

Cybersecurity – Solutions and Services

Technical Security Services

Analyzing the cybersecurity market, comparing provider portfolio attractiveness and competitive strengths

Customized report courtesy of:



Executive Summary 03

Provider Positioning 11

Introduction

Definition 24

Scope of Report 26

Provider Classifications 27

Appendix

Methodology & Team 38

Author & Editor Biographies 39

About Our Company & Research 42

Star of Excellence 35

Customer Experience (CX) Insights 36

Technical Security Services 28 – 34

Who Should Read This Section 29

Quadrant 30

Definition & Eligibility Criteria 31

Observations 32

Provider Profile 34

*Report Author: Bhuvaneshwari Mohan,
Gowtham Sampath, Dr. Maxime Martelli*

Zero trust, cloud and data security are the key security priorities of the UK enterprises

In the UK, the threat landscape is poised to expand in volume and complexity, further amplified by technological advancements such as the increased use of AI, cloud, 5G and edge with the proliferation of connected products and devices. This expansion exponentially broadens the potential attack surface, presenting greater opportunities for causing harm and disruption. Moreover, experts anticipate that the integration of AI, including large language models (LLMs), will increase the sophistication of cyberattacks. However, this escalation applies equally to developing defensive measures against cyber threats.

There are around 3,000 managed service providers (MSPs) in the UK providing comprehensive IT management, including cybersecurity services. Additionally, there are

3,000 dedicated managed security service providers (MSSPs) in the UK that focus on cybersecurity solutions and services, according to the research published in 2024 by the UK Department of Science, Innovation and Technology. The line between MSPs and MSSPs that focus solely on cybersecurity services is blurred. More MSPs are adding cyber to their portfolios, which means the MSSPs must differentiate themselves by providing more specialized security services. Amidst the current economic downturn, UK enterprises are seeking heightened assurance of the quality and return on investment (ROI) of their cybersecurity investments.

The UK government undertook multiple initiatives in 2023 that will impact 2024 and beyond, solidifying its commitment to developing robust cybersecurity standards and guidance. As the landscape continues to evolve, ongoing vigilance and collaborative efforts will remain crucial in safeguarding the UK's digital infrastructure and critical assets to improve the economy's and society's cyber resilience.

UK businesses
necessitate a
**dynamic and
multi-layered
security approach.**



Regulations evolve: The EU Commission issued guidelines clarifying the relationship between the NIS2 Directive and the Digital Operational Resilience Act (DORA), ensuring clarity for financial entities subject to both regulations. The government announced plans to incorporate proposals for strengthening cybersecurity laws into the Network and Information Systems (NIS) Regulations, further bolstering the UK's regulatory framework.

Focus on emerging threats: The UK NCSC (National Cyber Security Centre) continued its vital role in raising awareness of evolving threats. It published a white paper delving into the tactics employed by organized crime groups in ransomware attacks, emphasizing the importance of good cyber hygiene practices. It issued a warning regarding the security vulnerabilities of AI systems, urging organizations to implement appropriate safeguards.

National Cyber Strategy Progress: The government published its annual National Cyber Strategy 2022 – 23 Progress report, highlighting key achievements throughout the year. The report showcased progress in bringing

all private sector businesses working in critical national infrastructure (CNI) within the scope of cyber resilience regulations, a significant step towards safeguarding critical infrastructure.

The report also highlighted the continued significance of the Russian state as a significant threat actor targeting the UK. The NCSC has confirmed attempted cyberattacks on UK media, telecommunications and energy infrastructure.

Addressing shadow IT risks: Recognizing the potential dangers associated with unauthorized IT usage, the NCSC published guidance on “shadow IT.” This guidance equips organizations with strategies to mitigate the risks associated with this practice, promoting secure and controlled IT environments.

Becoming proactive: Enterprises must embrace proactive and adaptive cybersecurity with effective incident response strategies to thrive in this dynamic landscape. There is a high need for a layered approach towards security measures that focuses on **integrating** individual security tools into a unified security framework. This allows for **orchestrated responses**

based on real-time threat intelligence and risk assessments. The modern, layered approach goes beyond simply layering various security measures. It emphasizes a dynamic, integrated, continuously evolving security posture that adapts to the ever-changing threat landscape and prioritizes user education and awareness.

The ever-evolving cybersecurity landscape demands a multipronged approach from enterprises. ISG identifies the below as the **key themes for the enterprises in the UK** market.

Growing recognition of zero trust and IAM

Zero trust is rapidly gaining traction in the UK, shaping the market increasingly focused on robust identity management and least-privilege access. Enterprises must shift their security approach to a more dynamic and adaptive model. The UK government actively promotes and invests in cybersecurity initiatives, emphasizing the importance of identity security and zero trust as foundational elements. Industry bodies also underscore the importance of zero trust and offer guidance for implementation. Identity and access

management is gaining much traction in the market and stakeholders view it as a foundational component for attaining zero trust. Decentralized identities, adaptive authentication and authorization, converged IAM, passwordless authentication and identity fabrics are the few considerations while selecting IAM solutions.

Integration of AI and ML revolutionizes the traditional security approach

AI and ML technologies empower businesses to foster a cybersecurity posture that evolves with the ever-changing threat landscape. AI aids in understanding potential threats and vulnerabilities by integrating threat intelligence from diverse sources. ML ensures that the gathered intelligence is constantly updated by continuously learning from it. Internal teams can utilize threat intelligence to defend against threats and improve operational efficiency, enabling them to enhance situational awareness of the threat landscape, prioritize security efforts and adapt defensive strategies accordingly.



Providers are widely using threat intelligence for proactive education of industry-specific threats and challenges to their clients in the respective industries and to provide early warning of emerging threats and risks to their digital footprint. Enterprises should consider integrating AI and ML into their security strategies, ensuring adequate data security and privacy measures, supplementing with human expertise to mitigate bias and ensuring threat intelligence data quality and accuracy.

Strong need for automation

Automation is critical in enhancing security teams' operational performance and reliability. It helps security teams to save time on routine tasks and focus on higher-impact work. Several critical areas, including detection and response and creating actionable context from vast data sets, are experiencing significant momentum, leading to alert overload and increased complexity. Automation to its full effect in such cases could help security teams to overcome these challenges and allow for strategic resource allocation to spend more time on deriving insights. Other areas with a

high need for automation include reporting and risk quantification or assessments. AI-driven automation helps enterprises to respond to incidents faster and more effectively.

Increased focus on data privacy and security

Stringent data protection regulations such as the **General Data Protection Regulation (GDPR)** and the upcoming **Data Protection and Digital Information Bill** mandate the need for secure solutions, privacy-enhancing technologies such as decentralized identities, differential privacy analytics techniques, self-sovereign identity, data encryption and classification techniques and compliance expertise. These regulations also create significant opportunities for security vendors and providers to innovate and help their clients adapt to a privacy-first security landscape. Additionally, evolving regulations mandating stricter access control and data protection align with the core principles of zero trust, making it a compelling choice to strengthen compliance.

Growing awareness of security measures in the SMB market

Small and midsize businesses are recognizing the urgency of enhancing their security posture due to the escalating demand from larger enterprises. These enterprises hesitate to engage with SMBs lacking robust privacy and security protocols. This heightened awareness stems from the growing risk of supply chain attacks, underscoring the critical need for SMBs to fortify their defences against cyber threats. The NIS2 legislation, a revised version of the existing NIS Directive on Security of Network and Information Systems, which is set for implementation in October 2024, requires SMBs to adhere to it due to increased attention towards third-party risk management. Reflecting on this, in 2022, the government brought all the managed service providers serving the UK market into the scope of the NIS regulations to keep the digital supply chains secure.

Rapid surge in IoT security

The growing importance of OT/IoT security in the UK market is expected to drive demand

for endpoint security solutions. With the proliferation of IoT devices in offices and industrial settings, the number of potential entry points for cyberattacks is also increasing, making it critical for businesses to secure these devices and protect their networks.

Rising need for cyber insurance

Enterprises' increasing adoption of cyber insurance is expected to fuel the demand for comprehensive risk assessments. Enterprises will need to thoroughly evaluate their cybersecurity posture to obtain adequate coverage and minimize potential losses in case of a cyberattack. This trend is driving the adoption of cyber risk quantification services among enterprises. They are facing higher levels of scrutiny for cyber-related requirements before providing cybersecurity cover, in addition to increased premiums from insurance providers.

Cyber literacy is gaining momentum at the board level

Business and cyber leaders are aligning on cyber-related topics. With cyber experts now being included on corporate boards, there



is a shift in the mindset among business leaders as cybersecurity is not seen just as an IT issue but as a business problem. By incorporating cyber resilience governance into their business strategy, businesses can ensure that cybersecurity is a priority at all levels of the organization, from the board of directors to front-line employees. This helps create a cybersecurity awareness culture and ensures employees understand their role in protecting the enterprise's assets.

Scarcity of cyber talent

Cyber talent recruitment and retention remain major challenges in the industry, particularly given the high demand and competition for skilled professionals. One potential solution is to focus on upskilling and reskilling existing talent to meet evolving cybersecurity needs. This can involve investing in training and development programs and fostering a culture of continuous learning and innovation. Some enterprises are also focusing on incentivizing cybersecurity training programs.

A strategic approach to cyber resilience

A well-defined cyber resilience strategy is no longer optional for UK enterprises. To improve their security posture, businesses should have a broad understanding of risks in the environment they are operating in and develop a comprehensive roadmap with clear goals and objectives for cyber resilience aligned with business goals. Enterprises should conduct regular security audits and penetration testing to identify potential vulnerabilities and update their cybersecurity strategies and processes accordingly. Enterprises should also ensure that their cyber strategies capture and respond to changes in best practices and developments in the enterprise, including technological infrastructure.

Increasing need for security compliance:

Enterprises are increasingly required to demonstrate cybersecurity compliance to their end customers. Managing the growing complexity and time-consuming nature of reporting requirements in the UK is a big challenge for enterprises. While compliance with legislation is important, much of the effort

is reactive, focusing on post-incident actions that are considered critical for protecting an organization's legal interests and building a strong case for potential legal action. Enterprises should also utilize the preserved evidence proactively to refine security controls and optimize the incident response plan, thereby preventing the recurrence of such incidents.

Enterprises must also brace themselves for a surge in AI regulatory initiatives in the next few years, encompassing guidelines, data collection and enforcement measures. Global companies will inevitably confront regulatory discrepancies as they navigate through international jurisdictions.

Increasing need for user awareness and training

Enterprises should focus on regular and engaging training sessions covering trends such as phishing and social engineering techniques. This creates a security-centric culture across the enterprise where security is at the top of the mind. Realistic simulations can be used to reinforce training that helps

employees practice the recognition and reporting of threats in a safe environment.

Security vendor consolidation

Vendor consolidation has gained importance in recent years. Enterprises drive this shift due to key challenges that enterprises face, including managing numerous security solutions with different interfaces, encountering different integration issues resulting in security coverage gaps and facing increased costs leading to high overall security expenditures. Enterprises are investing in integrated product suites or single vendor platforms that cover the entire security spectrum with end-to-end security solutions.

SASE and SSE gaining traction

As enterprises consolidate security and remote access services under a single framework, security service edge (SSE) offerings provide a unified management console for real-time visibility of security events across the entire security infrastructure. This unification helps businesses maintain compliance with various security regulations and standards by providing a single control point for security policies and configurations. SSE solutions improve the



efficiency of enterprises' security operations and are gaining popularity as a trial run before implementing secure access service edge (SASE) solutions.

Rise of quantum computing

While the rise of quantum is still in the early stages, enterprises should keep an eye on government regulations and guidance. The UK government is funding more initiatives to increase quantum technology adoption in healthcare, energy and transport. In the years to come, as quantum systems mature, existing cryptographic methods will become vulnerable. The needs for quantum-resistant encryption methods will rise, which will be critical for securing applications and systems for enterprises that rely on them. Some providers are leading this field by developing proof of concept (PoC) projects tailored to industry-specific scenarios. They showcase their commitment through investments, market visibility via proofs of value (PoVs), white papers and ongoing thought leadership. They also engage with clients proactively.

GenAI-related threats

While GenAI offers promising applications across various sectors, its integration also introduces unique security challenges for enterprises. If the AI training environment or data storage systems are compromised, attackers could gain access to the training data, potentially leading to data breaches and further compromising the security of sensitive information during training and model deployment. Robust data governance frameworks, robust identity controls, AI security governance and model testing, are critical for enterprises that use GenAI effectively. The UK's NCSC has additionally noted that advancements in GenAI and LLM models will pose challenges for cybersecurity professionals in recognizing phishing, identity spoofing and social engineering attempts. Furthermore, the market is expected to witness a surge in ransomware attacks.

This study examines the evolving market demands in the UK in 2024 and offers a comprehensive overview. It also provides valuable guidance to aid clients in evaluating and assessing the offerings and performance of providers.

Cybersecurity is becoming a strategic component that aligns security measures with overall business goals. Operational resilience is a primary concern for UK businesses, emphasizing a proactive approach to threat detection and response to reduce disruptions and downtime. New regulatory obligations, such as NIS2, DORA and the EU-AI Act, are also exerting pressure on the UK enterprises.



As enterprises increasingly rely on cloud applications, remote workforces and interconnected systems, the complexity and sophistication of cyberthreats have escalated. This dynamic environment requires advanced security measures that go beyond traditional perimeter defenses. As cyberthreats continue to grow in sophistication, the adoption of such cutting-edge security measures will be essential for maintaining a strong cybersecurity posture.

The necessity for advanced cybersecurity solutions such as extended detection and response (XDR) and security service edge (SSE) is driven by the evolving threat landscape, increased cloud adoption and the need for comprehensive security frameworks. These innovative platforms address critical challenges faced by enterprises, ensuring resilient and efficient protection of digital assets and business operations.

Some of the existing challenges are listed below:

Complexity in security architectures: Managing disparate security tools and solutions can lead to inefficiencies and gaps in protection, making integrated platforms such as XDR and SSE critical for streamlined operations.

Reactive threat detection and response:

Traditional security measures often fail to provide real-time visibility and response capabilities. XDR leverages advanced analytics and automation to detect, investigate and respond to threats across various endpoints.

Lax data privacy and governance:

Ensuring data privacy and governance in a decentralized IT environment is challenging. SSE offers centralized security policies and governance frameworks to manage data protection effectively.

Lack of scalability and performance:

As organizations grow, their security solutions must scale accordingly without compromising IT or business operational performance. XDR and SSE are designed to provide scalable, high-performance security across expansive and evolving IT landscapes.

Poor user experience: Balancing robust security with a seamless user experience is essential. Enterprises require innovative solutions designed to be minimally intrusive while maximizing protection and security posture.

Extended detection and response (XDR) trends

The XDR market is witnessing various innovative trends to improve threat detection, response and the overall security posture. XDR solutions are gaining traction due to their ability to collect and correlate data across multiple security layers, including emails, endpoints, servers, cloud workloads and networks, providing a multifaceted view of the organization's security posture.

The key trends in the XDR space are listed below:

Integration of AI and ML: One of the latest trends in XDR is the integration of AI and ML algorithms to enhance threat detection and response capabilities. These advanced technologies enable XDR platforms to identify complex threats, predict potential attacks and automate response actions, thereby reducing the burden on security teams.

Convergence with other security solutions: Another emerging trend is the convergence of XDR with other security solutions such as security information and event management (SIEM) and security orchestration, automation and response (SOAR). This convergence creates

a unified security architecture, improving threat visibility, detection and response times while streamlining security operations.

Threat intelligence integration: XDR platforms increasingly integrate with threat intelligence feeds to enhance threat detection and response. Combining internal security data with external threat intelligence allows XDR solutions to provide contextual insights into potential threats. This helps security teams to make informed decisions and prioritize their response efforts.

XDR for cloud and SaaS environments: As organizations continue to adopt cloud and SaaS applications, XDR solutions are expanding their coverage to include these environments. Cloud-native XDR platforms can monitor and secure cloud workloads, containers and serverless applications while providing visibility on SaaS application usage and potential risks.

Threat and compromise detection capabilities: XDR solutions incorporate user and entity behavior analytics (UEBA) capabilities to detect insider threats and account compromises.



UEBA uses ML algorithms to analyze user behavior patterns and identify anomalies that could indicate malicious activity, helping organizations detect and respond to threats that might otherwise go unnoticed.

XDR enhancing security for ICS and OT environments: As the threat landscape for industrial control systems (ICS) and OT environments continues to evolve, security experts are tailoring XDR solutions to address these systems' unique security challenges. XDR for ICS and OT can monitor and analyze data from specialized industrial control systems, detecting threats early and enabling rapid response to minimize potential damage.

Compliance and regulatory support: With the increasing focus on data privacy and security regulations, organizations are enhancing XDR solutions to meet compliance requirements.

Enterprises are navigating a dynamic landscape characterized by increased adoption of cloud environments and evolving cyberthreats, necessitating security solutions that are scalable, flexible and robust. SSE solutions address these challenges by providing

centralized visibility, advanced threat detection powered by AI and ML and seamless policy enforcement across all endpoints. By adopting SSE, organizations can ensure secure access to applications and data from any location, maintain compliance with regulatory standards and safeguard against data breaches and insider threats, thereby supporting business continuity and resilience in the face of a constantly changing threat landscape.

Challenges addressed by SSE Solutions are listed below:

Security of cloud applications:

The proliferation of cloud services creates security complexities. SSE centralizes security policies and enforces consistent access control across all cloud applications.

Remote workforce security: With more employees working remotely, traditional perimeter-based security models become less effective. SSE provides secure access to cloud applications from any location, regardless of the device.

Data loss prevention (DLP): Data breaches and leaks are major concerns. SSE helps

prevent sensitive data from being exfiltrated by enforcing DLP policies and data encryption across cloud services.

Shadow IT: Employees often use unsanctioned cloud applications. SSE provides visibility into shadow IT usage and allows for secure access control even for unapproved applications.

Complexity of security management:

Managing multiple security point solutions can be complex and time consuming. SSE offers a unified platform for managing security policies across all cloud applications.

The SSE market is experiencing significant growth due to the increasing adoption of cloud applications, remote workforces and the need for a consolidated security approach.

Key trends shaping the market are listed below:

Cloud-native architectures: As businesses migrate to cloud environments, they adopt cloud-native security solutions that scale with workloads and support dynamic, distributed setups.

Convergence of security and networking:

There is a growing trend to integrate networking and security functions into a single platform,

streamlining operations and reducing the complexity of managing security and network performance.

Integration of SWGs and CASBs: Secure web gateways (SWGs) and cloud access security brokers (CASBs) are converging into comprehensive SSE solutions, providing unified threat protection, DLP and access control for cloud services.

Emphasis on zero trust security: SSE solutions are increasingly incorporating zero trust principles, granting access based on least privilege and continuous verification, enhancing security by minimizing the attack surface and lateral movement within the network.

SASE adoption: SSE is a foundational element of secure access service edge (SASE) architectures, which integrate network security and cloud access security into a unified cloud-delivered service.

AI and ML integration: SSE solutions leverage AI and ML to automate threat detection, improve anomaly identification and personalize security policies based on user behavior.



Focus on user experience: Balancing security with UX is crucial. SSE solutions are designed to be transparent to users, ensuring minimal disruption to their workflow while maintaining robust security.

Unified management consoles: There is a trend toward developing unified management interfaces that consolidate various security functions into a single dashboard, simplifying administration and providing a holistic view of the security landscape.

User and entity behavior analytics (UEBA): UEBA tools analyze the behavior of users and entities to identify potential security threats. By establishing baselines and detecting deviations, UEBA helps identify anomalous activities.

Identity-centric security: Emphasis on identity and access management (IAM) is becoming central to security strategies, ensuring that only authenticated and authorized users can access resources.

As businesses prioritize robust cybersecurity and navigate the complexities of the digital environment, the demand for innovative solutions such as XDR and SSE will be at the forefront of safeguarding their digital assets. As cyberthreats become more sophisticated and businesses rely increasingly on cloud services, XDR and SSE will be crucial in safeguarding enterprise security.





Provider Positioning

Page 1 of 13

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Accenture	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
Adarma	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Product Challenger
Beta Systems	Contender	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
Bitdefender	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
BlackBerry	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Bridewell	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In






Provider Positioning

Page 2 of 13


	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Capgemini	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger	Not In
Check Point Software	Not In	Product Challenger	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
Claranet	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Leader
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In
Cognizant	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Not In
Computacenter	Not In	Not In	Not In	Leader	Not In	Market Challenger	Not In	Market Challenger



 Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Cross Identity	Product Challenger	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
CyberArk	Leader	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
CyberProof	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger
Cyberes	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Leader
Deloitte	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
DXC Technology	Not In	Not In	Not In	Product Challenger	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



 Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Ericom Software	Not In	Not In	Product Challenger	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
Eviden	Product Challenger	Not In	Not In	Leader	Leader	Not In	Leader	Not In
EY	Not In	Not In	Not In	Rising Star ★	Leader	Not In	Leader	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Leader	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortra	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Contender	Not In	Market Challenger	Not In
Getronics	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In





Provider Positioning

Page 5 of 13

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Globant	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In
GTT	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Happiest Minds	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger
HCLTech	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
HPE (Aruba)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Not In	Leader	Not In
iboss	Not In	Not In	Product Challenger	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
IN Groupe	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In





Provider Positioning

Page 6 of 13

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Infosys	Not In	Not In	Not In	Leader	Product Challenger	Not In	Rising Star ★	Not In
Integrity360	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	Product Challenger	Not In	Contender
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
KPMG	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	Product Challenger	Not In
Kudelski Security	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger
Kyndryl	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Contender	Not In
Logicalis	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger





Provider Positioning

Page 7 of 13

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Lookout	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
LRQA Nettitude	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
LTIMindtree	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Not In
ManageEngine	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Microland	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In
Mphasis	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
NCC Group	Not In	Not In	Not In	Not In	Market Challenger	Leader	Not In	Leader
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In





Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
NTT DATA	Not In	Not In	Not In	Product Challenger	Leader	Not In	Product Challenger	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	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
OpenText	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Leader	Product Challenger	Not In	Product Challenger	Leader
Palo Alto Networks	Not In	Leader	Leader	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	Product Challenger
Perimeter 81	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In





Provider Positioning

Page 9 of 13


	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Persistent Systems	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Ping Identity	Leader	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
Quorum Cyber	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Rackspace Technology	Not In	Not In	Not In	Product Challenger	Not In	Rising Star ★	Not In	Product Challenger
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Redscan	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
RSA	Market Challenger	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






	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Saviynt	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Product Challenger	Not In	Not In	Contender	Not In	Not In	Not In
SecurityHQ	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Rising Star ★
SenseOn	Not In	Contender	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
Shearwater Group	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger
Skyhigh Security	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Softcat	Not In	Not In	Not In	Market Challenger	Contender	Not In	Contender	Not In



 Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Sopra Steria	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	Not In
Tata Communications	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
TCS	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Leader
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Telefonica Tech	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger	Not In	Contender
Telstra	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Not In



 Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Thales	Leader	Not In	Not In	Product Challenger	Product Challenger	Not In	Rising Star ★	Not In
Trellix	Not In	Rising Star ★	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
Trustwave	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Rising Star ★
Unisys	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
ValueLabs	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Verizon Business	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
WALLIX	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In



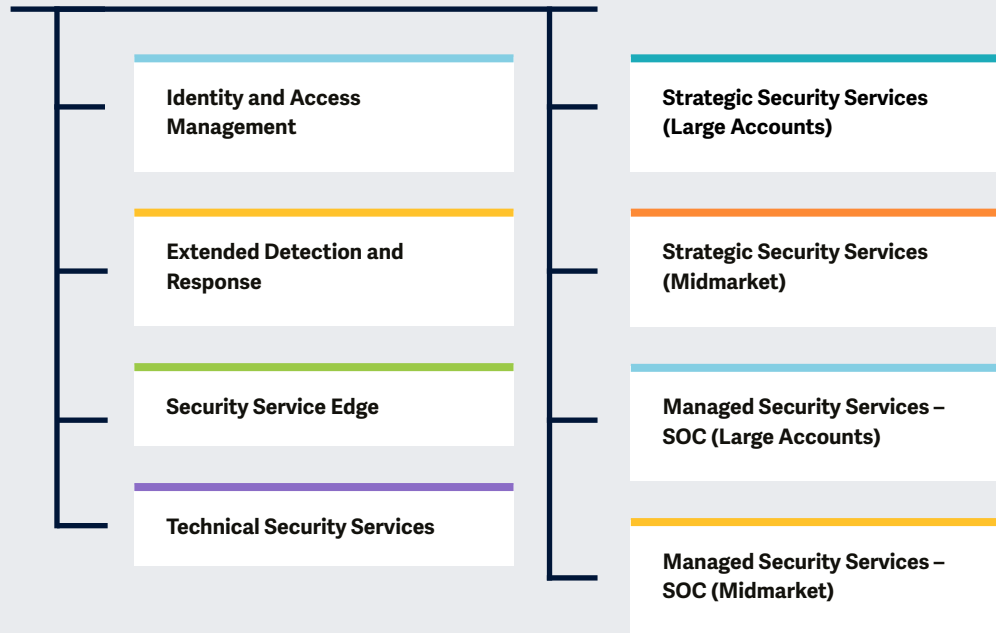


	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Wavestone	Not In	Not In	Not In	Not In	Rising Star ★	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Leader	Not In	Leader	Not In
Zensar Technologies	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In



Key focus areas for the Cybersecurity – Solutions and Services.

Simplified Illustration Source: ISG 2024



Definition

Cybersecurity in the Age of AI

The current cybersecurity landscape is dynamic, with changes occurring rapidly due to merging threats, technological advancements, and evolving regulatory environments. The year 2023 could be termed as tumultuous from a cybersecurity perspective; the year saw significantly increased sophistication and severity in the attacks. Enterprises responded by increasing their investments in cybersecurity and prioritizing relevant initiatives to prevent attacks and improve their security posture. Learnings from prior attacks in 2022 led to executives and businesses of all sizes and across industries investing in measures countering cyberthreats. AI brings both challenges and opportunities to cybersecurity, offering automation for analysis and detection while posing risks of bias and misuse.

From an enterprise perspective, even small businesses realized their vulnerability to cyber threats, fueling demand for (managed) security and cyber resiliency services that would enable recovery and operation restoration post-cyber



incidents. Therefore, service providers and vendors are offering services and solutions that help enterprises ensure recovery and business continuity.

Security services providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats, understanding the transformative impact of technologies such as AI and ML, and staying attuned to evolving regulatory frameworks on data protection, such as NIS-2, in the European Union. Cybercriminals exploited large-scale vulnerabilities, persistently using ransomware to disrupt business activities, specifically healthcare, supply chain and public sector services.

Consequently, businesses started to invest in solutions such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR), and cloud and endpoint security. The market is shifting toward integrated solutions such as security service edge (SSE) and extended detection and response (XDR), which leverage the best tools and human expertise augmented with behavioural and contextual intelligence and automation to deliver a superior security posture.



Scope of the Report

In this ISG Provider Lens™ quadrant report, ISG covers the following eight quadrants for services/solutions: Identity and Access Management, Technical Security Services, Strategic Security Services (Large Accounts), Strategic Security Services (Midmarket), Managed Security Services - SOC (Large Accounts), Managed Security Services – SOC (Midmarket), vendors offering Security Service Edge, Extended Detection and Response solutions are analysed and positioned from a global perspective rather than individual regions, as the market is still in its early stages and yet to mature.

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

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments
- Focus on Global market

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

Provider Classifications

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

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

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

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





Provider Classifications: Quadrant Key

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

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 a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

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.

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.





Technical Security Services

Who Should Read This Section

In this quadrant, ISG aims to assist UK enterprises in evaluating technical security service providers that specialise in implementing and integrating security products or solutions offered by other security vendors besides their proprietary products.

Enterprises are increasingly integrating security solutions and practices directly into their software development lifecycle (SDLC). Adopting a security shift-left approach, enterprises are ensuring security at every stage of the SDLC, covering aspects such as data privacy, secure coding practices and design security controls to cover the risk landscape.

Providers offer tools and frameworks to automate security processes such as vulnerability scanning, code reviews and compliance checks. Utilising security as code (SaC), enterprises can ensure the consistent application of security measures across their infrastructure and applications, thereby, enhancing resilience and reducing risk exposure. Managing multiple security tools from different providers to support their digital

transformation is also increasing complexity. Enterprises are undergoing consolidation to reduce the complexity and rationalise security solutions to streamline their security operations. Enterprises seek providers offering comprehensive services, covering all security domains and delivering integrated security platforms to streamline product diversity, enabling a unified management perspective. Providers are evolving their security information and event management (SIEM) platforms to easily integrate with a wide range of security tools and provide ready-to-use vendor-agnostic playbooks for quick client onboarding.



Security and data professionals should read this report to learn how providers help enterprises comply with data security and protection laws to stay updated with market trends.



Technology professionals should read this report to identify providers and offerings for automating security and advancing towards DevSecOps.

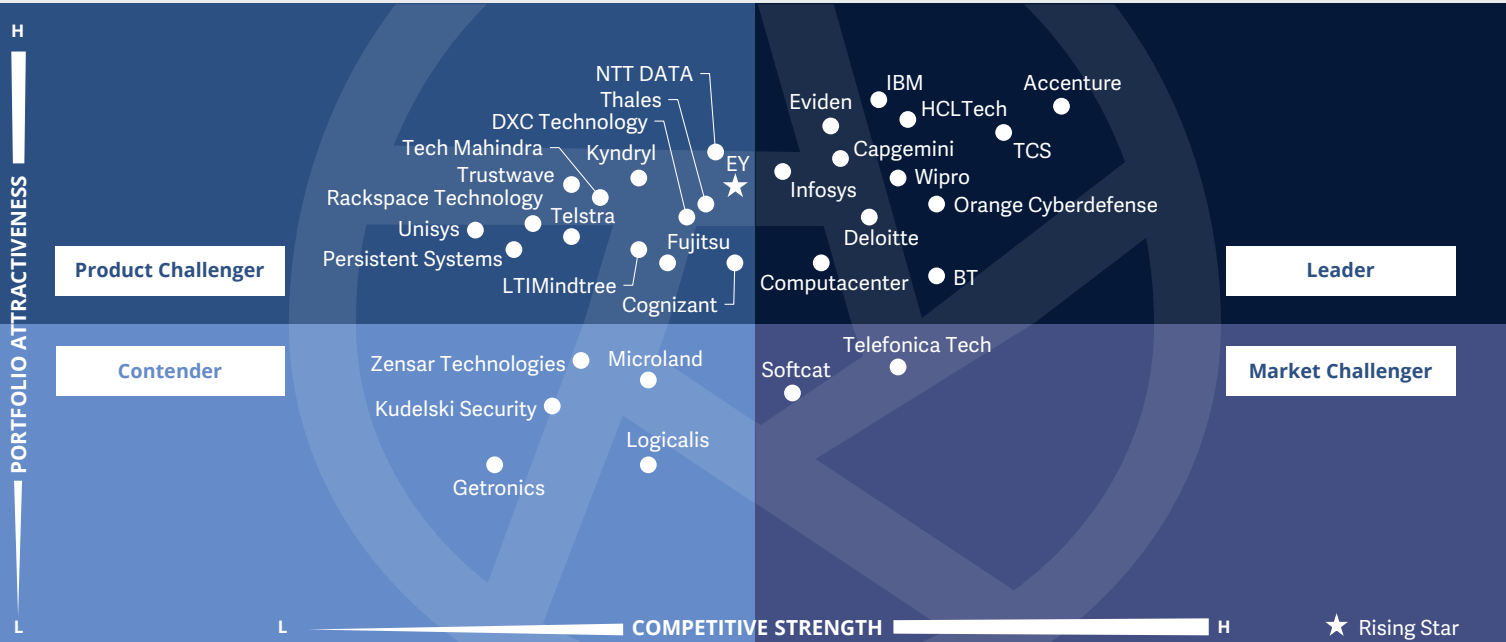


Digital professionals, including IT and digital transformation leaders, should read this report to understand the importance of early adoption and integration of security best practices.



Cybersecurity – Solutions and Services
Technical Security Services

U.K. 2024



This quadrant assesses service providers with capabilities to design, build and **transform** security environments, focusing on **cost** optimization and **security assurance** embedding secure by design approach.

Bhuvaneshwari Mohan



Technical Security Services

Definition

The TSS providers assessed for this quadrant cover integration, maintenance and support for both IT and OT security products or solutions. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security and SASE and others.

TSS providers offer standardized playbooks and roadmaps that aid in transforming an existing security environment with best-of-breed tools and technologies, improving security posture and reducing threat impact. Their portfolios are designed to enable complete or individual transformations of existing security architectures across domains such as networks, cloud, workplace, OT, IAM, data privacy and protection, risk and compliance management and SASE, among others. The offerings also include product or solution identification, assessment, design and development, implementation, validation, penetration testing, integration and deployment.

TSS providers invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio scope. This quadrant also encompasses classic managed security services provided without a security operations center (SOC).

This quadrant examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other vendors.

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Have gained **authorization by security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies



Technical Security Services

Observations

Below are some of the key developments that ISG observes in the space of Technical Security Services market in the UK:

Providers are investing in data privacy and compliance solutions to help clients identify and mitigate data risks, ensuring compliance with regulatory requirements such as the EU-AI Act, the UK's DPDI Bill and the traditional privacy implementation for GDPR. With the use of GenAI, capabilities such as data discovery, classification and privacy by design are gaining importance.

Enterprises are facing challenges managing multiple security tools and are offering unified consoles and reporting tools for a unified view of security activities. These integrated platforms help enterprises reduce the number of security vendors and use a more consolidated and visible security environment.

As the need for securing hybrid and multicloud environments is rising, providers are heavily teaming up with hyperscalers. There is immense focus on enhancing security capabilities within the cloud environment, such as developing cloud

security frameworks, new tools and techniques for protecting data and applications and robust access controls and security configurations.

As OT/IoT environments rapidly expand, the demand for specialized and industry-specific solutions to safeguard critical infrastructures, networks and connected devices are on the rise. Network security, microsegmentation, SASE and zero trust implementations are becoming significantly important.

Integrating DevSecOps and DevOps workflow into security practices throughout the SDLC is also gaining prominence, driven by the need for automation due to the lack of security experts, cost-saving initiatives and shift-left approach.

From the 82 companies assessed for this study, 33 qualified for this quadrant, with twelve being Leaders and a Rising Star.

accenture

Accenture's security innovation, combined with its global scale and delivery capabilities, offers enterprises robust cyber defence solutions that can be seamlessly integrated into its security fabric for enhanced protection.

BT

BT empowers public and private enterprises, to securely adopt advanced technologies such as cloud and IoT, placing a greater emphasis on cybersecurity resilience. Offerings are complemented by its regional presence in the UK and technical expertise.

Capgemini

Capgemini's industrialized SOC use case development, robust innovation via Applied Innovation Exchange (AIE) network, startup collaboration and emphasis on early integration of DevSecOps practices into clients' security transformation efforts stands out.

Computacenter

Computacenter combines vendor expertise, strategic relationships with partners and extensive technical knowledge honed through years of experience in delivering significant transformation services to its clientele.

Deloitte.

Deloitte bolsters strong industry expertise, technological innovation and strategic alliances and ecosystem relationships with hyperscalers and technology vendors to provide solutions for the complex needs of its clients.

EVIDEN an atos business

Eviden (an Atos Business) specializes in ensuring client security compliance, data protection and cloud security expertise, including cloud-native security, digital sovereignty, unified SASE and a zero trust approach.

HCLTech

HCLTech offers extensive technical expertise in key security domains, including networks, cloud, OT/IoT, IAM, data privacy and SASE. It partners with clients to drive security transformation, emphasizing ROI on their cyber investments.



Technical Security Services



IBM has extensive partners and alliances, which, combined with its advanced security products, go beyond integration to resilience and security innovation across the clients' security landscape to embed a secure core in their transformation efforts.



Infosys helps clients build robust security capabilities across OT, network, cloud, IAM, data privacy and digital workplace domains in collaboration with strategic partners and automation-led assets to minimize risk surface and strengthen security policies and controls.



Orange Cyberdefense has a large team of security experts with deep technical expertise possessing both vendor-led and professional certifications and provides security technology integration across all security domains, including OT.



TCS uses next-gen research and innovation capabilities to provide adaptable, innovative and contextualized solutions. It co-innovates with customers to drive security transformations and strengthen their cyber defence posture.



Wipro, which has over 9,000 security experts, delivers scalable solutions using accelerators, automation playbooks and methodologies that seamlessly integrate with clients' security infrastructure.



EY (Rising Star) combines its expertise in risk, compliance, IAM, data privacy and next-gen security operations with deep technical knowledge to provide assurance that clients will adopt and scale up innovation using emerging technologies.





“Computacenter helps clients develop an integrated security landscape from technology sourcing, integration and automation, using its global delivery expertise and deep partnership with various vendors.”

Bhuvaneshwari Mohan

Computacenter

Overview

Computacenter is headquartered in Hatfield, UK. It has more than 20,000 employees across over 70 offices in 23 countries. In FY23 the company generated GBP6.9 billion in revenue, with Technology Sourcing as its largest segment. Computacenter’s cybersecurity portfolio encompasses three service lines: technology sourcing, professional services and managed services, providing comprehensive solutions across IAM, infrastructure, OT, cloud, governance, risk and compliance (GRC) and workplace security. Computacenter delivers its services to customers across 70 countries. Its CyberLens service assists enterprises in consolidating their existing security solutions with a vendor-agnostic approach.

Strengths

Broad partner network: The company has partnerships with leading technology vendors such as CyberArk, Microsoft, Fortinet, CrowdStrike, Palo Alto Networks and Tanium that enable it to provide a broad portfolio of technology solutions to its clients. They structure their service delivery and project management capabilities to deliver scalable solutions in a timely, accurate and cost-effective manner by managing risks, schedules and resources throughout the project lifecycle.

Global delivery capability: Computacenter provides flexible delivery options for clients through its nearshore, far-shore, offshore and local delivery capabilities. It has an extensive local presence in the UK and helps clients navigate EU regulations and data privacy

compliances adhering to local regulatory standards. Its certified security experts offer a comprehensive portfolio with advanced tools.


Technology sourcing expertise:

Computacenter provides security product sourcing expertise to assist clients in navigating the intricate vendor landscape. Its vendor product evaluation and testing methodology comprises four stages: defining requirements and shortlisting vendors, evaluating shortlisted vendors, conducting detailed product comparisons and ultimately selecting the best vendor. The company helps clients with technical design validation, product management roadmaps and renewals.

Caution

Computacenter should continue to demonstrate its expertise in consolidating security vendors and tools and addressing the complex challenges of global enterprises. Additionally, it should highlight its proficiency in Microsoft 365 security services, particularly targeting upper-midmarket enterprises.





Star of Excellence

A program, designed by ISG, to collect client feedback about providers' success in demonstrating the highest standards of client service excellence and customer centricity.

Customer Experience (CX) Insights

In the ISG Star of Excellence™ research on enterprise customer experience (CX), clients have given feedback about their experience with service providers for their **Cybersecurity Solutions and Services**.

Based on the direct feedback of enterprise clients, below are the key highlights:

Industry Average CX Score



- ▲ Highest CX: 91.0
- ▼ Lowest CX: 64.8

CX Score: 100 most satisfied, 0 least satisfied
Total responses (N) = 419

Source: ISG Star of Excellence™ research program, Insights till June 2024

Client Business Role

- ▲ **Most satisfied**
Information Technology
- ▼ **Least satisfied**
Human Resources

Region

- ▲ **Most satisfied**
Africa
- ▼ **Least satisfied**
Eastern Europe

Industry

- ▲ **Most satisfied**
Chemicals
- ▼ **Least satisfied**
Public sector

Most Important CX Pillar

Execution and Delivery

Service Delivery Models	Avg % of Work Done
Onsite	53.6%
Nearshore	21.6%
Offshore	24.8%





Appendix

The ISG Provider Lens 2024 Cybersecurity – Solutions and Services study 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, Gowtham Sampath and Dr. Maxime Martelli

Editor:

Indrani Raha

Research Analyst:

Bhuvaneshwari Mohan

Data Analysts:

Rajesh Chillappagari and Laxmi Sahebrao

Consultant Advisors:

Anas Barmo and Reza Memarian

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 report includes research from the ISG Provider Lens program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of May 2024, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The study was divided into the following steps:

1. Definition of Cybersecurity – Solutions and Services 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 and Research Analyst

Bhuvaneshwari Mohan
Author and Research Analyst

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

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



Author

Gowtham Sampath
Senior Manager, ISG Provider Lens™

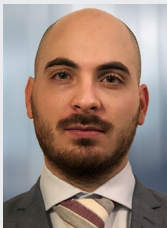
Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing 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 & Editor Biographies

Author



Dr. Maxime Martelli
Consulting Manager

Maxime Martelli is a Consulting Manager at ISG France. He takes part in ISG's "Digital & Strategy" solution for multinational firms and the public sector services, as well as applying his expertise around Information Security and Cloud Security projects.

Author, teacher and lecturer in the field of IT, Maxime is passionate about technology and applies his knowledge of processes, digital strategy, and IT organization to satisfy his clients' requirements.

As a Security Analyst, he conducts transformation and strategy projects for all kind of Security tools and solutions, with a strong focus on SOC/SIEM and SASE next-generation security transformations.

Study Sponsor



Heiko Henkes
Director and Principal Analyst

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 (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including AI and automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.





JULY, 2024

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES