

Cybersecurity – Solutions and Services

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

Customized report courtesy of:

Infosys®

Executive Summary	04
Provider Positioning	12
Introduction	
Definition	25
Scope of Report	27
Provider Classifications	28
Appendix	
Methodology & Team	82
Author & Editor Biographies	83
About Our Company & Research	86
Star of Excellence	79
Customer Experience (CX) Insights	80

Identity and Access Management	29 – 34
Who Should Read This Section	30
Quadrant	31
Definition & Eligibility Criteria	32
Observations	33

Extended Detection and Response	35 – 40
Who Should Read This Section	36
Quadrant	37
Definition & Eligibility Criteria	38
Observations	39

Security Service Edge	41 – 46
Who Should Read This Section	42
Quadrant	43
Definition & Eligibility Criteria	44
Observations	45

Technical Security Services	47 – 53
Who Should Read This Section	48
Quadrant	49
Definition & Eligibility Criteria	50
Observations	51
Provider Profile	53

Strategic Security Services (Large Accounts)

54 – 59

Who Should Read This Section	55
Quadrant	56
Definition & Eligibility Criteria	57
Observations	59

Strategic Security Services (Midmarket)

60 – 65

Who Should Read This Section	61
Quadrant	62
Definition & Eligibility Criteria	63
Observations	64

Managed Security Services – SOC (Large Accounts)

66 – 72

Who Should Read This Section	67
Quadrant	68
Definition & Eligibility Criteria	69
Observations	70
Provider Profile	72

Managed Security Services – SOC (Midmarket)

73 – 78

Who Should Read This Section	74
Quadrant	75
Definition & Eligibility Criteria	76
Observations	77

*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 has 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

	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

Page 3 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)
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

	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

Page 8 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)
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

	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



 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)
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

Page 11 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)
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



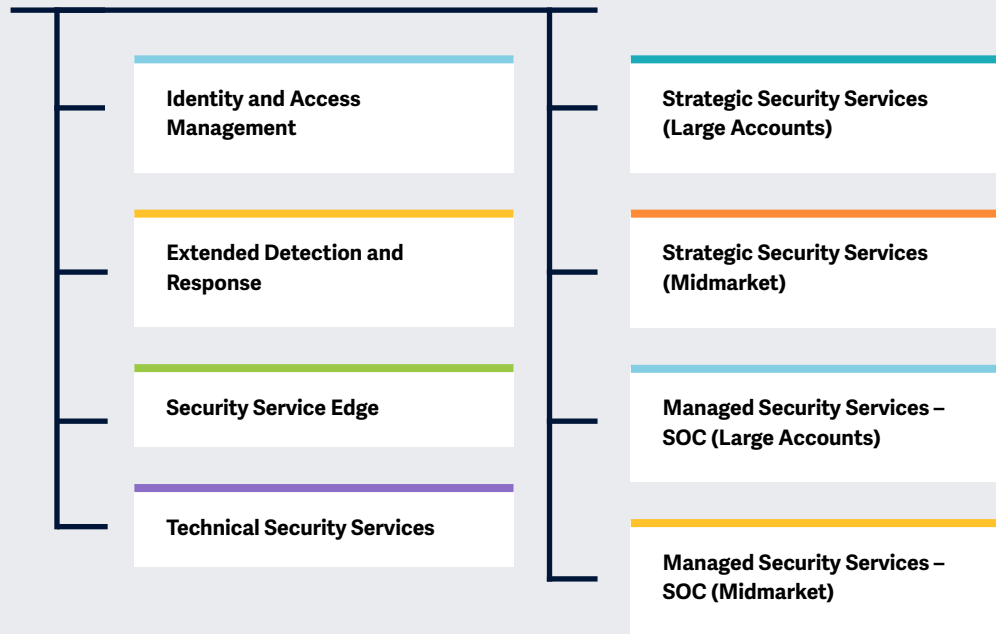


	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Wavestone	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.

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.

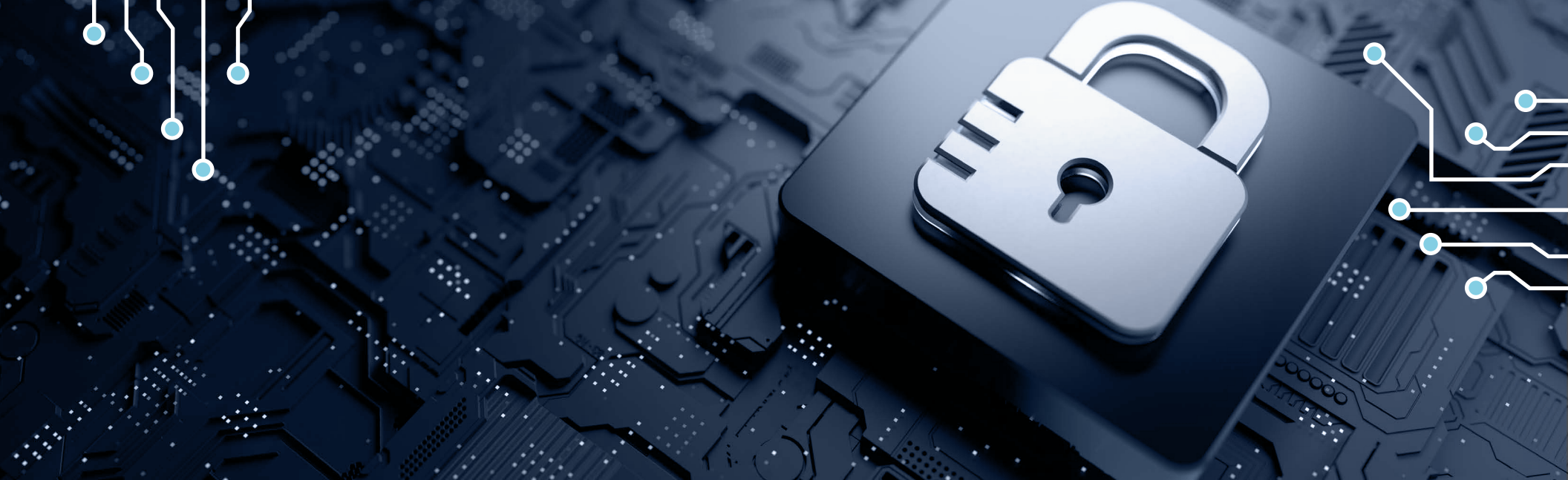
Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/ services and a follow sensible market approach with a goal of becoming a Product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

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

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

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





Identity and Access Management

Identity and Access Management

Who Should Read This Section

This quadrant is relevant to enterprises in the UK for evaluating identity and access management (IAM) solution providers. It assesses how each provider can help enterprises manage complex security challenges associated with securing user access and digital identities.

Enterprises in the UK are actively embracing zero trust principles and leveraging their existing IAM solutions to improve their security posture as an essential building block for zero trust. The emphasis is on optimising and enhancing their IAM capabilities by integrating IAM with additional technologies. This includes adopting new practices to enable least privileged access, continuous verification and robust access control, all-in line with core principles of zero trust. The adoption of passwordless authentication methods has increased as they offer a stronger security layer than traditional security methods. Enterprises in healthcare and finance are actively adopting advanced authentication technologies to address specific security and compliance requirements. Improved user convenience

is also becoming an important consideration for enterprises. IAM platforms are increasing their interfaces to improve user-friendliness and user flexibility through contextual access controls, adaptive multifactor authentication (MFA) and self-service options that reduce friction. With the continued reliance on virtual workforce models, enterprises are increasingly using mobile devices for daily operations. This has made it crucial for them to optimise their IAM platforms and access controls for mobile devices.



Cybersecurity professionals interested in zero trust implementation should read this report to better understand which IAM solution can best support their zero trust journey.

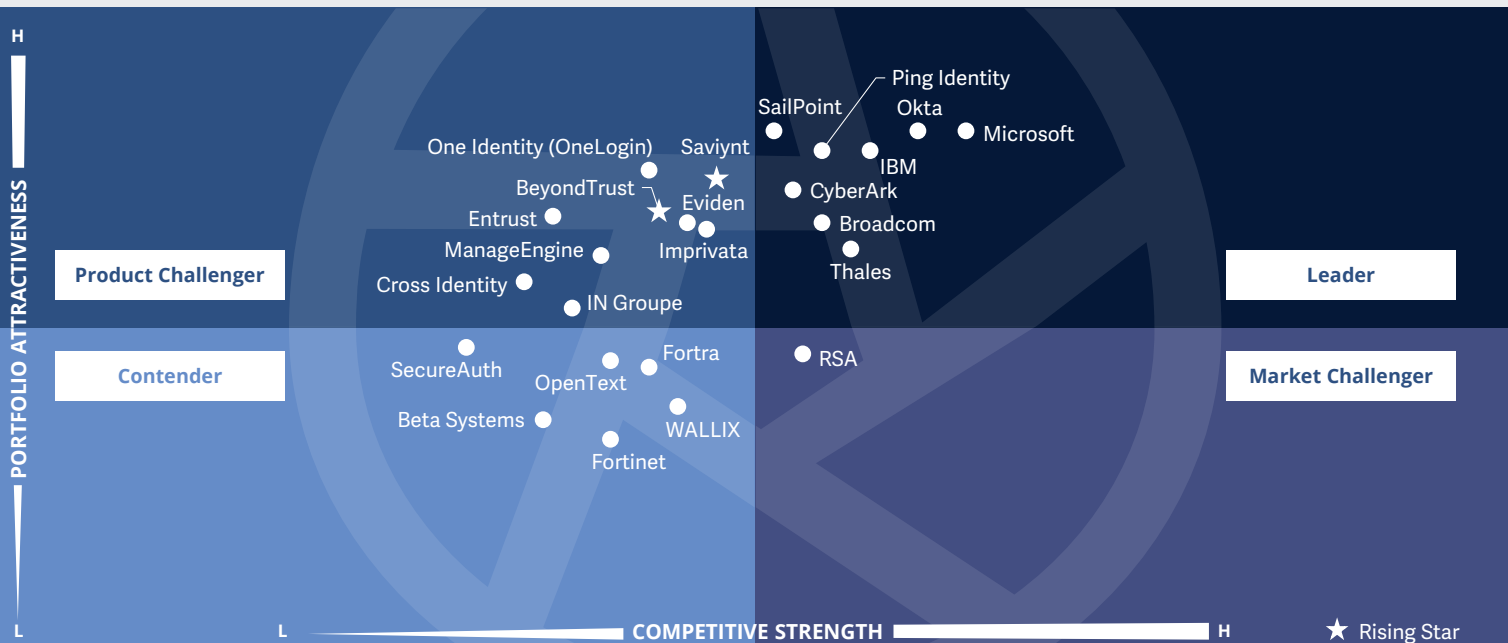


Strategy professionals should read this report to understand how IAM tools can enhance UX while improving the security and efficiency of their systems and data.



Compliance and governance professionals should read this report to learn how to better manage user access to the systems and data to ensure regulatory compliance and streamline audits.





This quadrant assesses providers' ability to manage user and machine identities.

Robust access controls provide a foundational layer for **zero trust** and a keen focus on understanding and **optimizing UX**.

Bhuvaneshwari Mohan



Identity and Access Management

Definition

IAM solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services for managing enterprise user identities and devices. This quadrant also includes SaaS offerings based on proprietary software. It excludes pure service providers that do not offer an IAM product (on-premises and/or cloud) based on proprietary software. Depending on organizational requirements, these offerings could be deployed in several ways, such as on-premises, customer-managed clouds or as-a-service models or a combination thereof.

IAM solutions aim to manage (collect, record and administer) user identities and related access rights and include specialized access to critical assets through privileged access management (PAM), where access is granted based on defined policies. To handle existing and new application requirements, IAM solution suites are increasingly embedded with secure

mechanisms, frameworks and automation (for example, risk analysis) to provide real-time user and attack profiling functionalities. Solution providers are also expected to offer additional functionalities for social media and mobile use to address specific security needs beyond traditional web and contextual rights management. This quadrant also includes machine identity management.

Eligibility Criteria

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



Identity and Access Management

Observations

The UK market has experienced a significant increase in cyberattacks in recent years, showcasing the need for robust identity, security and stronger security models such as zero trust. IAM solution providers are actively adapting to rising demands and expectations by enhancing their capabilities to incorporate key zero trust principles. This includes features such as granular access control, context-aware authorization and microsegmentation. At the same time, others are developing and marketing dedicated zero trust products built from the ground up.

Enterprises migrating their cloud applications and services are driving the demand for cloud-based IAM and hybrid solutions catering to on-premises infrastructure needs will remain relevant in the market. Enterprises make heavy investments in privileged access management (PAM) solutions and passwordless authentication methods.

Incorporating AI and ML for threat detection, anomaly analysis and user behaviour monitoring is becoming crucial to reducing identity risks. Enabling real-time identity threat prevention

based on user behaviour and location and device risk factors is required to continuously assess and mitigate identity risks.

With increased awareness of data privacy concerns, end users are demanding more control over their personal information and are implementing stricter access controls and strong authentication mechanisms. Decentralised identity solutions and user-centric identity management approaches are also gaining traction, reflecting this shift in priorities. Verifiable credentials enable safeguarding the digital identities of both human and non-human entities while exercising control over the digital journey of sensitive data.

From the 82 companies assessed for this study, 24 qualified for this quadrant, with eight being Leaders and two Rising Stars.

Broadcom

With a laser focus on microservices-centric architecture, **Broadcom's** IAM portfolio provides technically well-rounded solutions addressing key areas such as privileged access control, identity governance, secure authentication and seamless access management.

CyberArk

CyberArk differentiates itself with its security-first approach and AI-powered adaptive authentication capabilities that enterprises with enhanced identity security through continuous monitoring while maintaining frictionless UX.



IBM's Security Verify serves as a powerful platform, revolutionizing access management by offering robust solutions that are both modern and straightforward. It transforms the way organizations handle user access, simplifying processes while ensuring heightened security measures are in place.

Microsoft

Microsoft's Entra offers advanced security features such as PAM, identity governance and administration (IGA) and cloud access security broker (CASB) functionalities, providing comprehensive security coverage.

Okta

Okta empowers organizations to manage customer and workforce identities flawlessly through its cloud-based IAM platform. Its features include federation, single sign-on solutions, robust authentication and flexible policy control, catering to diverse needs.



Both **Ping Identity** and ForgeRock (which merged) have continued to focus on innovation in areas such as decentralized identity, threat intelligence, risk-based access control, API-driven security, contributing to deep security expertise.

SailPoint

SailPoint is focused on helping its clients mature their identity security programs. It delivers a seamlessly integrated platform that combines data security, access management, access governance, PAM and AI capabilities to drive their zero trust journey.



Identity and Access Management

THALES Building a future we can all trust

Thales, with its extensive global reach, a vast network of sales and distributors, strong authentication methods, phishing-resistant MFA and advanced fraud detection capabilities, is well-positioned to meet the complex security needs of enterprises.

BeyondTrust

BeyondTrust (Rising Star) provides a seamless approach that allows enterprises to scale privileged security across multiple environments, such as endpoints, cloud and networks, through its intuitive and flexible platform.

Saviynt

Saviynt's (Rising Star) cloud-native architecture, real-time analytics capabilities and seamless integration within the enterprise IT ecosystems and security environment establish a robust foundation for zero trust principles for its clients.





Extended Detection and Response

Extended Detection and Response

Who Should Read This Section

This quadrant is relevant to enterprises globally for evaluating extended detection and response (XDR) solution providers. It assesses how each provider helps enterprises increase visibility across all telemetry sources and obtain a unified view of threat detection and response. ISG offers an analysis of the current positioning of global XDR players with a comprehensive overview of the market's competitive landscape.

Enterprises recognize the need for a proactive approach to threat detection and response, driven by data science techniques and dynamically updated threat intelligence. XDR empowers enterprises of all sizes and security maturity levels to achieve robust threat detection and response capabilities, regardless of limited security personnel, expertise or budget for a dedicated security operations center (SOC). A well-built XDR solution is an SOC enabler that presents a descriptive view of threats and automates initial triage tasks.

Using MITRE ATT&CK framework and open-source intelligence, XDR models detect anomalies and classify attacks based on specific tactics and techniques, providing actionable insights for SOC analysts. It enriches alerts with context, correlating events to determine true threat severity and attack chain participation. This reduces false positives and saves valuable investigative time. Advanced XDR solutions prioritize alerts based on risk scoring and business impact, guiding incident response planning. Additionally, XDR solutions should have a robust set of APIs that allow the extension of workflow functionalities to other external systems to streamline containment actions to events.



Cybersecurity professionals can gain valuable insights into XDR solutions that aid enterprises in enhancing visibility across endpoints to enable unified threat detection and response.

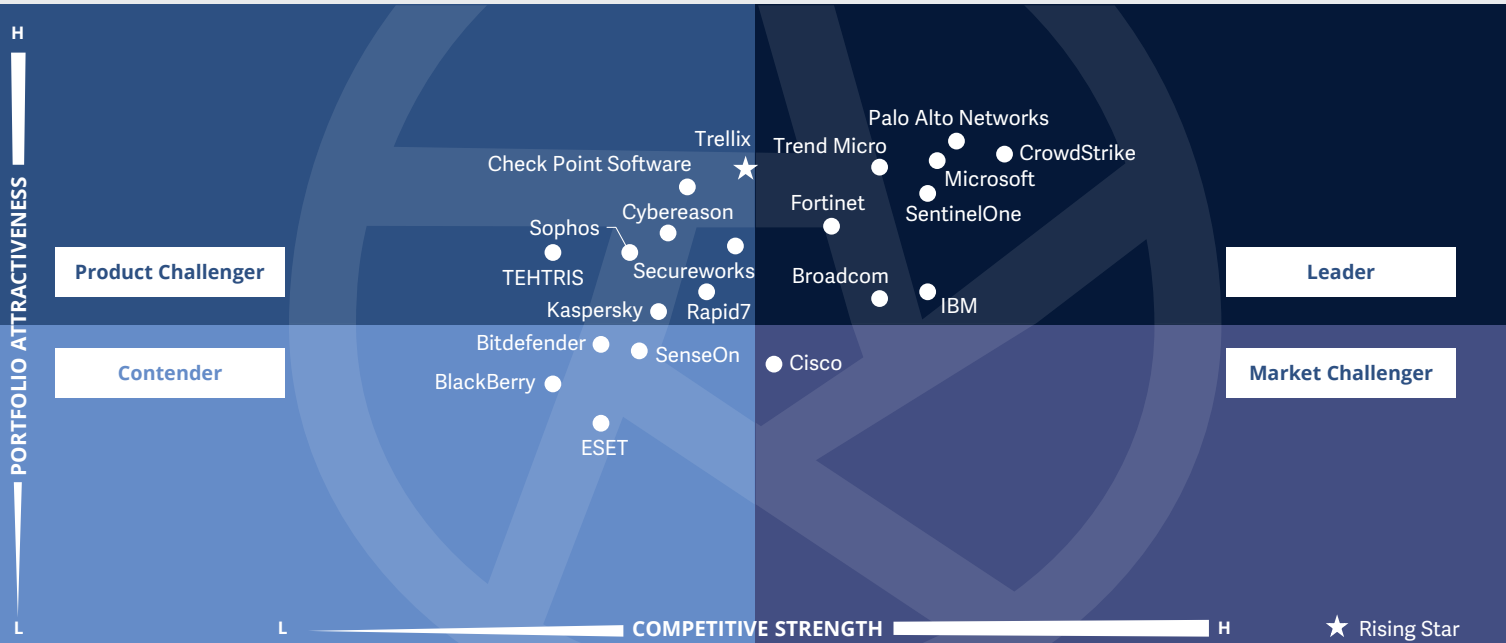


Technology professionals should read this report to understand XDR providers' integration capabilities and how they help with improved detection and faster response times to threats.



Strategy professionals should read this report to understand XDR providers' capabilities in helping enterprises manage security risks effectively and make informed security decisions.





The Extended Detection and **Response** quadrant assesses security vendors' ability to provide integrated threat detection, investigation and response capabilities across multiple endpoints, networks and cloud environments.

Dr. Maxime Martelli



Extended Detection and Response

Definition

The XDR solution providers assessed for this quadrant are characterized by their ability to offer a platform that integrates, correlates and contextualizes data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple-point solutions. It uses advanced analytics to correlate alerts from multiple sources, including weak individual signals, to enable accurate detections. XDR solutions consolidate and integrate multiple products, providing comprehensive security for workspaces, networks and workloads. Typically, XDR solutions are aimed at vastly improving visibility and context understanding of identified threats across the enterprise. Characteristics of these solutions include telemetry and contextual data analysis for detection and response. XDR solutions comprise multiple products integrated into a single pane of glass for sophisticated viewing, detection and response

capabilities. Their high automation maturity and contextual analysis offer tailored responses to affected systems, prioritizing alerts based on severity against known reference frameworks. This quadrant excludes **pure service providers that do not offer an XDR solution based on proprietary software**. XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expenses. They are particularly suitable for security operations teams struggling to manage diverse solution portfolios or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

Eligibility Criteria

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



Extended Detection and Response

Observations

In 2024, the XDR market is evolving with several new trends and advancements. XDR solutions are integrating advanced AI and ML capabilities, thus enhancing behavioral analytics and automating response actions based on learned patterns.

Vendors have also increased their focus on cloud security and are providing comprehensive visibility and protection across hybrid and multicloud environments. XDR platforms are closely aligning with the MITRE ATT&CK framework, enabling more informed threat-hunting and response strategies.

XDR vendors are expanding their offerings to include robust managed detection and response (MDR) services, catering to organizations facing skill shortages. Moreover, XDR solutions are leveraging advanced UEBA for proactive threat detection and response. Automation and orchestration capabilities within XDR platforms are maturing, thus streamlining incident response processes and

reducing manual tasks. XDR also aligns with zero trust principles, emphasizing continuous verification and strict access controls while incorporating features to support regulatory compliance requirements.

Such advancements underscore XDR's role in delivering sophisticated threat detection, response and compliance capabilities amid evolving cyber threats.

From the 35 companies assessed for this study, 21 qualified for this quadrant, with eight being Leaders and one a Rising Star.

Broadcom

Broadcom's XDR includes comprehensive visibility, advanced analytics, automated response and a simplified management console, enabling organizations to effectively protect their digital assets against evolving threats.

CrowdStrike

CrowdStrike's Falcon® Insight XDR flexibility meets the increasing market demand for a simplified and single-pane-of-glass control panel with its Falcon tool. It aims to increase industry robustness by supporting standards and frameworks like CrowdXDR Alliance.

Fortinet

Fortinet's FortiXDR can be seamlessly integrated with Fortinet Security Fabric and Fortinet's other security products to streamline incident response with automated workflows and playbooks. This integration allows fast containment and threat remediation.

IBM

IBM's Security QRadar XDR undertakes a proactive and coordinated approach to threat detection and response, with multiple modules and integration across networks, clouds, endpoints and other workloads.

Microsoft

Microsoft's extensive customer base and strong brand recognition have helped the company establish a prominent position in the XDR market. Its XDR integrates its Defender Advanced Threat Protection (ATP) to provide threat detection and response.

Palo Alto Networks

Palo Alto Networks' strong market presence, commitment to innovation and focus on secure access service edge/security service edge (SASE/SSE) solutions for organizations make Cortex XDR a robust product and Palo Alto Networks a Leader in the XDR quadrant.

SentinelOne

SentinelOne maintains its momentum as one of the leading XDR vendors by using patented behavioral AI algorithms to detect and classify malicious activities. All security functions are bundled in a single agent, thus eliminating the need for multiple security products.



Extended Detection and Response

Trend Micro

Trend Micro expanded its endpoint detection and response (EDR) capabilities into a next-generation XDR product, which aligns with the MITRE ATT&CK framework and offers dynamic risk assessments. Its automation capabilities deliver advanced XDR.

Trellix

Trellix (Rising Star) XDR boasts an adaptable and interoperable framework that seamlessly connects with a vast array of external security solutions, fostering a unified cybersecurity strategy combined with a sophisticated threat detection mechanism.





Security Service Edge

Who Should Read This Section

This report is relevant to enterprises globally for evaluating security service edge (SSE) solution providers. It assesses SSE solutions' key features, such as zero-trust network access (ZTNA), cloud access security broker (CASB) and secure web gateways (SWG). It evaluates how each provider helps enterprises ensure security across hybrid and multicloud ecosystems.

In this quadrant, ISG defines global SSE players' current positioning, offering a comprehensive overview of the competitive market landscape.

Due to the rapid shift to hybrid work models, enterprises seek solutions that accommodate employees, partners, suppliers, and customers accessing internal apps, the internet and SaaS applications. Enterprises want SSE solutions that simplify the adoption and deployment of security policies. A streamlined approach reduces complexity and accelerates implementation. Enterprises expect SSE platforms to monitor and track user activity across a network. Furthermore, SSE providers must protect all users from ransomware and other advanced malware threats.

Enterprises adopt SSE to address modern security challenges, simplify access and enhance digital experiences. They seek providers that offer streamlined solutions, robust protection and agility in a rapidly evolving landscape.

The need for unified, secure access in a hybrid workforce drives SSE adoption. Enterprises expect SSE providers to offer simplified deployment, VPN bypass and robust malware protection. Providers should innovate, customize, prioritize UX and expand their global reach to succeed.



Data management professionals should read this report to understand how SSE providers help enterprises overcome challenges posed by data regulation mandates with better policy controls and reporting.

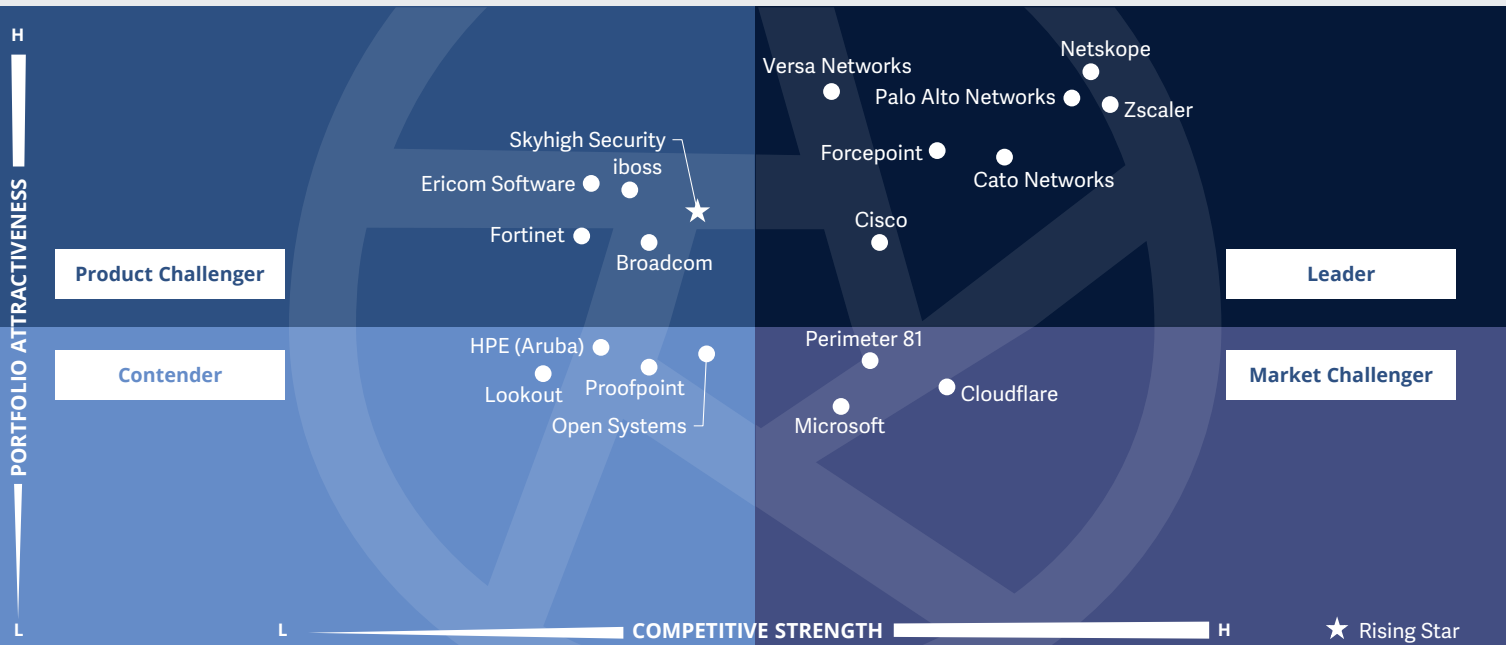


Strategy professionals can gain insights into SSE providers' critical capabilities and focus on user-centricity, delivering security to end users at the edge or devices through cloud.



Technology professionals will be able to understand how SSE providers assist enterprises in adopting an enterprise-wide zero-trust framework to improve their security posture.





This quadrant assesses SSE vendors that offer **cloud-centric solutions** that integrate individual solutions enabling **secure access to cloud services**, SaaS applications, web services and private applications with a **strong focus on UX**.

Gowtham Sampath



Security Service Edge

Definition

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

Vendors showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients.

This quadrant excludes the network components of secure access service edge (SASE), such as SD-WAN, which are covered in the ISG Provider Lens™ Network – Software Defined Solutions and Services 2024 study.

SSE solutions strongly focus on user-centricity, delivering security to end users at the edge or devices through the cloud – rather than allowing users to access enterprise applications and databases – over dedicated networks centrally. ZTNA creates exclusive connectivity between users and applications, using context-based behavioral analysis to manage access. CASB offers visibility, enforces security policies and compliance, and controls shadow IT cloud usage, while FWaaS and SWG prevent malicious threats and access to infected websites and applications. Typically, an SSE solution has a unified console for visibility and governance, with advanced automation to assess UX.

Eligibility Criteria

1. Provide SSE as an **integrated solution with zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**
2. Offer solutions **predominantly based on proprietary software, they may partially rely on partner solutions while avoiding complete dependency on third-party software**
3. Maintain **globally located POPs** to deliver these solutions
4. **Deliver SSE to both cloud and on-premises environments (including hybrid environments)**
5. Exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/UEBA)** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **globally availability of the solution**



Observations

The Security Service Edge market is currently witnessing rapid growth driven by the increasing adoption of cloud applications, expanding remote workforce and evolving cyber threat landscape. ISG's analysis reveals several enterprise challenges necessitating SSE deployments:

Organizations are increasingly using a mix of cloud platforms (public, private and hybrid), as traditional security solutions failed to ensure consistent security across these diverse environments.

With the rise of remote work, securing access to cloud applications from various locations and devices becomes crucial.

Managing a complex security ecosystem with multiple-point solutions can be challenging.

Strict regulations like the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA) and GDPR require robust data security measures.

Differentiation and characteristics in the SSE market:

Enterprises prioritize SSE vendors that cater to their industry-specific compliance and regulations and data security concerns.

They seek vendors offering open standards and pre-built integrations with existing security tools and cloud platforms to avoid vendor lock-in and simplify deployment.

SSE solutions need to scale effectively to accommodate growth in cloud application usage and user base, with low latency and reliable performance, which are essential for ensuring a positive UX for geographically dispersed workforces.

Enterprises prefer vendors with robust threat intelligence capabilities and a proven track record of security expertise.

Transparency in pricing and a clear understanding of the TCO, including integration costs, is critical for companies when selecting an SSE vendor.

From the 35 companies assessed for this study, 19 qualified for this quadrant, with seven being Leaders and a Rising Star.

Cato Networks

Cato Networks focuses on improving the integration and performance of its SSE solutions by upgrading its ZTNA capabilities within the Secure Connect platform and expanding its partnerships with cloud providers.

Cisco

Cisco prioritizes integrating its SSE solution, Secure Access, with other Cisco security products to achieve a unified approach. The company also strengthens partnerships with cloud providers like Microsoft to enhance Secure Access' functionalities.

Forcepoint

Forcepoint focuses on expanding the reach of its Forcepoint Cloud Security Gateway, an SSE platform, by launching integrations with additional cloud platforms. This strategic move aligns with the growing adoption of multicloud environments.

Netskope

Netskope is expanding its global data center network, aiming to offer lower latency, improved performance and user reach. The company is also focusing on partnerships with SIEM vendors to enhance threat detection and investigation capabilities within its SSE platform.

Palo Alto Networks

Palo Alto Networks has introduced improvements to UX and streamlined policy management tools within its Prisma SASE platform. The company also strengthened partnerships with cloud providers such as AWS to offer preconfigured security policies.

Versa Networks

Versa Networks has introduced enhanced cloud workload protection functionalities within its Versa SASE platform and established partnerships with threat intelligence providers to improve threat detection capabilities, ensuring comprehensive protection for customers.



Security Service Edge



Zscaler has expanded its global data center network to improve performance for its Zscaler ZSSP platform. It also increased focus on partnerships with SASE framework providers for industry-standard secure access, fostering a unified and secure cloud security ecosystem.

Skyhigh Security

Skyhigh Security (Rising Star) has launched Cloud Workload Protection Platform (CWPP) integration to offer comprehensive cloud security alongside its core SSE platform. This offering surpasses basic SSE functionalities, extending additional protection for cloud workloads.





Technical Security Services

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.

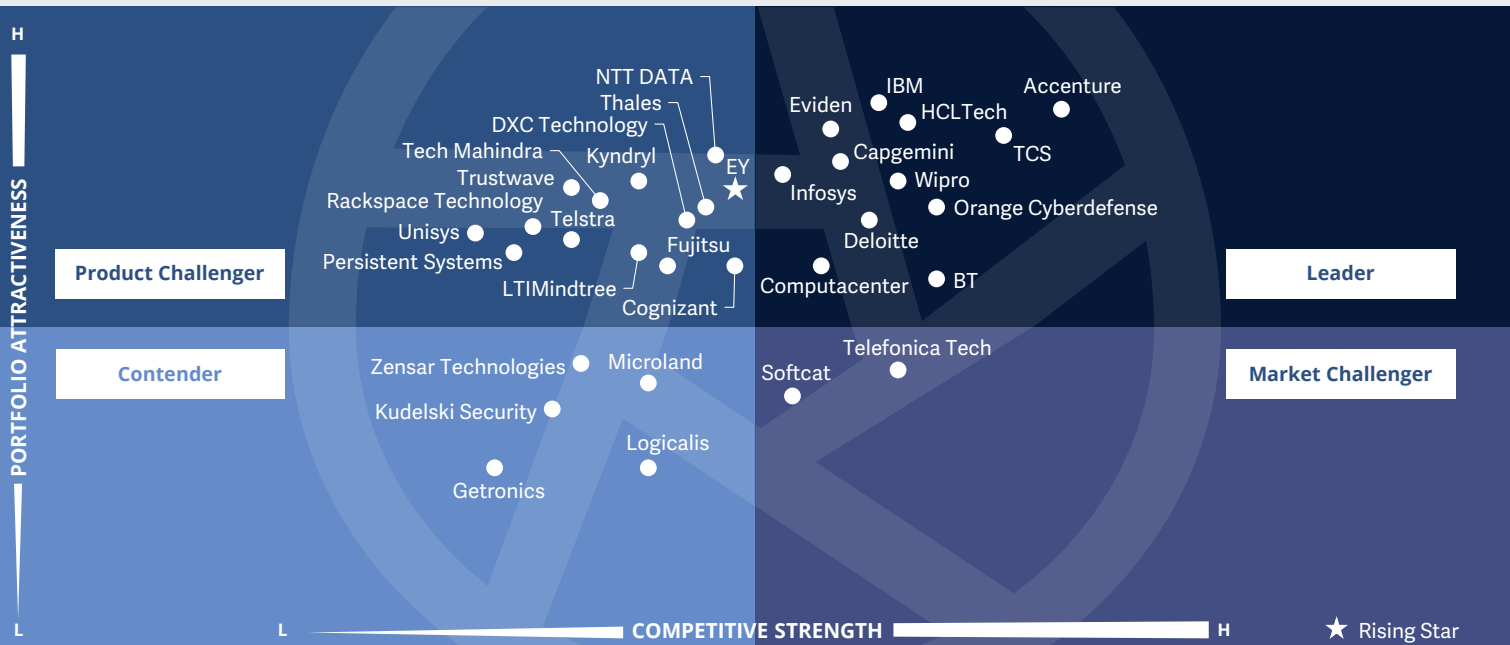


Digital professionals, including IT and digital transformation leaders, should read this report to understand the importance of early adoption and integration of security best practices.



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.

Cyberdefense

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

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.





“Infosys helps enterprises transform to next-gen security technologies with zero trust and security by design principles coupled with its deep technical expertise.”

Bhuvaneshwari Mohan

Infosys

Overview

Infosys is headquartered in Bengaluru, India. It has more than 322,600 employees across 274 offices in 56 countries. In FY23 the company generated \$18.2 billion in revenue, with Financial Services as its largest segment. Infosys has a large pool of 6,200 talented security experts, an extensive partner network of over 100 technology vendors and more than 15 startup partners. Infosys continues to invest in reusable artefacts and IPs to deliver agility and scale, focusing on tailored solutions based on client’s industry and regional preferences.

Strengths

Roadmap for security vendor consolidation:

Infosys tackles the complexities of disparate security tools within isolated setups by defining the roadmap for vendor consolidation. It offers consulting services for evaluating cost benefits and conducting zero trust assessments. The consulting aids enterprises in implementing tightly integrated security measures, serving as the bedrock for cyber mesh and zero trust frameworks.

Highly customizable solutions: Infosys’ integrated managed protection, detection and response (MPDR) solution built with its Cyber Next platforms helps to elevate overall security maturity for its clients. It has an extensive library of over 3,000 use cases covering multiple SIEM technologies and

over 250 automation playbooks, which are plug-and-play mode and quickly customizable as per customer needs.

High innovation focus: Infosys Cybersecurity invests 1-2 percent of its annual revenue in innovating and creating new solutions. It has launched four new intellectual property assets in the last 12 months, including Infosys Identity Management, DigiEye – Health Monitoring and Audit Framework, Infosys Infrastructure Security Workbench and Infosys Indicators of Compromise (IOC) Enrichment Platform.

Caution

In the UK, Infosys should continue to enhance its visibility and establish itself as a thought leader in cost optimization and security solutions rationalization. It should further demonstrate the value proposition it brings in its board-level engagements.





Strategic Security Services (Large Accounts)

Strategic Security Services (Large Accounts)

Who Should Read This Section

In this quadrant, ISG evaluates service providers specialised in strategic security services for large enterprises across industries in the UK that can assess their security maturity and risk posture to define tailored cybersecurity strategies.

Enterprises need a collaborative approach for a detailed gap analysis to identify potential risk areas and focus on mitigation plans. With the ever-changing regulatory requirements, enterprises also look for readiness and data protection impact assessments regarding GDPR, DORA, NIS2, DPDI Bill, EU-AI Act and other upcoming regulatory mandates such as the Product Security and Telecommunications Infrastructure Protection Act. Providers help clients develop comprehensive security strategies aligned with their business goals, risk tolerance and regulatory requirements while considering the adoption of emerging technologies such as cloud and IoT, considering the evolving threat landscape. Zero trust maturity assessments are also crucial for UK

enterprises to assess their existing security technologies and architecture, focusing on identity-based access controls and micro-segmentation. Enterprises must implement stricter security controls to mitigate risks and assess their trust in their measures. Supplier risk assessments are gaining traction as enterprises increasingly seek to optimise their supply chain security programs. Suppliers with high-risk scores are subjected to in-depth assessments to ensure security compliance. Offensive security services, especially attack surface management, penetration testing and breach simulations, are used to gain insights into the critical vulnerabilities and gaps across clients' security estates.



Cybersecurity professionals should read this report because it provides a broad perspective on security trends. It highlights providers' capabilities in helping enterprises devise security strategies.



Procurement professionals should read this report to identify potential security risks associated with specific technologies or vendors 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.

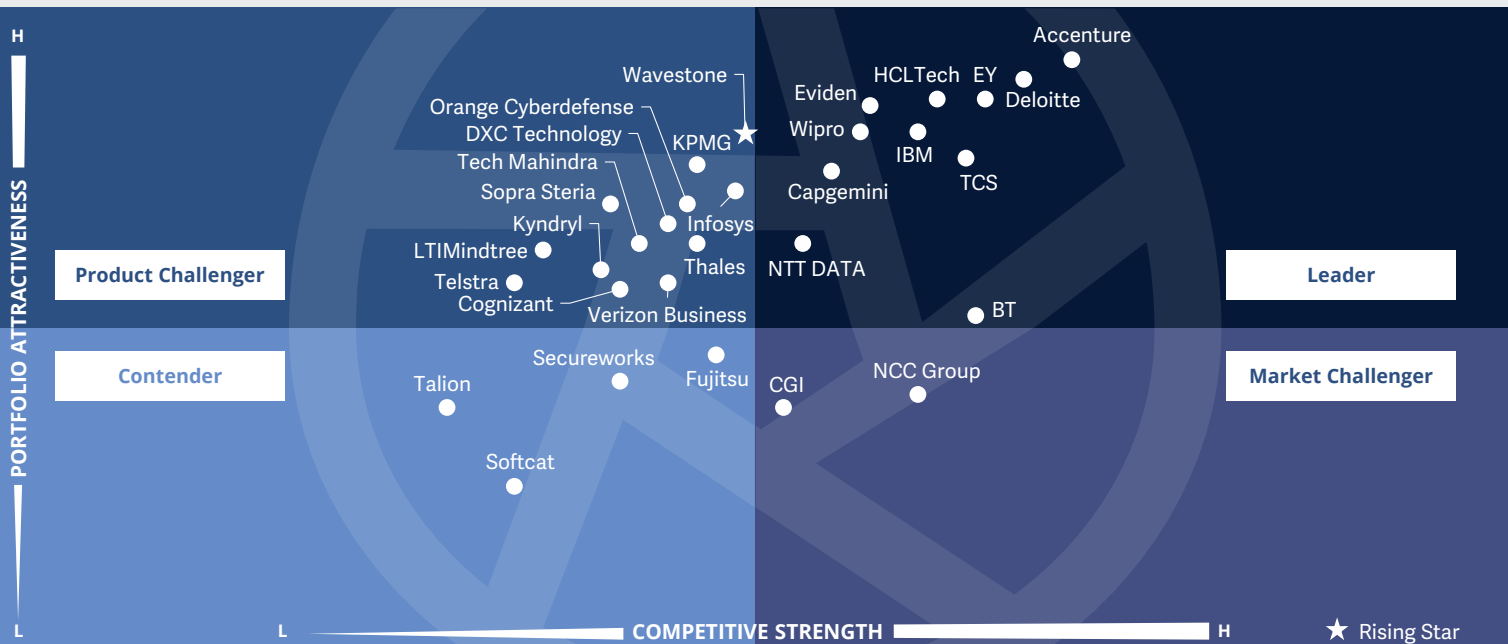


Data management professionals, including security and privacy officers, should read this report to understand the ever-evolving data protection standards and regulations in the UK and EU.



Cybersecurity – Solutions and Services
Strategic Security Services (Large Accounts)

U.K. 2024



This quadrant assesses service providers offering **flexible and tailored end-to-end security programs** to suit the unique needs of enterprises, guiding them with their **security investments** to make informed security decisions.

Bhuvaneshwari Mohan



Strategic Security Services (Large Accounts)

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with extensive experience in planning, developing and managing end-to-end security programs for enterprises. With the growing need for such services among SMBs and the lack of talent availability, SSS providers should also make these experts available on-demand through vCISO (virtual chief information security officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity roadmaps and prioritize business-critical applications for recovery.

They should also conduct periodic tabletop exercises and cyber drills for board members, key business executives and employees to help them develop cyber literacy and establish best practices to better respond to actual threats and cyberattacks. They should also be adept with security technologies and products available in the market and offer advice on choosing the best product and vendor suited to an enterprise's specific requirements.

This quadrant examines service providers that are not exclusively focused on proprietary products or solutions. The services analyzed here cover all security technologies, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Offer at least one of the above strategic security services in the respective country
3. Provide security consulting services using frameworks
4. No exclusive focus on proprietary products or solutions



Strategic Security Services (Large Accounts)

Observations

The key developments in the strategic security services space in the UK market have been centered around enhancing the capabilities around the below areas, coupled with investments.

Providers are assisting organizations in optimizing their security investments to maximize return on investment (ROI). This includes conducting security assessments, identifying redundant or underutilized tools and recommending cost-effective solutions that align with the organization's security priorities and budget constraints.

The new requirements of NIS2 and DORA for financial institutions focuses on incident reporting, vulnerability disclosures and third-party security risk management. Providers are enhancing their capabilities with AI-powered risk assessment, threat modelling and ready-to-use assessment frameworks.

Quantum security risk exposure assessment is gaining traction helping enterprises evaluate their vulnerabilities to emerging quantum threats.

Cyber risk quantification and benchmarking tools are becoming more relevant in the market. There is a rising need for real-time visibility of risk scores at all levels, which helps with better decision-making at the board level.

Zero-trust road mapping, OT maturity assessments and associated compliance, data privacy compliance, cloud security posture assessments, vulnerability assessments covering the complete attack surface, penetration testing and assurance services are gaining prominence.

GenAI-related advisory services, such as governance guardrails and model testing for ethics validation and tracking of GenAI assets and other services, will increase and mature in the next 6-12 months.

From the 82 companies assessed for this study, 30 qualified for this quadrant, with eleven being Leaders and a Rising Star.

accenture

Accenture positions itself as a reliable partner for enterprises seeking to fortify their security strategies and safeguard enterprise value by embracing zero trust principles and securing digital assets across the entire technology spectrum as businesses evolve.

BT

BT, honing on its extensive experience in network and cloud security, enables enterprises to use a proactive security approach to secure their digital transformations by building visionary security architectures based on their risk tolerance level.

Capgemini

Capgemini consistently enhances its portfolio, integrating new elements such as zero-trust framework, ERP secure design blueprint, DevSecOps and 5G security use cases. It benchmarks clients' security state with regulatory standards, aiding informed ROI-driven investments.

Deloitte.

Deloitte's unique industry perspective, complemented by its broad risk advisory experience, empowers enterprises to grasp their industry-specific threat landscapes and effectively reduce disruptions and business impact.

EVIDEN an atos business

Eviden (an Atos business) follows an outcome-based approach to help clients realize greater value from their security investments. It works with its clients to develop measurable security goals and delivers services designed to achieve them.

EY

EY's consultants bring cross-functional and multidisciplinary expertise, empowering clients with industry best practices and extensive domain knowledge, providing holistic insights and threat intelligence with a risk-based approach to provide resilience across clients' digital programs.



Strategic Security Services (Large Accounts)

HCLTech

HCLTech follows an outcome-driven approach, using proven assessment methodologies and frameworks to enable clients to make risk-based decisions and embed security and privacy by design measures with an established GRC practice.



IBM provides comprehensive security maturity assessments, assists clients in embedding security best practices in their digital transformation journey and provides customized approaches to help clients adhere to compliance and streamline security operations.



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



TCS fosters strong relationships with clients, enables it to use deep contextual knowledge of their environments, enhances its board-level visibility and be a trusted and credible partner to them with a heavy emphasis on cyber resilience.



Wipro provides a holistic approach to risk assessment and management, empowering enterprises to make informed security decisions, prioritize investments, identify critical gaps and provide security recommendations proactively.

Wavestone

Wavestone (Rising Star) has a dedicated inhouse research team that provides actionable insights derived from global data sources, coupled with its unique consulting methodologies and tools that help clients in informed decision-making.





Strategic Security Services (Midmarket)

Strategic Security Services (Midmarket)

Who Should Read This Section

In this quadrant, ISG presents the strategic security services providers and the support they offer to small and midmarket enterprises to combat security threats. It also provides insights into how each provider addresses the critical challenges and unique security requirements of SMB clients.

SMBs are an integral part of the UK's cybersecurity landscape. Given their involvement in large supply chains, cyberattacks on these targeted businesses pose significant security concerns on multiple levels. SMBs often lack robust security measures and are alluring targets for cybercriminals seeking to exploit vulnerabilities. Additionally, breaches within SMBs can serve as entry points for attackers to infiltrate larger organisations within the supply chain.

Pure-play cybersecurity providers and MSSPs in the UK recognise these challenges and offer guidelines and best practices tailored to SMBs to bolster their cybersecurity defenses with a risk-based approach to drive continuous improvements. Providers offer comprehensive risk assessment services for adaptive cybersecurity processes to address ransomware attacks and other emerging threats and vulnerabilities. The services include the setup of controls aligned with the National Institute of Standards Technology (NIST) ransomware risk management framework and defense-in-depth-based tiered setup of security controls to bolster defense mechanisms against such attacks. Enterprises are turning to virtual chief information security officer (CISO) services to mitigate such risks, resulting in an ever-increasing demand for specialised services in the UK market.



Cybersecurity professionals should read this report because it provides a broad perspective on security trends. It highlights providers' capabilities in helping enterprises devise security strategies.



Procurement professionals should read this report to anticipate potential security risks associated with specific technologies or vendors and make informed sourcing decisions.

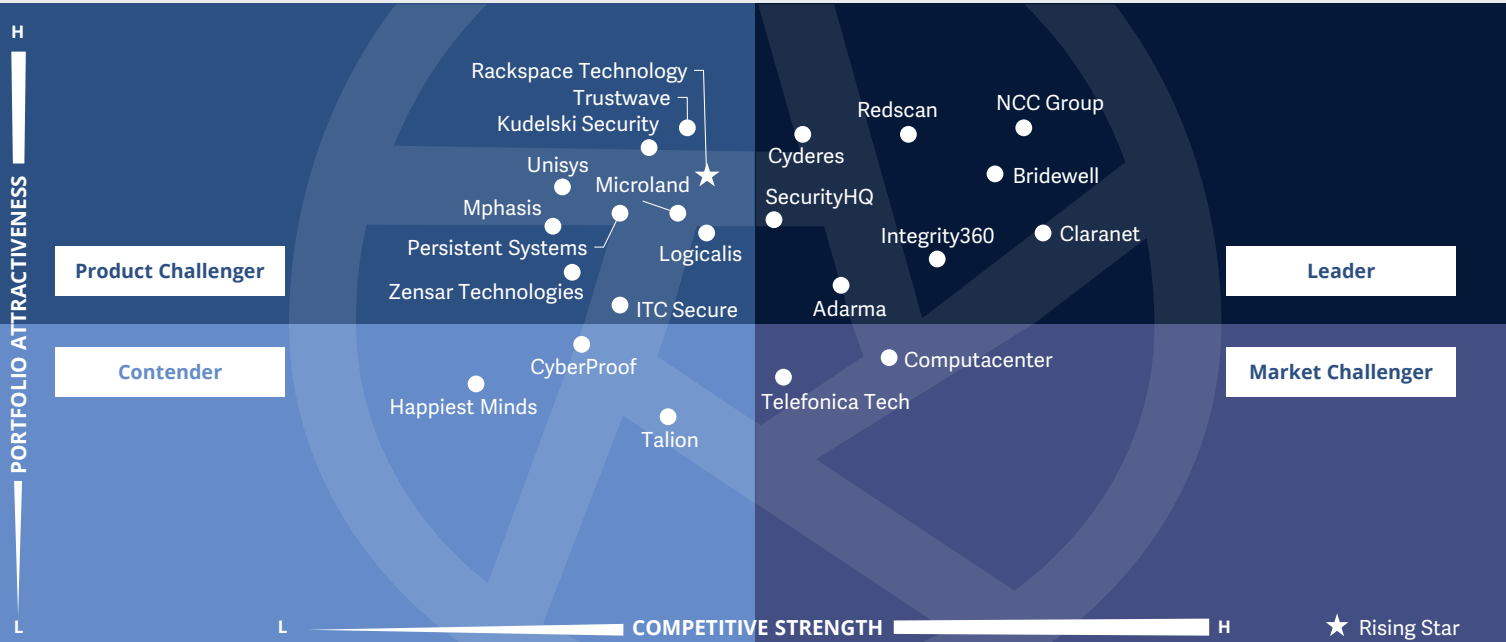


Risk management professionals involved in risk management, compliance and governance should read the report to understand the providers' risk-based approaches and risk assessment services.



**Cybersecurity – Solutions and Services
Strategic Security Services (Midmarket)**

U.K. 2024



This quadrant assesses service providers offering **flexible and tailored end-to-end security programs** to suit the unique needs of enterprises, guiding them with their **security investments** to make informed security decisions.

Bhuvaneshwari Mohan



Strategic Security Services (Midmarket)

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with extensive experience in planning, developing and managing end-to-end security programs for enterprises. With the growing need for such services among SMBs and the lack of talent availability, SSS providers should also make these experts available on-demand through vCISO (virtual chief information security officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity roadmaps and prioritize business-critical applications for recovery.

They should also conduct periodic tabletop exercises and cyber drills for board members, key business executives and employees to help them develop cyber literacy and establish best practices to better respond to actual threats and cyberattacks. They should also be adept with security technologies and products available in the market and offer advice on choosing the best product and vendor suited to an enterprise's specific requirements.

This quadrant examines service providers that are not exclusively focused on proprietary products or solutions. The services analyzed here cover all security technologies, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Offer at least one of the above strategic security services in the respective country
3. Provide security consulting services using frameworks
4. No exclusive focus on proprietary products or solutions



Strategic Security Services (Midmarket)

Observations

The small and mid-sized enterprises of the UK seek the help of service providers with regional presence and have security advisory offerings tailored to their specific needs. SMB clients rely on these providers as trusted advisors that can deliver strategic services with a proven track record of success. These services are instrumental in crafting and articulating cybersecurity strategies and programs that meet regulatory requirements and effectively mitigate risk.

Providers must demonstrate extensive expertise in identifying security gaps, assessing associated risks and devising comprehensive remediation plans to minimize risk exposure. With cloud and remote workforce adoption rising, enterprises are unaware of the cloud security requirements. They need advisory services for technical controls such as endpoint protection. Providers support enterprises by conducting regular risk assessment reviews and vulnerability testing, identifying concerns and deploying automated monitoring and testing tools.

They also need support, training and guidance in preparing their business for Cyber Essentials accreditation, a UK government scheme for SMBs to strengthen their cybersecurity posture and build trust among their clients. Cyber Essentials certification has become a basic requirement for midmarket enterprises to participate in UK public contracts. It has also emerged as an effective tool for lowering their cyber insurance policy premiums.

To strengthen the security measures of the midmarket clients, providers are helping them with regular cyber awareness training for their employees to improve their security awareness and reduce human error.

From the 82 companies assessed for this study, 23 qualified for this quadrant, with eight being Leaders and a Rising Star.

Adarma

Adarma equips clients to make informed cybersecurity decisions by quantifying cyber risks, analyzing business impact and prioritizing investments for maximum protection against evolving threats.

Bridewell

Bridewell provides top-notch cybersecurity advisory services for clients with complex and high-risk security requirements. It has a strategic focus on protecting and transforming critical national infrastructures.

claranet

Claranet's penetration and application security testing capabilities are comprehensive and designed to help enterprises identify and address security vulnerabilities proactively and effectively.

Cyberes

Cyberes provides a comprehensive cloud security assessment with a risk-based approach, enabling clients to evaluate and optimise security architectures and policies to create a prioritized roadmap for improving security and reducing risk across the enterprise.

Integrity360

Integrity360 collaborates closely with clients to understand their challenges, offering tailored expert advice backed by a team known for integrity and innovation that serves over 1,500 clients in the UK and Ireland.

NCC Group

With a risk-focused approach and extensive industry expertise, **NCC Group** aids in understanding their risk landscape, identifying and prioritising security vulnerabilities and developing customized security roadmaps.

Redscan

Redscan, a Kroll Business, offers a wide range of strategic security advisory and consulting services and a proactive approach to incident response and detection, plus MDR and DFIR services to enhance clients' cyber resilience.



Strategic Security Services (Midmarket)

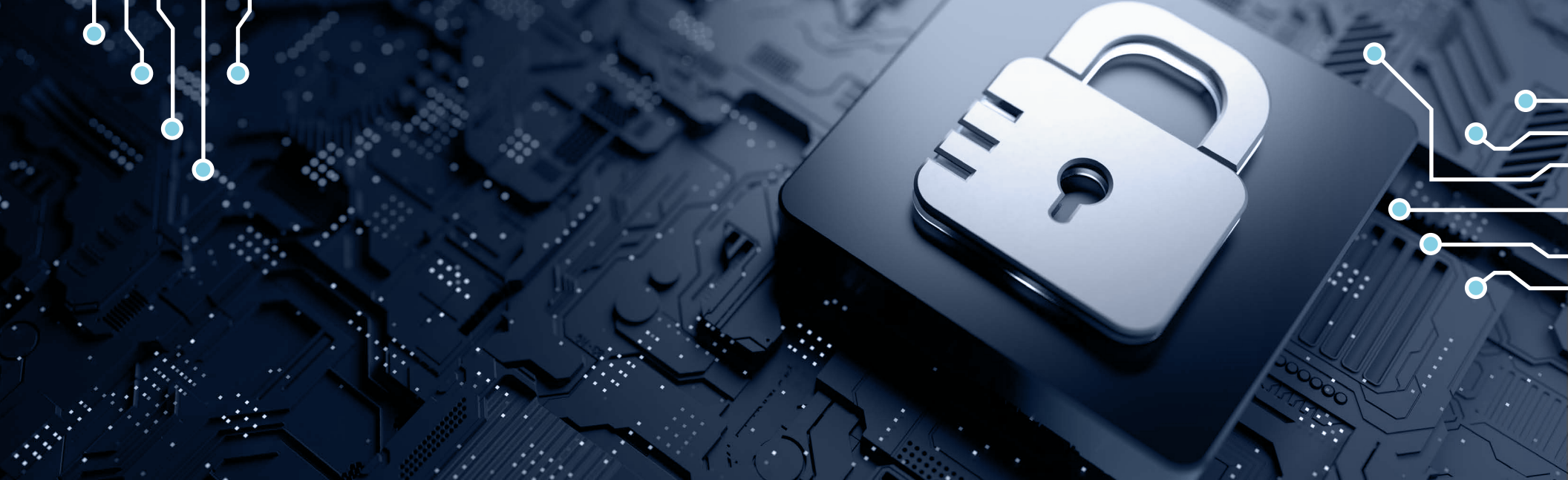
SecurityHQ

SecurityHQ takes a risk-based approach to identify critical vulnerabilities and gaps in client's security infrastructure, providing contextualized risk assessments with expert guidance to enhance security posture.

rackspace technology.

Rackspace Technology (Rising Star) provides security assessments to identify gaps, plus information security strategy services and cloud security resiliency and compliance, enabling clients to shape security outcomes with best-practice architecture design and processes.





Managed Security Services – SOC (Large Accounts)

Managed Security Services – SOC (Large Accounts)

Who Should Read This Section

In this quadrant, ISG evaluates providers specialising managed security SOC services for large enterprises across industries in the UK, helping them combat security threats. It also provides insights on how each provider addresses critical market challenges.

Enterprises require continuous monitoring of their IT and OT security infrastructures to keep up with the rising expansion of attack surfaces due to the ongoing adoption of digital technologies. A great emphasis lies on industry-specific detection and response capabilities. AI and automation play an important role in the incident detection and response processes, and enterprises are increasingly looking for enhanced protection with reduced incident volumes. Current market challenges drive an increased focus on improving security operations' productivity and efficacy, optimising existing technology's effectiveness and establishing unified visibility and security monitoring aligned with digital transformation strategies. Current and upcoming regulations include challenging compliance requirements that burden security teams. Automated

reporting and compliance checks reduce manual work and ensure consistent compliance adherence. The increasing complexity of threats from diverse IT and OT environments of enterprises across on-premises, hybrid and multicloud requires robust threat intelligence, proactive threat hunting, contextualised threat analysis using AI and ML and faster response times. Enterprises increasingly shift from traditional MSS to managed detection and response models as they offer more proactive threat detection and response capabilities.



Technology professionals, including CISOs and CXOs, should read this report to identify the emerging trends and immediate threats to make strategic decisions, enhance productivity and reduce security complexity.



Business professionals, including line of business (LOB) and industry practitioners, should read this report to understand industry-specific threats and vulnerabilities for quick threat response.

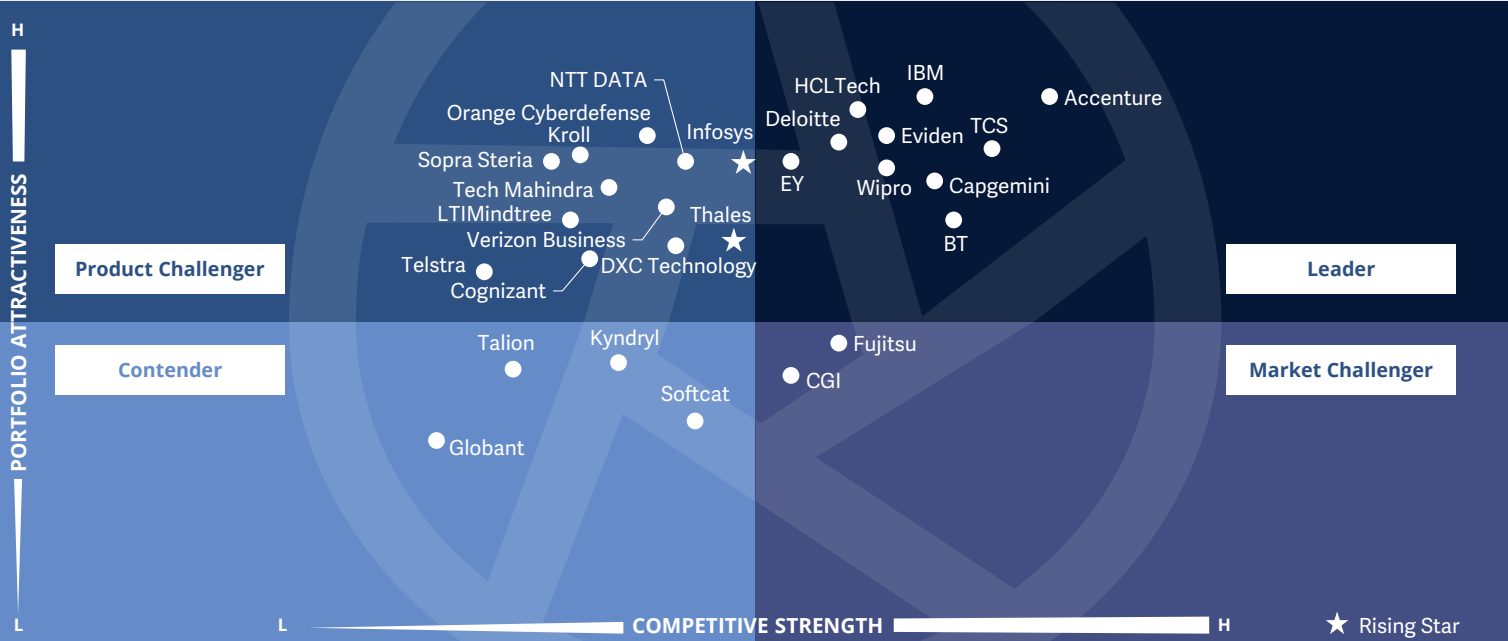


Operations professionals, including IT, security operations and networking leaders, should read this report to gain insights into reducing complexity and enhancing efficiency.



Cybersecurity – Solutions and Services
Managed Security Services - SOC (Large Accounts)

U.K. 2024



This quadrant evaluates providers' ability to blend traditional managed security services with innovative capabilities, offering **advanced threat detection**, thorough **monitoring**, industry-specific use cases, **automation** efficiency, and **scalable service models**.

Bhuvaneshwari Mohan



Managed Security Services – SOC (Large Accounts)

Definition

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

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional managed security services with innovation to fortify clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies and infrastructure.

They must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, security information and event management (SIEM) services**, security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. **Manage own SOCs**
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models



Managed Security Services – SOC (Large Accounts)

Observations

MSS providers are expanding their SOC capabilities in new geographies to enhance their cybersecurity offerings and provide global coverage. This expansion allows MSSPs to cater to the specific cybersecurity needs of diverse industries and regions and offer localized threat detection and response services. At the same time, enterprises should be ensured they have access to 24/7 security monitoring and incident response services.

Most MSPs offering IT services capitalize on this opportunity to integrate security-related services for clients. In the UK, there is a notable trend where security teams collaborate closely with workplace services teams to deliver advanced security services to clients.

AI-powered SOCs are the new norm. Organisations integrate AI into threat detection, incident response and security analytics. AI can analyze large volumes of data, reduce false positives and recommend real-time actionable insights to SOC analysts.

Security solution vendors such as CrowdStrike, Microsoft and Palo Alto Networks are developing specialized managed security services, which pose a significant challenge to MSSPs and increase competition and price pressures.

Providers have started demonstrating their capabilities in the OT/IoT side of SOC operations. The convergence of OT/IT ecosystems for effective protection against cyber threats, as OT environments, such as those in manufacturing and industrial settings, are often targeted by sophisticated attacks that disrupt operations. Recently, CISOs and CIOs have been considering the responsibility for protecting these environments as a direct liability, adding another layer of challenge to an already complex issue.

From the 82 companies assessed for this study, 28 qualified for this quadrant, with ten being Leaders and two Rising Stars.

accenture

Accenture's comprehensive approach draws from extensive expertise and innovative capabilities to provide a 360-degree view of the client's security posture. It uses advanced analytics and automation to encompass threat exposure management, robust threat detection and response.

BT

BT's Eagle-i cyber defence platform provides real-time threat detection and response. This platform uses AI, automation and predictive analytics to provide comprehensive threat defence across multicloud environments.

Capgemini

Capgemini provides dedicated tools, resources and technologies across its cyber defense centres (CDCs), with extensive R&D investments to deliver services that are specifically created around each client's industry, risk profile and security objectives.

Deloitte.

Deloitte adopts a business-led approach in its client engagements, orchestrating outcome-based solutions that are tailor-fit to industry and regional specifications with a wide array of cloud-based assets and modular platforms.

EVIDEN

an atos business

Eviden (an Atos Business) offers advanced SOC capabilities via its Alsaac platform employing cyber mesh architecture to extend protection across cloud and edge, enhancing visibility, enabling threat hunting using AI, ML and SOAR integrated automated containment.

EY

EY, with a platform-based approach, provides strategic value to clients with robust threat intelligence, threat hunting and vulnerability management capabilities. It enables intelligent automation for enhanced cyber resilience and streamlined security infrastructure.



Managed Security Services – SOC (Large Accounts)

HCLTech

HCLTech stands out for its dedication to helping clients maintain dynamic security postures. It achieves this through advanced threat intelligence, automation, tailored solutions and proactive strategies to empower organizations to evolve their security.

IBM

IBM delivers robust security outcomes using real-time threat detection and response using AI and ML and rich contextual threat intelligence from the X-Force team, enhancing clients' overall security posture with 360 degree visibility.

tcs TATA CONSULTANCY SERVICES

TCS boasts over 450 use case libraries and 50 automation playbooks. Continuously refining in the enterprise context enhances the true positive rate of detection rules for security alerts, enabling adept responses to help enterprises defend off cyber threats.



Wipro designs its cyber defence platforms to improve security posture and resilience by taking a holistic approach to unified threat detection and response, using its strong relationships with security vendors and globally spread CDCs.

Infosys

Infosys (Rising Star) builds its MPDR and Cyber Next platforms on an integrated and comprehensive architecture. It allows BYOT (bring your own technology), making it a modular, feasible, flexible and optimal option for clients across all verticals.

THALES Building a future we can all trust

Thales' (Rising Star) cyber detection services portfolio includes a wide range of services such as MSS, MDR, threat hunting and intelligence, DFIR, EASM, SOC build and transfer and deceptive security services, including MSS for highly regulated perimeters.





“Infosys’ cyber capabilities that provide holistic alignment with zero trust architecture and automation and an intellectual property-enabled platform-based approach set it apart.”

Bhuvaneshwari Mohan

Infosys

Overview

Infosys is headquartered in Bengaluru, India. It has more than 322,600 employees across 274 offices in 56 countries. In FY23 the company generated \$18.2 billion in revenue, with Financial Services as its largest segment. It has multiple platforms delivering MSS, such as Cyber Gaze, Cyber Hunt, Cyber Compass and Cyber Central and constantly upgrades them to keep them in line with market trends and customer requirements. It offers end-to-end cybersecurity services from advisory to implementation, and managed services across all key security domains such as IAM, infrastructure security, data security and privacy, GRC, cloud security, vulnerability management and OT security.

Strengths

Outcome-based approach: Infosys employs a tailored SecOps delivery model that drives business outcomes for its clients. The Infosys Cyber Next platform helps enterprises with scalable and resilient ecosystems. It integrates fully automated response playbooks and AI-led predictions to preempt similar threats in the future for improved threat detection and response.

Thought leadership: Infosys demonstrates a dedicated focus on thought leadership through various initiatives, publishing over 40 reports and whitepapers covering diverse cybersecurity domains, including GenAI. The recent launch of its annual report, TechCompass, underscores its commitment to tracking the latest cybersecurity trends and collaborating with industry bodies

such as NASSCOM and the Information Security Forum and engaging with CXOs of its clients through advisory councils, solidifying its scalability and commitment to deliver excellence.

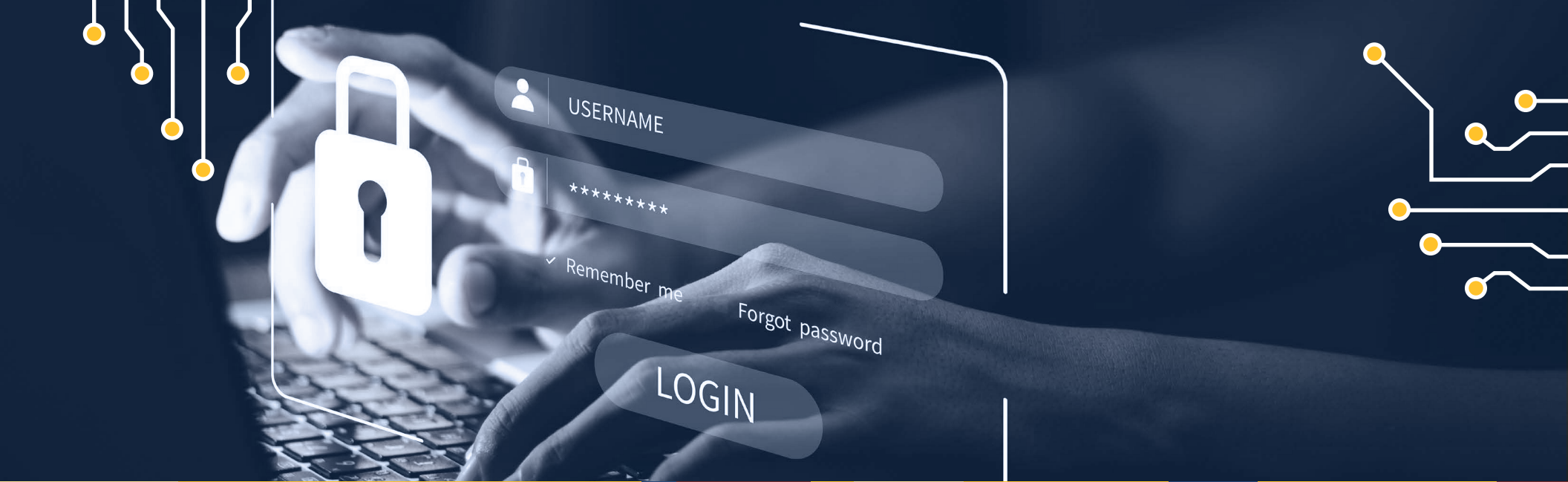
Automation-led delivery: Infosys’ dedicated team for automation helps build use cases, bots and accelerators. It has developed over 100 reusable use cases spanning IAM, infrastructure security and data security, along with 200 reusable bots, automation platforms and 300 detection use cases. It has created over 20 automated incident response playbooks for risk-based vulnerability remediation management governance.

Caution

Using its deep technical expertise and skilled resources, Infosys should continue to invest in OT security capabilities, developing assets and accelerators to target industry-specific use cases in the UK.

Infosys should expand its UK presence with local talent and a business development team.





Managed Security Services – SOC (Midmarket)

Managed Security Services – SOC (Midmarket)

Who Should Read This Section

In this quadrant, ISG evaluates the providers of managed security SOC services and the support they offer to small and midmarket enterprises to combat security threats. It also provides insights into how each provider addresses the critical challenges in the market.

SMBs seek SOC services based on Microsoft security technologies to capitalise on their E5 licensing investments or for services that integrate with their existing systems. Enterprises are looking for end-to-end services from assessment to implementation and managed services specific to the Microsoft security ecosystem. Providers engage with these clients, providing skilled resources for improved protection against insider threats, zero-day attacks, ransomware and data breaches. Some providers also engage with these clients in a co-managed SOC approach. In addition to optimising and streamlining their security infrastructures, these services provide clients with enhanced protection

in areas such as cloud security, workplace security, data security, threat protection and IAM. Many small and midsize providers in the UK that claim to offer managed detection and response services specifically target SMBs; however, they often have limited capabilities and lack robust telemetry support. These providers usually lag behind larger competitors when prioritising alert fatigue, proactive threat hunting and incident response workflow automation. Therefore, enterprises must be careful when selecting providers to ensure that they offer tailored features and deployment options. Large providers are starting to catch up by downscaling their services to cater to the SMB market in the UK.



Compliance and governance professionals

should read this report to understand how service providers help enterprises address security needs, mitigate risks and ensure regulatory compliance.



Business and strategy professionals,

including LOB leaders and CXOs, should read this report to stay up-to-date on security solutions, identify gaps in their current security posture and choose effective tools.

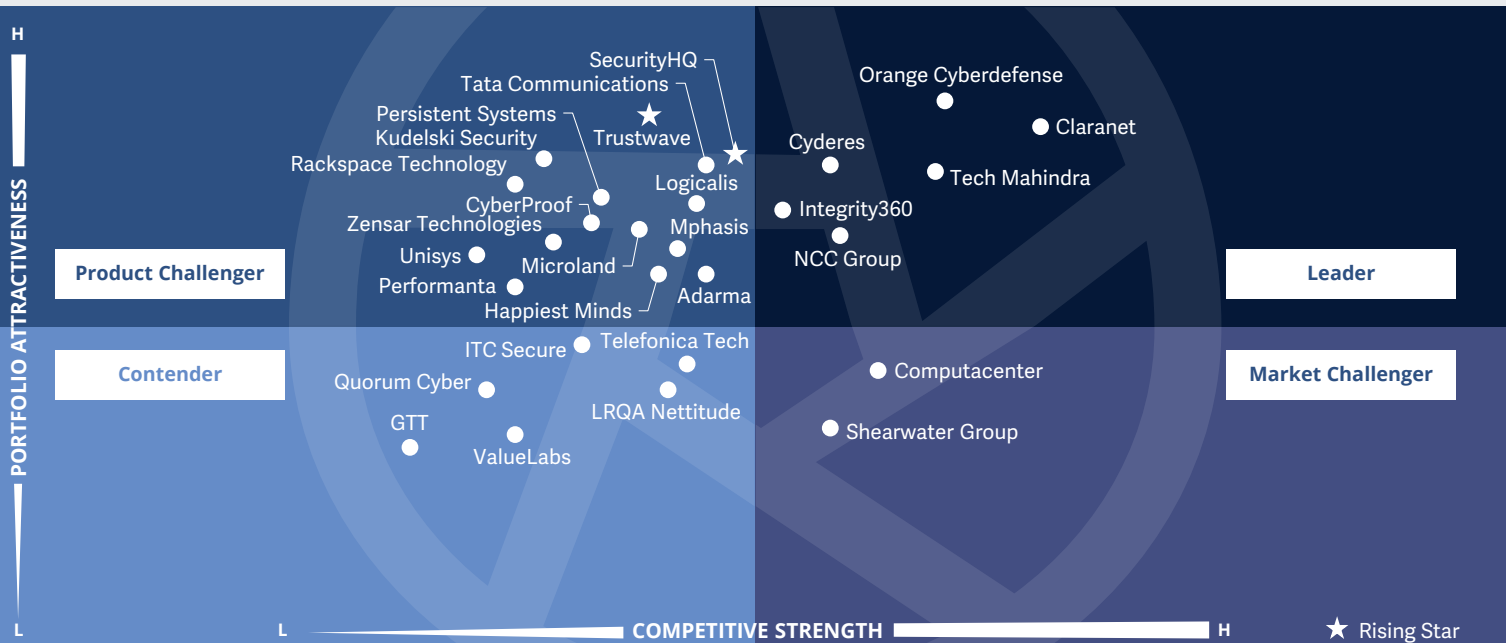


Technology professionals should read this report to gain insights into emerging trends, tailored security platforms and strategic objectives to stay apace with the evolving security landscape.



Cybersecurity – Solutions and Services
Managed Security Services - SOC (Midmarket)

U.K. 2024



This quadrant evaluates providers that excel in offering **cost-effective security solutions** and **scalable service models** that align with the budget realities of mid-sized businesses, providing **faster detection and response** and **greater operational efficiency**.

Bhuvaneshwari Mohan



Managed Security Services – SOC (Midmarket)

Definition

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

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional managed security services with innovation to fortify clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies and infrastructure. They

must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, Security Information and Event Management (SIEM) services**, security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. **Manage own SOCs**
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models



Managed Security Services – SOC (Midmarket)

Observations

The need for managed detection and response services is constantly increasing among enterprises. MSS providers are extensively partnering with MDR and XDR platform providers to accommodate their clients' business requirements and security priorities.

Midmarket clients require a proactive approach to cybersecurity, enabling them to respond promptly to threat intelligence and industry-specific information they receive. MSS providers focus on tailoring their clients' threat intelligence and threat hunting services. ISG observes that there is also increased focus on these specialized services and tailored recommendations.

Providers are also implementing measures to guarantee that clients' data adheres to regional data residency and protection regulations, ensuring compliance while using the appropriate technology stack such as data localization, encryption and protection tools, network segmentation and access controls and talent.

MSS providers are integrating their MDR offering to include digital forensics and incident response services to become the trusted partners for their clients throughout the incident lifecycle.

Most providers focus on expanding their comprehensive suite of services across Microsoft's security portfolio. There is an increased need from customers to help optimize their security posture and configurations, maximizing the value of the security toolsets available within their Microsoft licensing investments.

From the 89 companies assessed for this study, 29 qualified for this quadrant, with six being Leaders and two Rising Stars.

claranet

Claranet's cloud and security expertise, proactive approach, global support capabilities, proven track record and focus on delivering tangible business benefits through its MDR and MSS SOC services set it apart in the market.

Cyderes

Cyderes provides a cohesive approach to help enterprises safeguard from cloud security risks with comprehensive threat detection, investigation and workflow, rich reporting for compliance use cases and improvement of their overall security risk posture.

Integrity360

Integrity360, with its continuous investments in SOC facilities in and around the UK, has a comprehensive set of security services, including MDR, ensuring robust security outcomes with security monitoring across on-premises and cloud environments, ensuring compliance mandates.

NCC Group

NCC Group offers tailored security monitoring services with customized detections and enhanced automation to match the risk tolerance of enterprises, ensuring clear visibility into threats across data, OT/IoT, multicloud and DevOps environments.

Cyberdefense

Orange Cyberdefense's Cyber SOC delivers comprehensive MDR services that offer advanced threat intelligence and incident response and with a dedicated incident response team and a large pool of 3,000 seasoned security experts, including 140 Microsoft-certified experts.

TECH **mahindra**

Tech Mahindra's MSS services, powered by cloud-native security platform and next-gen SOC solution, provide continuous real-time threat detection and response using a wide array of pre-built SIEM use cases, which are vendor-agnostic, speeding up client onboarding.



Managed Security Services – SOC (Midmarket)


SecurityHQ

SecurityHQ (Rising Star) provides complete visibility into client's security environment with 24/7 continuous security monitoring, detection and response powered by AI and security analytics, ensuring compliance and risk reduction with flexible client options.

Trustwave

Trustwave (Rising Star) powered by its robust threat intelligence, provides customized use cases for unique business needs and ongoing SIEM optimization, accelerating time-to-value and timely threat detection through proven methodologies.





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.



Appendix

Methodology & Team

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