on diverse consulting initiatives.

With over a decade of experience in technology, business, and market research, Monica brings valuable expertise to ISG clients. Previously, she worked at a research firm specializing in IoT, product engineering, vendor profiling, and talent intelligence.

Author (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 - 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 (Global)

Sandya Kattimani

Senior Research Analyst

Sandya Kattimani is a senior research analyst at ISG and is responsible for supporting and co-authoring ISG Provider Lens™ studies on Contact Center, Life Sciences, Mainframes. Sandya has over 6 years of experience in the technology research industry and in her prior role, she carried out research delivery for both primary and secondary research capabilities. Her area of expertise lies in Competitive Intelligence, Customer Journey Analysis, Battle Cards, Market analysis and digital transformation.

She is responsible for authoring the enterprise content and the global summary report, highlighting regional as well as global market trends and insights. Prior to this role she has worked as technology research analyst, where she was responsible for project work which includes detail technology scouting, competitive intelligence, company analysis, technologies study and other Ad hoc business research assignments

Study Sponsor

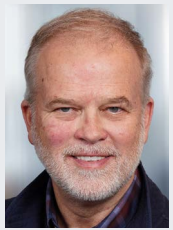
Heiko Henkes

Director & Principal Analyst, Global IPL Content Lead

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

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

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

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

ISG Provider Lens™

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

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

ISG Research™

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

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

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

ISG

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

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

For more information, visit isg-one.com.

ISG Provider Lens™

JULY, 2025

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS