ISG Provider Lens®

Cybersecurity – Services and Solutions

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

Customized report courtesy of:

SCC

QUADRANT REPORT | JUNE 2026 | UK

Table of Contents

Executive Summary

Report Author: Bhuvaneshwari Mohan

Cybersecurity is moving beyond compliance to measurable enterprise resilience outcomes

This ISG Provider Lens® study evaluates cybersecurity service providers supporting organisations across strategic security services, technical security services and next-gen SOC/MDR services in the UK. The assessment covers both large enterprise and midmarket segments, focusing on how providers enable organisations to strengthen resilience, align with regulatory requirements and secure increasingly complex, hybrid digital environments.

Market Context

In 2026, UK enterprises are transitioning from a compliance-driven cybersecurity stance towards an operationally integrated resilience model. Cybersecurity has moved from a perimeter control function to a core element of business continuity, governance and enterprise risk management. ISG analysis finds that UK organisations are embedding security into every aspect of operations, responding to escalating AI-enabled threats, heightened regulatory expectations and the need to protect digital trust across supply chains.

The four forces driving this shift are:

- **AI-driven and state-sponsored threats:** The proliferation of GenAI and advanced attack automation has expanded the threat surface, forcing enterprises to prioritise continuous detection and adaptive defence.
- **Board and investor pressure for resilience metrics:** Cybersecurity has become a board-level accountability measure, driving demand for quantifiable risk reporting and readiness scoring.
- **Customer and supply chain trust:** Organisations now view cyber maturity as integral to brand integrity and contractual assurance, especially in regulated industries.

Cybersecurity is now measured by **resilience outcomes**, not **standalone control** deployment.

- **Regulatory evolution towards ongoing compliance:** Frameworks such as DORA, NIS2 and UK sectoral mandates are shifting from static audits to dynamic, real-time assurance models.

The UK government and National Cyber Security Centre (NCSC) analysis underscore the scale and strategic importance of this shift. The Cyber Security Sectoral Analysis 2025 values the sector at over £13.2 billion in revenue in 2025 with more than 67,000 professionals, reflecting sustained growth and increasing economic significance. The NCSC highlights that cyber risk is no longer a technical issue but a board-level priority, with organisations required to ensure operational continuity and resilience to address escalating threats.

The findings also point to a predominantly service-led market structure and increasing consolidation, alongside rising dependence on managed security services. Combined with heightened exposure across supply chains, critical national infrastructure and AI-enabled attack surfaces, the market is shifting towards outcome-driven security models where continuous assurance, resilience engineering and real-time response become core requirements.

Supply chain risk is becoming a primary concern, with organisations required to demonstrate visibility, control and assurance across third-party and ecosystem dependencies. Convergence of IT and operational technology is further increasing exposure in critical infrastructure environments, requiring security models that account for both digital and physical system dependencies.

Parallel demand is rising across strategic advisory, engineering-led implementation and continuous monitoring and response, requiring organisations to operate these domains as a coordinated capability rather than standalone functions, despite increasing regulatory pressure and persistent talent constraints.

Enterprise Priorities

Enterprise priorities reflect a shift from compliance-driven execution to operational discipline, where cybersecurity is embedded into risk decision-making, business continuity and measurable outcomes.

- Large enterprises show high baseline maturity, maintaining formal cyber continuity plans and providing staff cyber training. However, ISG observes signs of plateauing progress due to the complexity of governance models and the diffusion of cyber accountability across functions.
- SMBs, in contrast, are showing sharper maturity gains. They are operating continuity plans and benefit from increased government-backed cybersecurity programs and greater reliance on managed service providers for enablement.

The result is a dual-speed market: large enterprises optimise for integration and automation, while SMBs accelerate through outsourced resilience partnerships.

In 2026, enterprise buyers are pivoting towards interoperability, transparency and real-time resilience metrics as top selection criteria.

Key buyer expectations now include:

- API - driven open architectures supporting multi-vendor ecosystems
- Transparent AI decisioning and explainability aligned with the UK's 2025 AI Cybersecurity Code of Practice
- Continuous validation and audit readiness, including automated evidence trails for insurance and regulatory audits
- Outcome-based contracts, measured by dwell time reduction, MTTR and resilience KPIs rather than static SLAs

Across the cybersecurity lifecycle, organisations are prioritising clearer risk ownership, stronger architectural alignment and improved response readiness, reflecting a shift from control deployment to demonstrable resilience outcomes.

Enterprises are also moving away from undifferentiated control expansion towards control effectiveness, focusing on risks that materially impact operations, including service disruption, third-party exposure and identity-related vulnerabilities. This shift is driving the increased adoption of attack path analysis, scenario-based testing and risk-aligned decision frameworks to demonstrate how investments reduce real-world exposure.

Tool consolidation is becoming a priority, with organisations reducing overlapping security solutions and standardising platforms to improve visibility, reduce operational overhead and strengthen control consistency across environments.

Execution of cybersecurity programmes is increasingly constrained by legacy complexity, fragmented ownership and competing enterprise priorities, slowing the pace of transformation despite clear strategic intent.

Cost efficiency remains significant but is no longer the dominant factor. Providers that can prove operational impact, along with delivering technical coverage, are outperforming competitors in client evaluations.

Provider Dynamics

The shifts in enterprise demand are shaping how providers structure, deliver and differentiate their cybersecurity services, with a clear move towards integrated, outcome-driven models. Differentiation is increasingly based on measurable resilience aligned to regulatory and business priorities rather than standalone technical depth.

Key provider responses that coalesce around several consistent patterns include:

- **AI-enabled operations:** Investment in automation, AI-assisted detection and response and orchestration frameworks, driven by the need to improve response speed, reduce analyst workload and scale operations amid persistent talent shortages.
- **Platform integration:** Development of unified platforms combining threat intelligence, analytics and cross-domain visibility, enable the consolidation of fragmented security stacks and improve end-to-end visibility across complex environments.
- **Sovereign delivery:** Expansion of UK-based SOCs and data residency-aligned operations reflect the regulatory expectations around data control, jurisdiction and in-country accountability, particularly in regulated sectors.
- **Co-managed models:** Blending provider capabilities with internal teams through shared visibility and workflows allow enterprises to retain governance control while augmenting operational scale and specialist expertise.

The expansion of native security capabilities within hyperscaler platforms is increasing pressure on providers to differentiate through orchestration, cross-platform integration and domain expertise rather than tool access alone.

Providers are expanding resilience-led advisory and risk quantification while strengthening engineering-led implementation through platform consolidation and multi-domain security integration. In parallel, operating models are evolving towards AI-driven, co-managed and platform-led security operations that enable continuous monitoring, faster response and improved detection accuracy.

Security operations are increasingly assessed based on decision quality and response effectiveness rather than alert volume, reflecting a shift from activity-driven monitoring to outcome-driven operations.

The persistent UK talent shortage spanning technical, regulatory and governance skills continues to constrain market growth.

This is driving changes in provider delivery models, including:

- Investment in UK-based SOCs, ensuring compliance with data sovereignty and defence-grade security mandates.
- Partnerships with NCSC, universities and apprenticeship programs to cultivate AI-driven cybersecurity expertise.
- AI-assisted operations (AIOps and SecOps) to augment human analysts and accelerate threat detection.

Explainable AI and assurance testing frameworks are rapidly maturing from differentiators into de facto standards. Human oversight, traceable AI model governance and continuous validation are now embedded expectations across leading SOC/managed detection and response (MDR) environments.

Outlook

The three defining developments that ISG forsees in the UK cybersecurity market over the next 18-24 months include:

Market consolidation: Rising demand for unified platforms will accelerate consolidation among managed security providers and security integrators. Niche specialists will sustain relevance in regulated verticals by leveraging deep local expertise and compliance credibility.

AI regulation and cross-border data governance: The intersection of UK AI assurance frameworks with EU operational resilience and privacy laws will make explainable AI and sovereign data operations key differentiators in sourcing decisions.

Regulated resilience metrics: The move towards mandated resilience reporting, including continuous assurance dashboards and readiness scores, will formalise cyber resilience as a regulated business function.

In parallel, emerging priorities such as post-quantum cryptography readiness and resilience engineering will gain traction, as organisations prepare for long-term cryptographic risk and increasingly complex, interconnected digital environments.

Across the market, advisory, implementation and operations are converging into unified, platform-led security models, where continuous validation and resilience-by-design become core operating principles.

Resilience is increasingly defined in operational terms, including response coordination, recovery assurance and continuity of critical business operations, rather than prevention metrics alone.

Strategic Implications

For enterprises: Security must operate as a measurable business discipline. Organisations should operationalise resilience KPIs, automate assurance evidence and treat AI transparency as a core governance requirement.

For providers: Competitive advantage will hinge on combining platform integration with sovereign operations. Providers must demonstrate auditable AI governance and risk quantification aligned to sectoral mandates.

For the ecosystem: Collaboration across government, academia and the private sector will be vital to scale talent and sustain innovation in AI-enabled resilience.

By 2027, the UK cybersecurity market will be defined by AI-augmented, continuously validated and sovereignty-aware resilience platforms. Providers that can demonstrate trust, transparency and tangible risk reduction will be best positioned in an increasingly regulated, AI-driven landscape.

ISG Provider Lens Methodology Updates

Important updates from this year's study are as follows:

- ISG has refined its evaluation criteria for the IPL Cybersecurity – Services and Solutions 2026 study to provide a more granular view of provider maturity and competitiveness. The updated methodology places stronger emphasis on the quantity and quality of client case studies submitted by service providers to better assess real-world delivery capability and execution maturity. As a result, these recalibrated criteria and weightings have influenced provider positioning in the quadrant grids, including movement for some providers and exclusion where evidence did not meet the updated thresholds.
- In the Next-Gen SOC/MDR Services quadrant, this year's assessment places greater emphasis on AI-enabled automation, co-managed delivery maturity, SOC sovereignty and threat intelligence integration. Eligibility criteria have also been tightened to ensure providers demonstrate credible UK delivery capability and measurable MDR outcomes, with inclusion in the midmarket segment requiring clear alignment to UK midmarket service models and customer traction.
- This report assesses independent security service providers that offer advisory, integration and managed security services on a vendor-agnostic basis. While platform vendors continue to shape enterprise security technology decisions, their delivery models and engagement approaches differ from those of service providers. To maintain methodological consistency, the study focuses on providers whose core remit is the delivery of end-to-end cybersecurity services, regardless of underlying technologies.

UK enterprises are shifting from compliance validation to continuous assurance, requiring real-time visibility, audit-ready evidence and measurable resilience across hybrid environments.

Provider Positioning

Page 1 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Accenture	Leader	Not In	Leader	Not In	Leader	Not In
Atos	Product Challenger	Not In	Product Challenger	Not In	Leader	Not In
Bechtle	Not In	Contender	Not In	Product Challenger	Not In	Not In
Bridewell	Not In	Leader	Not In	Leader	Not In	Leader
BT Business	Market Challenger	Not In	Leader	Not In	Leader	Not In
Capgemini	Leader	Not In	Leader	Not In	Leader	Not In
Capita	Not In	Not In	Contender	Not In	Contender	Not In
CDW	Not In	Not In	Not In	Contender	Contender	Not In
CGI	Contender	Not In	Contender	Not In	Contender	Not In
Claranet	Not In	Leader	Not In	Leader	Not In	Leader

Provider Positioning

Page 2 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Cognizant	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Computacenter	Contender	Not In	Leader	Not In	Market Challenger	Not In
CyberProof	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
Cyderes	Not In	Not In	Not In	Not In	Not In	Product Challenger
Deloitte	Leader	Not In	Leader	Not In	Leader	Not In
DXC Technology	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
EY	Leader	Not In	Leader	Not In	Leader	Not In
Fujitsu	Contender	Not In	Product Challenger	Not In	Market Challenger	Not In
Genpact	Not In	Not In	Contender	Not In	Not In	Not In
Getronics	Not In	Contender	Not In	Leader	Not In	Contender

Provider Positioning

Page 3 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Globant	Not In	Not In	Not In	Not In	Contender	Not In
HCLTech	Leader	Not In	Leader	Not In	Leader	Not In
Hitachi Digital Services	Not In	Leader	Not In	Leader	Not In	Leader
IBM	Leader	Not In	Leader	Not In	Leader	Not In
Infosys	Product Challenger	Not In	Rising Star ★	Not In	Product Challenger	Not In
Insight	Not In	Contender	Market Challenger	Market Challenger	Not In	Not In
Integrity360	Not In	Leader	Not In	Not In	Not In	Product Challenger
ITC Secure	Not In	Product Challenger	Not In	Not In	Not In	Contender
KPMG	Leader	Not In	Not In	Not In	Not In	Not In
Kroll	Not In	Leader	Not In	Not In	Not In	Leader

Provider Positioning

Page 4 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Kudelski Security	Not In	Product Challenger	Not In	Contender	Not In	Product Challenger
Kyndryl	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
LevelBlue	Not In	Rising Star ★	Not In	Product Challenger	Not In	Rising Star ★
Littlefish	Not In	Not In	Not In	Not In	Not In	Contender
Logicalis	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
LRQA Nettitude	Not In	Not In	Not In	Not In	Not In	Contender
LTM	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Microland	Not In	Leader	Not In	Leader	Not In	Leader
Mphasis	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
NCC Group	Market Challenger	Leader	Not In	Leader	Not In	Leader

Provider Positioning

Page 5 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
NTT DATA	Leader	Not In	Leader	Not In	Leader	Not In
Orange Cyberdefense	Product Challenger	Not In	Leader	Not In	Product Challenger	Leader
Performanta	Not In	Not In	Not In	Not In	Not In	Contender
Persistent Systems	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
PwC	Leader	Not In	Leader	Not In	Leader	Not In
Quorum Cyber	Not In	Contender	Not In	Not In	Not In	Contender
Rackspace Technology	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
SCC	Not In	Product Challenger	Not In	Rising Star ★	Not In	Leader
Secureworks (Sophos Group)	Contender	Not In	Not In	Not In	Not In	Not In
SecurityHQ	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger

Provider Positioning

Page 6 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Smarttech247	Not In	Not In	Not In	Not In	Not In	Product Challenger
Softcat PLC	Contender	Not In	Market Challenger	Market Challenger	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Product Challenger	Not In
Talion	Contender	Contender	Not In	Contender	Contender	Not In
Tata Communications	Not In	Not In	Not In	Not In	Not In	Product Challenger
TCS	Leader	Not In	Leader	Not In	Leader	Not In
Tech Mahindra	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Telefonica Tech	Not In	Market Challenger	Not In	Contender	Not In	Market Challenger
Telstra	Contender	Not In	Contender	Not In	Contender	Not In
Thales	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In

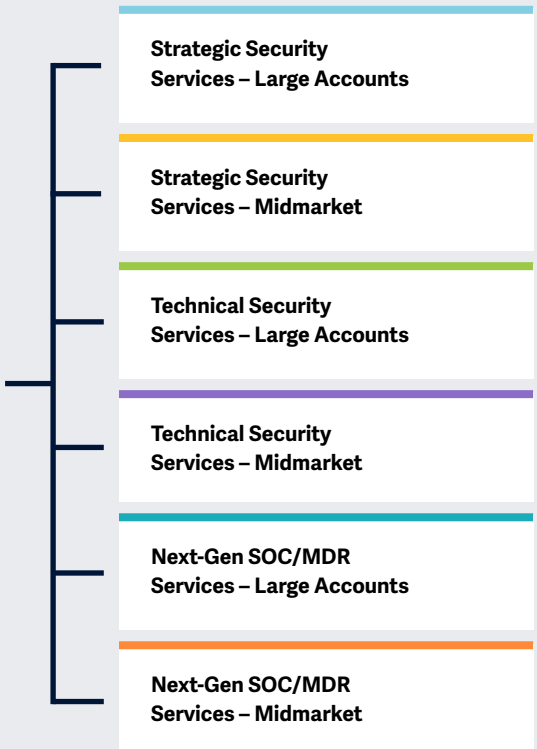
Provider Positioning

Page 7 of 7

	Strategic Security Services – Large Accounts	Strategic Security Services – Midmarket	Technical Security Services – Large Accounts	Technical Security Services – Midmarket	Next-Gen SOC/MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Unisys	Not In	Product Challenger	Not In	Contender	Not In	Product Challenger
Verizon Business	Product Challenger	Not In	Not In	Not In	Product Challenger	Not In
Vodafone	Not In	Not In	Not In	Not In	Not In	Market Challenger
Wavestone	Product Challenger	Not In	Not In	Not In	Not In	Not In
Wipro	Leader	Not In	Leader	Not In	Leader	Not In
WWT	Not In	Not In	Contender	Market Challenger	Not In	Not In
Zensar Technologies	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger

Key focus areas for **Cybersecurity — Services and Solutions 2026**.

Simplified Illustration Source: ISG 2026



Definition

In 2026, the cybersecurity landscape is expected to witness an increase in threat sophistication, expanding regulatory demands and a rapid shift towards intelligence-driven defence models. Enterprises across industries are under pressure to secure their increasingly distributed architectures, protect sensitive data across hybrid environments and respond to the surge in AI-enabled attacks. Meanwhile, boards and regulators seek demonstrable cyber resilience and verifiable control effectiveness, paving the way for security programs as part of digital transformation agendas.

In this light, the market is reorganising itself into clearly defined capability domains. While technical security services (TSS) ensure configuration integrity, secure implementations and continuous hardening, strategic security services (SSS) are gaining importance as executives prioritise cybersecurity with governance, risk and architectural alignment.

Next-generation SOCs and managed detection and response (MDR) services are also gaining traction, driven by the demand for 24/7 threat monitoring, AI-supported analysis and outcome-based response models. Additionally, risk-based vulnerability management reinforces preventive security by prioritising exposures using business context and attack path insights. Finally, post-quantum encryption consulting enters the market scope as organisations begin preparing cryptographic inventories and transition strategies to safeguard long-term data confidentiality.

This IPL study covers the mentioned capability domains, among others, and offers a comprehensive view how providers differentiate in an environment defined by speed, intelligence and resilience.

Scope of the Report

This ISG Provider Lens® quadrant report covers the following six quadrants for services/solutions: Strategic Security Services – Large Accounts, Strategic Security Services – Midmarket, Technical Security Services – Large Accounts, Technical Security Services – Midmarket, Next-Gen SOC/MDR Services – Large Accounts and Next-Gen SOC/MDR Services – Midmarket.

This ISG Provider Lens® study offers IT & Security decision-makers:

- Transparency on the strengths and weaknesses of relevant providers
- Differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on different markets, including Australia, Brazil, France, Germany, Switzerland, the UK, the US and the US public sector
- Country-specific characteristics: Postquantum encryption consulting in Germany and the U.S., XDR and risk-based vulnerability management analysis in Brazil and DLP analysis in Germany

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

Provider Classifications

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

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

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

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

Provider Classifications: Quadrant Key

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

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

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

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

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

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

Strategic Security Services – Large Accounts

Who Should Read This Section

This report is valuable for service providers offering **strategic security services (SSS**) in the **UK** to understand their market position and for large enterprises looking to evaluate these providers. Strategic security services, including frameworks, assessments, architecture consulting, and governance, are vital in developing cohesive cybersecurity strategies.

Cybersecurity professionals

Cybersecurity professionals should read this report to better manage evolving risks, strengthen threat detection capabilities, and understand how providers address advanced threats using emerging technologies such as AI. The insights help align cybersecurity strategies with broader business objectives while staying current on key security and risk management trends.

Technology professionals

Technology professionals should read this report to identify security partners that embed protection into digital initiatives. The analysis highlights how providers leverage AI, automation, and tailored security services to counter advanced threats, integrate security across complex environments, and support secure innovation within largescale digital transformation programs.

Strategy professionals, CFOs, and CEOs

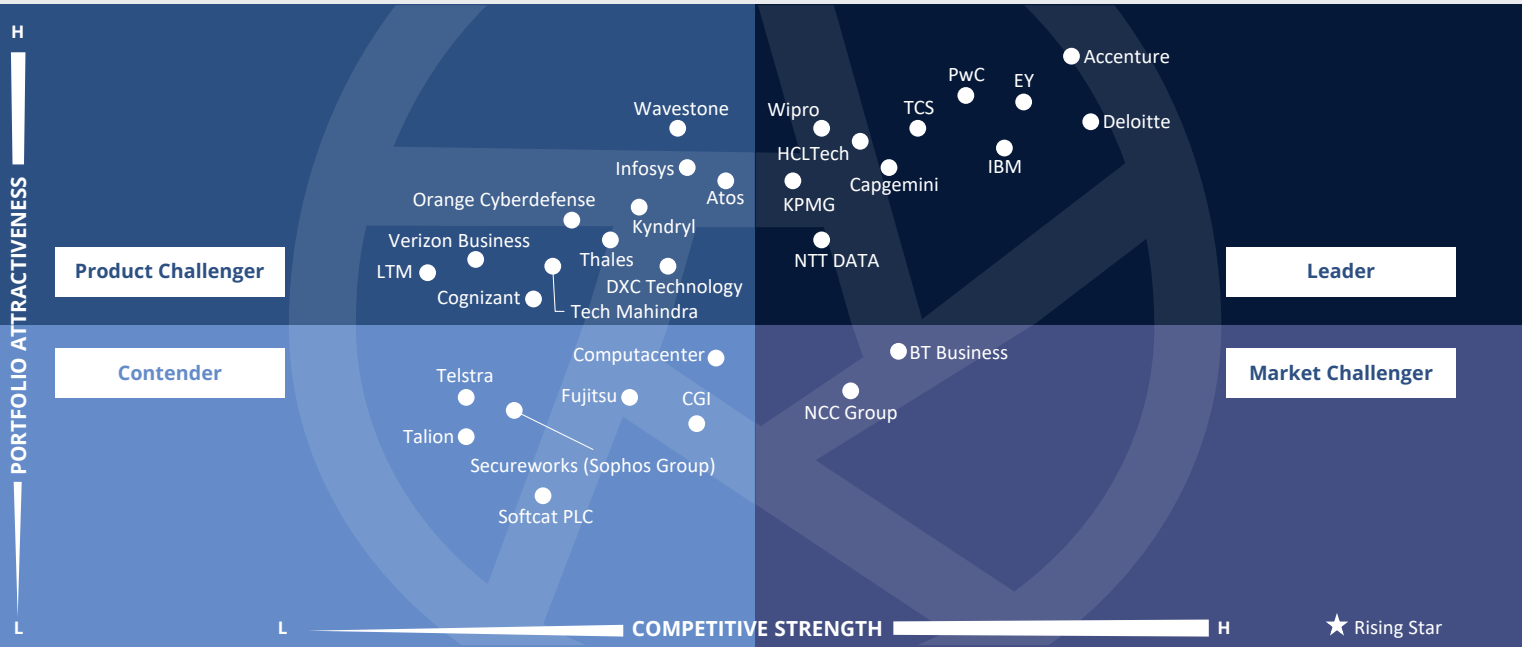
Strategy professionals should read this report to assess providers' partnership capabilities, scalability, and potential for cost optimization. CFOs and CEOs can use the insights to evaluate costeffective security solutions, strengthen enterprise cybersecurity posture, and ensure investments align with longterm business resilience and strategic priorities.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Strategic Security Services – Large Accounts

U.K. 2026



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

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that deliver consulting-led cybersecurity services focusing on strategy, governance, risk management and organizational transformation for IT and OT environments. These providers assess security maturity, quantify risks, define target operating models and develop cybersecurity strategies, policies and roadmaps aligned with business objectives and regulatory requirements. Their offerings include audits, assessments, security awareness programs, business continuity planning, tabletop exercises and advisory on technology selection. These providers also employ experienced consultants who guide enterprises through program design, governance improvements and capability development, including virtual Chief Information Security Officer (vCISO) models for ongoing or on-demand strategic leadership. Unlike TSS, which emphasize hands-on integration and engineering, SSS providers focus on advisory outcomes rather than operational monitoring or proprietary product execution.

Eligibility Criteria

1. Provide **vendor-agnostic security consulting** covering maturity assessments, strategy development, policy design, governance models and roadmap creation
2. Demonstrate capabilities in strategic domains such as risk quantification, regulatory readiness, vendor selection, business continuity planning and broader cyber risk advisory
3. **Apply recognized frameworks** and comply with standards (such as ISO 27000, NIST CSF, CIS Controls) when guiding enterprise programs
4. **Deliver at least one of the above** strategic security service within the target region through **qualified and certified** consultants
5. Present **documented evidence of engagements** that improved clients' security posture, governance structures, compliance readiness or risk-based decision-making
6. Provide **structured consulting methodologies**, templates or playbooks for assessments, strategic planning or organizational transformation
7. Operate as **consulting-led service providers** rather than product vendors, while allowing proprietary frameworks or tools that support advisory delivery
8. **Do not** focus exclusively on proprietary products

Observations

In 2026, the UK large enterprise Strategic Security Services (SSS) segment is shaped by rising board scrutiny, regulatory convergence and the complexity in operating across global digital environments. Expectations from UK regulators and authorities including, PRA, FCA and NCSC are reinforcing cybersecurity as a core component of enterprise risk, with increasing focus on continuous assurance rather than periodic compliance.

A clear shift is underway from compliance-led advisory to risk-driven programme design. Providers are supporting organisations in recalibrating risk models across interconnected business units and supply chains, aligning investment decisions with frameworks such as DORA and NIS2. Engagements increasingly emphasise continuous risk visibility, quantification and defensible governance.

Operating model transformation remains a central challenge, particularly in financial services and critical national infrastructure. Movement towards federated security structures is driving demand for providers that can define accountability, funding models and assurance processes across regions while maintaining consistency with UK regulatory expectations.

Providers are also playing a larger role in shaping multi-year transformation programmes. Cloud adoption, platform consolidation and resilience initiatives are being executed in parallel, requiring structured prioritisation, architectural alignment and governance discipline. AI governance and model risk are emerging as new advisory domains, alongside early-stage demand for post-quantum readiness and crypto-agility assessments.

Enterprise resilience is evolving into a measurable capability, with incident response, crisis management and recovery planning integrated into unified, regulator-aligned operating models.

In this environment, differentiation is driven by regulatory depth, ability to operationalise resilience and strength in emerging domains such as AI governance and continuous assurance.

From the 67 companies assessed for this study, 31 qualified for this quadrant, with 11 being Leaders.

accenture

Accenture's strategic security services integrate transformation, resilience and AI-driven advisory, enabling organisations to align cybersecurity with large-scale digital initiatives and enterprise risk priorities.

Capgemini

Capgemini delivers sovereignty-aligned cyber strategy through structured frameworks and regulatory expertise, supporting organisations in embedding resilience and compliance into enterprise security transformation.

Deloitte.

Deloitte's strategic security services focus on risk-led cyber advisory, integrating governance, compliance and resilience to help organisations align cybersecurity with enterprise risk and regulatory requirements.

EY

EY delivers transformation-aligned cyber strategy, combining risk, compliance and business integration to help organisations embed cybersecurity into enterprise change and resilience programmes.

HCLTech

HCLTech's strategic security services emphasise resilience-led cyber strategy supported by AI-driven frameworks and integration with large-scale enterprise transformation programmes.

IBM

IBM's strategic security services combine consulting, threat intelligence and platform-driven insights to help organisations design cyber strategies aligned to risk, resilience and digital transformation.

KPMG delivers governance-focused cyber strategy, integrating risk, compliance and audit expertise to support organisations in strengthening security posture and regulatory alignment.

NTT DATA provides resilience-led cyber strategy supported by platform-driven insights and global delivery, enabling organisations to align security with risk, compliance and transformation objectives.

PwC's strategic security services focus on business-aligned cyber strategy, integrating risk, resilience and governance to support enterprise-wide transformation and value-driven security outcomes.

TCS delivers resilience-led cyber strategy integrated with large-scale transformation, enabling organisations to align security with evolving risk, regulatory and digital priorities.

Wipro's strategic security services combine consulting depth, resilience frameworks and emerging technology focus to support enterprise-wide cyber transformation and risk management.

Strategic Security Services – Midmarket

Who Should Read This Section

This report is valuable for service providers offering **strategic security services (SSS)** in the **UK** to understand their market position and for midmarket enterprises looking to evaluate these providers. In this quadrant, ISG highlights the value of these services for midmarket enterprises, focusing on risk management, business continuity and proactive strategies. The report emphasises aligning security with business goals and integrating governance, compliance and risk assessments.

Cybersecurity professionals

Cybersecurity professionals should read this report to better manage evolving risks, strengthen threat detection capabilities, and understand how providers address advanced threats using emerging technologies such as AI. The insights help align cybersecurity strategies with broader business objectives while staying current on key security and risk management trends.

Technology professionals

Technology professionals should read this report to identify security partners that embed protection into digital initiatives. The analysis highlights how providers leverage AI, automation, and tailored security services to counter advanced threats, integrate security across complex environments, and support secure innovation within largescale digital transformation programs.

Strategy professionals, CFOs, and CEOs

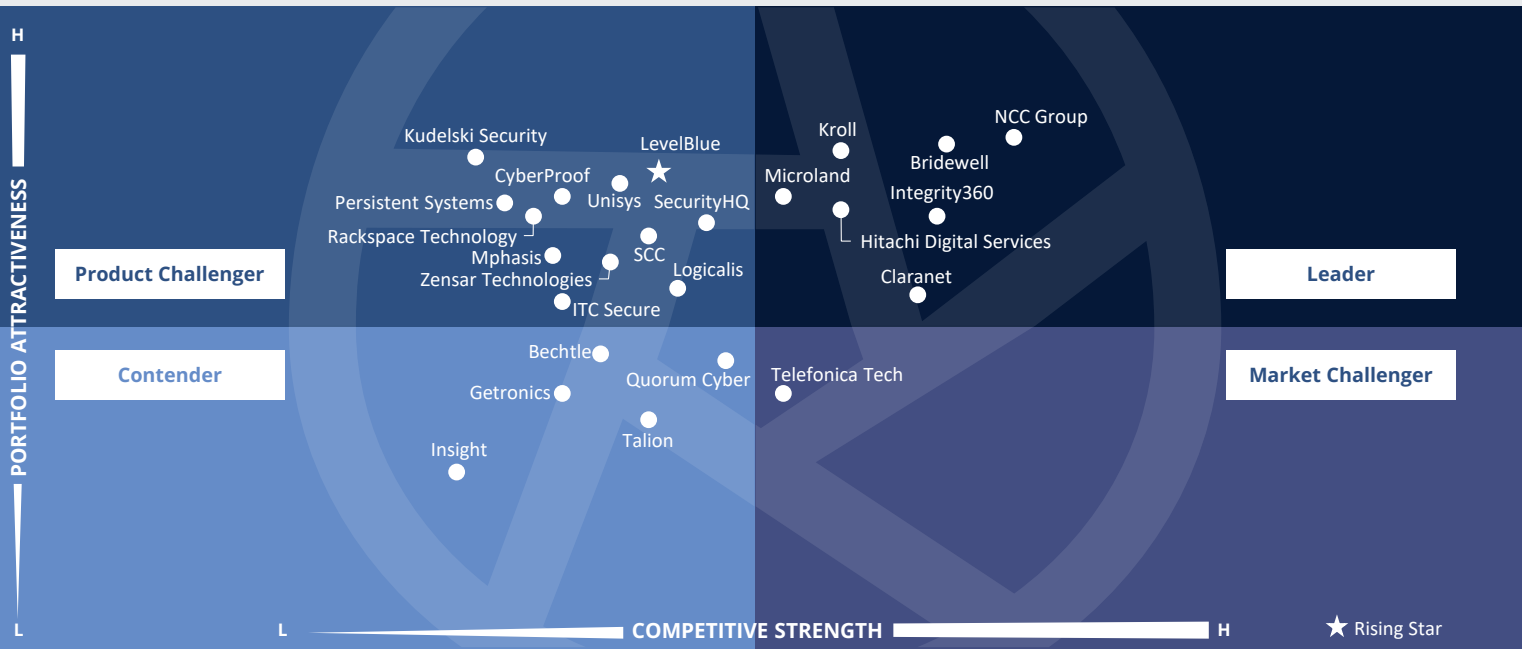
Strategy professionals should read this report to assess providers' partnership capabilities, scalability, and potential for cost optimization. CFOs and CEOs can use the insights to evaluate costeffective security solutions, strengthen enterprise cybersecurity posture, and ensure investments align with longterm business resilience and strategic priorities.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Strategic Security Services – Midmarket

U.K. 2026



This quadrant focusses on providers that offer **predefined security road maps, vCISO capabilities** and **scalable advisory models** to help **midmarket firms** align with **industry best practices** and **prioritise risk management**.

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that deliver consulting-led cybersecurity services focusing on strategy, governance, risk management and organizational transformation for IT and OT environments. These providers assess security maturity, quantify risks, define target operating models and develop cybersecurity strategies, policies and roadmaps aligned with business objectives and regulatory requirements. Their offerings include audits, assessments, security awareness programs, business continuity planning, tabletop exercises and advisory on technology selection. These providers also employ experienced consultants who guide enterprises through program design, governance improvements and capability development, including virtual Chief Information Security Officer (vCISO) models for ongoing or on-demand strategic leadership. Unlike TSS, which emphasize hands-on integration and engineering, SSS providers focus on advisory outcomes rather than operational monitoring or proprietary product execution.

Eligibility Criteria

1. Provide **vendor-agnostic security consulting** covering maturity assessments, strategy development, policy design, governance models and roadmap creation
2. Demonstrate capabilities in strategic domains such as risk quantification, regulatory readiness, vendor selection, business continuity planning and broader cyber risk advisory
3. **Apply recognized frameworks** and comply with standards (such as ISO 27000, NIST CSF, CIS Controls) when guiding enterprise programs
4. **Deliver at least one of the above** strategic security service within the target region through **qualified and certified** consultants
5. Present **documented evidence of engagements** that improved clients' security posture, governance structures, compliance readiness or risk-based decision-making
6. Provide **structured consulting methodologies,** templates or playbooks for assessments, strategic planning or organizational transformation
7. Operate as **consulting-led service providers** rather than product vendors, while allowing proprietary frameworks or tools that support advisory delivery
8. **Do not** focus exclusively on proprietary products

Observations

In 2026, the UK midmarket Strategic Security Services (SSS) segment is shaped by increasing executive accountability for cyber risk, expanding regulatory expectations and continued constraints on in-house security leadership capacity. UK-specific requirements, including NCSC guidance, Cyber Essentials and insurance-driven controls, are pushing organisations to formalise governance while relying more heavily on external advisory support.

A clear shift is visible from compliance-led assessments to more practical, decision-oriented advisory. Providers are expected to translate cyber risk into business and operational terms, supporting leadership teams in prioritising investments under budget and resource constraints. Generic maturity assessments are giving way to more contextual, outcome-focused engagements.

Providers are differentiating through structured and repeatable advisory models suited to mid-market operating realities. Virtual CISO services, cyber investment roadmaps and resilience planning are increasingly delivered as ongoing engagements, often alongside managed services, enabling organisations to adapt to evolving risk, regulatory scrutiny and technology change.

AI is emerging primarily in governance and risk advisory. Providers are supporting organisations in assessing AI-related exposure, defining governance principles and aligning adoption with UK expectations around security, privacy and accountability, while supporting human-led decision-making.

Governance clarity and resilience ownership are becoming more prominent. Providers are supporting definition of decision rights, escalation paths and accountability structures, alongside scenario planning and tabletop exercises to improve preparedness.

In this segment, differentiation is driven by the ability to deliver practical, scalable advisory that aligns with UK regulatory expectations while remaining simple to adopt and operate within mid-market constraints.

From the 67 companies assessed for this study, 25 qualified for this quadrant, with seven being Leaders and one Rising Star.

Bridewell

Bridewell focuses on cybersecurity advisory, resilience and regulatory alignment, supporting UK public sector and critical infrastructure organisations with governance-led risk management and transformation.

claranet

Claranet helps organisations align cybersecurity with cloud and digital transformation, combining advisory and architecture capabilities to support secure adoption of hybrid and multi-cloud environments.

Hitachi Digital Services

Hitachi Digital Services combines cyber advisory, risk management and resilience planning across IT and OT environments, supporting enterprises and industrial organisations in complex transformation programs.

Integrity360

Integrity360 provides cybersecurity advisory and governance capabilities focused on risk management and compliance, supporting organisations across the UK and Europe in strengthening their security posture.

MICROLAND®

Microland takes a risk-led, outcome-driven approach to cybersecurity, focusing on resilience, AI governance and identity-centric strategies aligned to business priorities.

NCC Group

NCC Group combines cyber assurance, risk advisory and threat intelligence to help organisations assess, prioritise and manage cyber risk across regulated and complex environments.

Kroll

Kroll brings together cyber risk advisory, incident preparedness and digital risk management to support organisations in aligning security with business, legal and regulatory requirements.

LevelBlue

LevelBlue (Rising Star) integrates advisory, risk management and transformation capabilities to help organisations align cybersecurity with enterprise operations across network, cloud and digital environments.

Technical Security Services – Large Accounts

Who Should Read This Section

This report is valuable for service providers offering **technical security services (TSS)** in the **UK** to understand their market position and for large enterprises looking to evaluate these providers. It provides a deeper analysis based on their expertise in technologies such as IAM, OT, cloud security, SASE, and XDR and their ability to manage large and complex security transformations.

Technology professionals

Technology professionals should read this report to understand how security service providers address compliance, market evolution, and integration challenges. The insights help evaluate provider capabilities in adopting advanced, vendorneutral technologies that support innovation, improve scalability, and strengthen threat mitigation across complex enterprise environments.

Security and data professionals

Security and data professionals should read this report to gain practical insights into compliance requirements, risk management approaches, and modern threat detection capabilities. The analysis helps align cybersecurity strategies with business objectives while assessing providers' ability to deliver scalable, costeffective, and integrated security solutions.

Business professionals

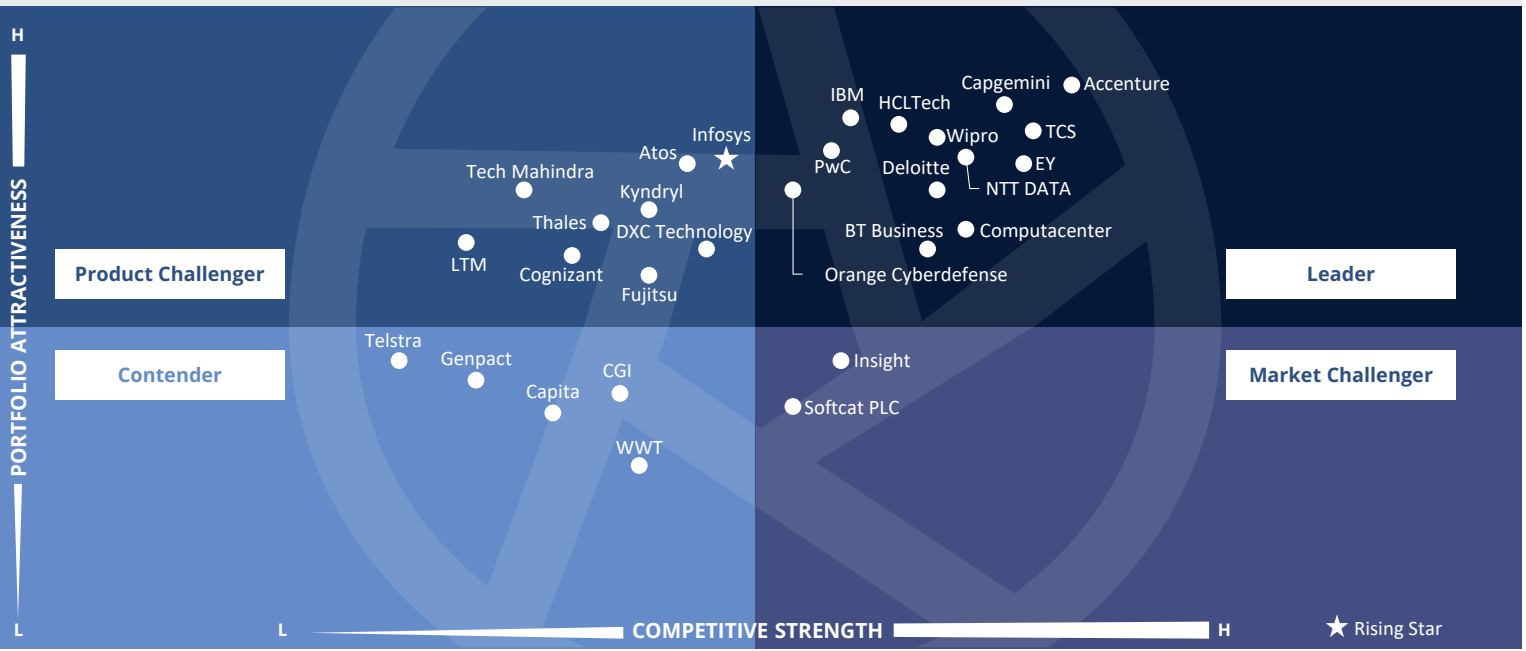
Business professionals should read this report to better navigate the balance between data security, customer experience, and privacy expectations. The findings support informed decision making during digital transformation initiatives, helping organizations manage risk, maintain trust, and select providers that align security investments with business priorities.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services – Large Accounts

U.K. 2026



This quadrant assesses providers offering **scalable, expert-driven technical implementation** and **customised security integration** for **complex enterprise environments**, focusing on **compliance, platform resilience** and **cloud-native architecture alignment**.

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that design, integrate, implement and modernise IT and OT security technologies across multi-vendor environments. Their services include deploying and configuring security controls for identity and access management, cloud and data centres, SASE/SSE, endpoints, networks, OT and industrial control systems (ICS), and related domains. Providers use reference architectures, automation frameworks and proprietary accelerators to deliver engineering-led transformations that streamline implementation and enhance control effectiveness. They maintain strong partnerships with security vendors, hold specialised certifications and support lifecycle tasks such as hardening, tuning, patching and device management. Unlike SSS, which focus on advisory and governance, technical security service (TSS) providers emphasise hands-on technical execution. They do not offer SOC-based monitoring or MDR operations, but may provide traditional managed security services.

Eligibility Criteria

1. Demonstrate experience in **designing, integrating and implementing** IT and/or OT security technologies, supported by multi-vendor certifications and OEM partnerships
2. Deploy **accelerators, proprietary toolsets or reference architectures** that enhance implementation quality, interoperability and time-to-value
3. Employ **certified engineers and architects** adept at configuring, customising, and optimising security solutions across cloud, networks, endpoints and OT environments
4. Show a **structured, methodology-driven approach** for evaluating, selecting and integrating security technologies that align with client requirements, risk profiles and architectural constraints
5. Deliver **lifecycle engineering services** such as configuration management, policy tuning, patching, control hardening and technology modernisation
6. Present documented **case studies** demonstrating successful security technology deployments or transformations within the target region
7. Operate as **service-led integrators** rather than standalone ISVs, permitting proprietary accelerators or internally developed tools that support service delivery
8. **Do not** focus exclusively on proprietary products

Observations

In 2026, the Technical Security Services (Large Accounts) quadrant is defined by large-scale architecture renewal as organisations stabilise accumulated technical debt while accelerating the adoption of cloud-native security foundations. Providers are selected not for basic integration, but for their ability to reengineer control frameworks across heterogeneous, global infrastructures without disrupting mission-critical operations.

Enterprises demand execution across multi-year, multi-domain transformation portfolios, including replatforming identity and access management (IAM) at scale, normalising fragmented network architectures, consolidating tooling from M&A cycles and embedding policy-as-code across multicloud environments. TSS engagements have evolved beyond isolated deployments towards full-stack modernisation, where identity, endpoint, network, data and cloud controls operate as a coordinated system.

A key differentiator is cross-domain observability engineering. Providers must design telemetry pipelines that correlate identity, endpoint, network and cloud signals, enabling real-time visibility into control drift and attack paths. This requires deep capability across SIEM/XDR engineering, cloud-native security, ITSM integration and orchestration frameworks.

Platform rationalisation remains central, with organisations reducing tool sprawl and standardising architectures to improve efficiency and reduce risk while aligning with the UK's regulatory expectations. There is increasing emphasis on continuous validation of control effectiveness, with engineering approaches evolving towards ongoing assurance and resilience rather than point-in-time deployment.

Execution complexity is heightened in sectors such as financial services and critical infrastructure, where uptime, regulatory scrutiny and IT and OT convergence introduce additional constraints. Success is defined by engineering depth, architectural discipline and the ability to deliver integrated, continuously effective security at scale.

From the 67 companies assessed for this study, 29 qualified for this quadrant, with 13 being Leaders and one Rising Star.

accenture

Accenture delivers technical cybersecurity services in the UK, focusing on engineering and implementation across cloud, identity, data and OT environments, supporting large-scale digital transformation and regulatory-driven security modernisation.

BT Business

BT Business's TSS combine deep telecommunications infrastructure expertise with applied cyber defence, particularly in critical national infrastructure. Its UK-based threat engineering and secure network architecture capabilities reinforce trust at scale.

Capgemini

Capgemini differentiates through industrialised security and sovereign architecture capabilities. Its structured implementation models and focus on regulated environments position it well for organisations prioritising standardisation, compliance and large-scale rollout across European operations.

Computacenter

Computacenter's technical edge lies in integrating security into infrastructure and workplace environments. Its strength in identity, endpoint and secure access, combined with deep OEM alignment, makes it a practical choice for enterprises securing and modernising existing IT estates.

Deloitte.

Deloitte's strength lies in bridging risk, compliance and technical implementation. Its ability to translate regulatory and governance requirements into executable security architectures makes it relevant for organisations navigating complex regulatory and assurance-driven environments.

EY

EY's technical security positioning is rooted in risk-led implementation and compliance alignment. Its strength in integrating security controls with regulatory, audit and transformation programmes supports enterprises prioritising governance, reporting and financial risk visibility.

HCLTech

HCLTech combines engineering scale with platform-led delivery to support security implementation across hybrid and cloud environments. Its strength lies in operationalising security within large IT estates, particularly for clients seeking cost-efficient, standardised deployment models.

IBM

IBM's technical edge is driven by platform-centric security engineering, anchored in its software ecosystem. Its ability to integrate security technologies with consulting and implementation capabilities positions it strongly for organisations adopting product-led security architectures.

NTT DATA

NTT DATA delivers technical security services through infrastructure and network-centric integration capabilities. Its strength lies in embedding security into connectivity, cloud and IT operations, supporting enterprises with distributed and telecom-heavy environments.

Cyberdefense

Orange Cyberdefense leverages its telecom heritage to deliver network-centric security implementation. Its strength lies in embedding security within connectivity and traffic visibility layers, supporting enterprises with distributed and network-dependent environments.

pwc

PwC's technical security services focus on operationalising risk and compliance frameworks within enterprise environments. Its strength lies in aligning implementation with regulatory expectations and business risk priorities, particularly in highly scrutinised sectors.

TCS TATA CONSULTANCY SERVICES

TCS differentiates through scale-driven delivery and platform-supported implementation across global IT estates. Its strength lies in executing security transformation programmes efficiently, particularly for large enterprises seeking standardised and repeatable deployment models.

wipro

Wipro combines engineering capabilities with platform-led accelerators to support security implementation across cloud and infrastructure environments. Its strength lies in integrating automation and delivery frameworks to drive consistency across large-scale engagements.

Infosys

Infosys (Rising Star) focuses on platform-led security implementation integrated with digital transformation initiatives. Its strength lies in delivering scalable, automation-driven security engineering across cloud and enterprise platforms.

Technical Security Services – Midmarket

Who Should Read This Section

This report is valuable for service providers offering **technical security services (TSS)** in the **UK** to understand their market position and for midmarket enterprises looking to evaluate these providers. The report provides actionable insights for enterprises aiming to enhance security posture while balancing cost and scalability. It highlights the need for modular services and adaptable frameworks tailored to organisational and industry-specific needs

Technology professionals

Technology professionals should read this report to understand how security service providers address compliance, market evolution, and integration challenges. The insights help evaluate provider capabilities in adopting advanced, vendor neutral technologies that support innovation, improve scalability, and strengthen threat mitigation across complex enterprise environments.

Security and data professionals

Security and data professionals should read this report to gain practical insights into compliance requirements, risk management approaches, and modern threat detection capabilities. The analysis helps align cybersecurity strategies with business objectives while assessing providers' ability to deliver scalable, costeffective, and integrated security solutions.

Business professionals

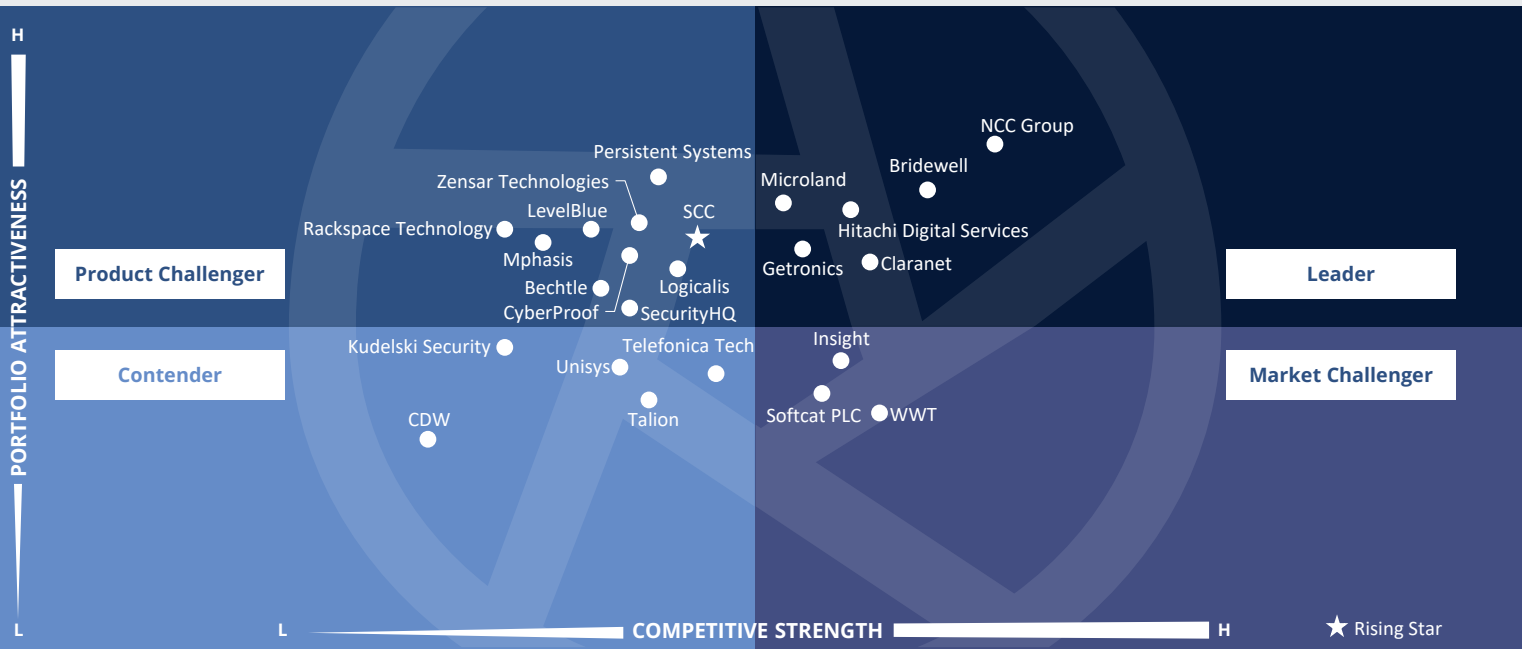
Business professionals should read this report to better navigate the balance between data security, customer experience, and privacy expectations. The findings support informed decision making during digital transformation initiatives, helping organizations manage risk, maintain trust, and select providers that align security investments with business priorities.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services – Midmarket

U.K. 2026



This quadrant evaluates providers offering **pre-integrated, scalable security solutions** that enable **rapid deployment, automation-led efficiencies** and **modular controls** designed for **lean teams** and **accelerated cyber maturity**.

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that design, integrate, implement and modernise IT and OT security technologies across multi-vendor environments. Their services include deploying and configuring security controls for identity and access management, cloud and data centres, SASE/SSE, endpoints, networks, OT and industrial control systems (ICS), and related domains. Providers use reference architectures, automation frameworks and proprietary accelerators to deliver engineering-led transformations that streamline implementation and enhance control effectiveness. They maintain strong partnerships with security vendors, hold specialised certifications and support lifecycle tasks such as hardening, tuning, patching and device management. Unlike SSS, which focus on advisory and governance, TSS providers emphasise hands-on technical execution. They do not offer SOC-based monitoring or MDR operations but may provide traditional managed security services.

Eligibility Criteria

1. Demonstrate experience in **designing, integrating and implementing** IT and/or OT security technologies, supported by multi-vendor certifications and OEM partnerships
2. Deploy **accelerators, proprietary toolsets or reference architectures** that enhance implementation quality, interoperability and time-to-value
3. Employ **certified engineers and architects** adept at configuring, customizing and optimizing security solutions across cloud, networks, endpoints and OT environments
4. Show a **structured, methodology-driven approach** for evaluating, selecting and integrating security technologies that align with client requirements, risk profiles and architectural constraints
5. Deliver **lifecycle engineering services** such as configuration management, policy tuning, patching, control hardening and technology modernisation
6. Present documented **case studies** demonstrating successful security technology deployments or transformations within the target region
7. Operate as **service-led integrators** rather than standalone ISVs, permitting proprietary accelerators or internally developed tools that support service delivery
8. **Do not** focus exclusively on proprietary products

Observations

In 2026, the Technical Security Services (midmarket) quadrant in the UK reflects a clear shift away from episodic, compliance-driven testing towards engineering-led, outcome-oriented assurance. Organisations are under pressure to demonstrate continuous control effectiveness, often with lean internal teams, increasing reliance on providers that can deliver repeatable validation and measurable risk reduction.

Buyers are placing greater emphasis on how technical testing supports sustained security improvement, regulatory confidence and operational decision-making. One-off assessments are being replaced by continuous validation models, with stronger demand for evidence that aligns with UK frameworks such as Cyber Essentials, the NCSC Cyber Assessment Framework and DSPT, as well as cross-border resilience requirements influenced by DORA, NIS2 and the UK NIS regime. Reporting quality has become a key differentiator, particularly where findings are translated into actionable remediation and audit-ready outputs.

Providers are differentiating through execution discipline and depth across cloud, identity and application security. There is growing adoption of approaches that establish configuration baselines, enable drift detection and support ongoing verification of control effectiveness, allowing organisations to maintain alignment with both internal policies and regulatory expectations.

Delivery models are evolving towards sustained optimisation rather than project-based implementation. Providers increasingly support periodic validation and continuous assurance alongside broader managed or co-managed services, reflecting the midmarket demand for practical, scalable security operations without full internal ownership.

In this quadrant, engineering quality, clarity of assurance outputs and the ability to deliver consistent, regulator-aligned validation within midmarket resource constraints are the major differentiators.

From the 67 companies assessed for this study, 24 qualified for this quadrant, with six being Leaders and one Rising Star.

Bridewell

Bridewell delivers TSS across consulting, assurance and testing, with a strong focus on regulatory alignment, cyber resilience and OT and IT security for UK-regulated and critical infrastructure sectors.

claranet

Claranet delivers TSS across consulting, implementation and assurance, integrating cloud, network and application security expertise to support midmarket organisations.

getronics

Getronics delivers TSS as part of its broader digital workplace and infrastructure portfolio, combining security consulting, implementation and compliance services for midmarket and enterprise clients.

Hitachi Digital Services

Hitachi Digital Services delivers TSS, combining cyber advisory, engineering and resilience capabilities across IT, OT and industrial environments, supporting complex enterprise and critical infrastructure clients.

MICROLAND®

Microland delivers TSS across advisory, engineering and risk-led transformation, focusing on outcome-driven security, AI governance and identity-centric architectures for midmarket and enterprise clients.

NCC Group

NCC Group delivers TSS across cyber assurance, testing and advisory, combining offensive security expertise, threat intelligence and risk-led consulting for regulated and enterprise clients.

SCC

SCC (Rising Star) delivers TSS across consulting, assurance and implementation, combining compliance-led advisory, security engineering and SecOps-aligned capabilities for midmarket and public sector organisations.

Rising Star

"SCC differentiates through its execution-focused TSS, combining compliance-led advisory with automation-driven implementation to deliver practical and operationally aligned security outcomes."

Bhuvaneshwari Mohan

SCC

Overview

SCC is headquartered in the UK and operates across Europe as part of SCC Digital. The company employs over 7,000 people globally and supports cybersecurity operations through a growing team of specialists and certified professionals. SCC's TSS are closely integrated with its broader security operations and IT capabilities, enabling a unified approach across consulting, implementation and operational security. Its UK presence is strengthened by deep engagement with public sector clients, including NHS and government organisations, and alignment with frameworks such as NCSC guidance and Cyber Essentials.

Strengths

Execution-led technical security delivery: SCC combines advisory with strong engineering and implementation capabilities across infrastructure, cloud and endpoint security. Its services span deployment and integration of security platforms within hybrid environments, ensuring alignment between architecture design and operational controls.

Compliance and public sector alignment: SCC demonstrates strong expertise in UK regulatory frameworks, including NCSC guidance and Cyber Essentials, with deep penetration across public sector, healthcare and government clients. Its services align security controls with sector-specific compliance and governance requirements.

Automation-led SecOps integration: SCC differentiates through its automation-first approach, leveraging proprietary IP such as the Pulse platform to automate L1 triage, enrichment and response workflows. This approach reduces analyst dependency while improving speed and consistency in security operations.

Integrated visibility and governance: SCC's Secure Vision platform aggregates telemetry across tools and services, delivering unified dashboards, compliance reporting and executive-level insights. This supports continuous monitoring, governance and data-driven decision-making across security environments.

Caution

Although SCC delivers strong execution and compliance alignment, further strengthening its depth in advanced technical security domains, including offensive security and threat validation capabilities, alongside more standardised service offerings, will enhance its positioning among midmarket organisations.

Next-Gen SOC/MDR Services – Large Accounts

Who Should Read This Section

This report is valuable for service providers offering **next-gen SOC services** in the **UK** to understand their market position and for large enterprises looking to evaluate these providers. In this quadrant, ISG highlights the importance of establishing a robust foundation for continuous threat detection and response to enable proactive risk management and uphold compliance in dynamic operational environments.

Cybersecurity professionals

Cybersecurity professionals should read this report to understand how next generation SOC and MDR providers align services with compliance requirements while supporting enterprise transformation. The analysis highlights approaches to building resilient security strategies, managing complex environments, and mitigating risk by combining AI driven threat hunting and forensics with established security operations.

Technology professionals

Technology professionals should read this report to stay informed on SOC and MDR trends and evaluate providers offering tailored, scalable security platforms. Compliance leaders can identify SOCaligned providers that meet regulatory needs, while IT leaders gain insight into vendorneutral expertise that supports diverse infrastructures and strengthens security integration across enterprise systems.

Business professionals

Business professionals should read this report to gain practical insights into simplifying security operations without compromising effectiveness. The findings highlight how enterprises can reduce operational complexity, improve efficiency, and select providers that deliver measurable value by integrating advanced security capabilities into streamlined, costeffective operating models.

Cybersecurity professionals

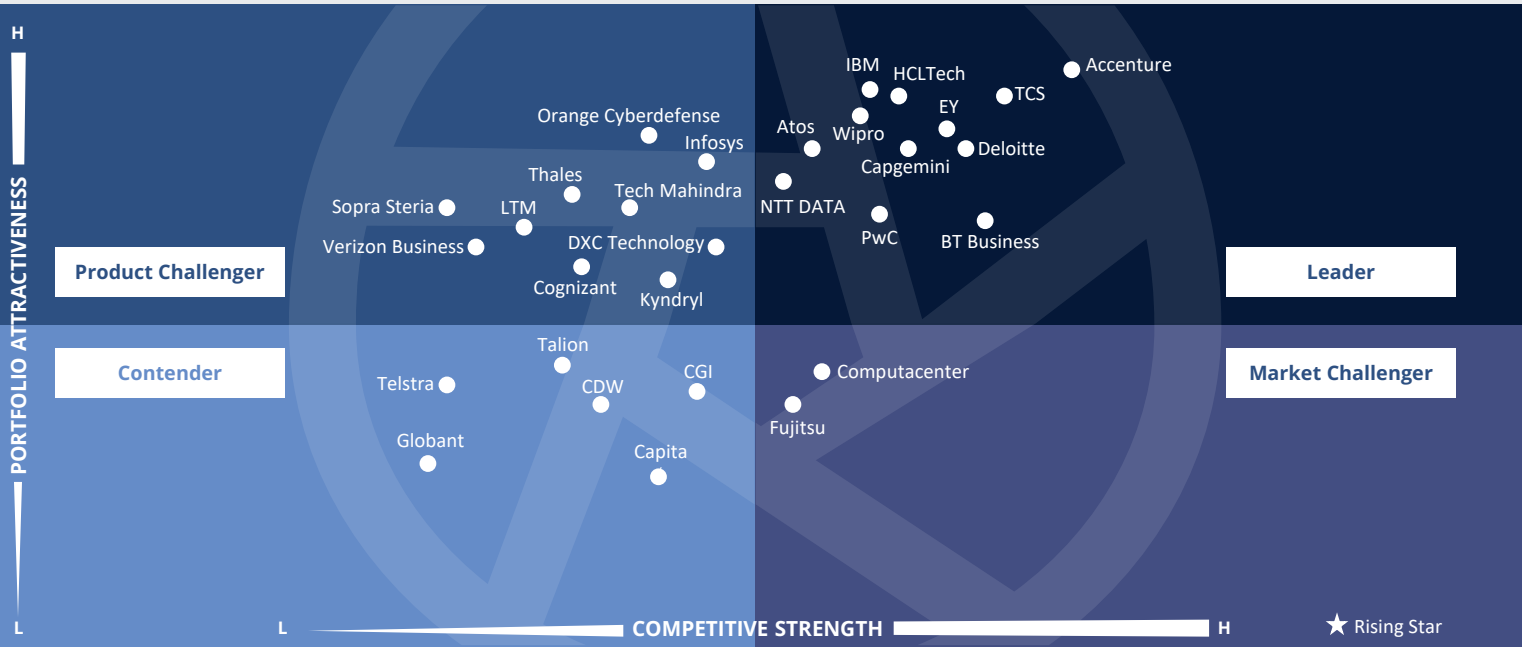
Cybersecurity professionals should read this report to understand how next generation SOC and MDR providers align services with compliance requirements while supporting enterprise transformation. The analysis highlights approaches to building resilient security strategies, managing complex environments, and mitigating risk by combining AI driven threat hunting and forensics with established security operations.

ISG Provider Lens®

Source: ISG RESEARCH

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

U.K. 2026



This quadrant assesses providers with **AI-driven SOC operations, real-time threat intelligence** and **custom detection engineering**, enabling **enterprise-grade SOC/MDR** tailored to **complex hybrid environments** and **multi-region risk profiles.**

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that deliver continuous monitoring and MDR services through SOCs. Their offerings span the entire incident lifecycle, including detection, triage, investigation, containment and coordinated remediation. Providers integrate and operate modern security technologies, apply threat intelligence and advanced analytics, and deliver human-led and automated threat hunting to strengthen enterprise resilience. Next-gen SOC/MDR services combine managed security operations with innovative AI-driven analytics, autonomous triage and security orchestration, automation and response (SOAR)-based orchestration to reduce response times and improve threat visibility across IT and OT environments. They support co-managed models and do not focus on strategic advisory or technology implementation, which fall within the scope of SSS and TSS, respectively.

Eligibility Criteria

1. Deliver 24/7 **monitoring, detection and response** services through **owned SOCs,** covering IT and/or OT environments
2. Provide **MDR-specific capabilities**, including behavioural analytics, large language model (LLM)-aware threat intelligence integration, human-led and automated threat hunting, and advanced detection engineering
3. **Operate and manage** Security Information and Event Management (SIEM), SOAR, endpoint detection and response (EDR), network detection and response (NDR) and other relevant security technologies, supported by OEM accreditations
4. Demonstrate a structured **incident response approach** covering triage, investigation, containment, remediation coordination and post-incident improvement
5. Use **AI-driven** analytics, autonomous triage agents and SOAR workflows to accelerate detection and reduce mean time to respond (MTTR)
6. Offer **co-managed service** models with enterprise teams, enabling shared visibility, analyst collaboration and joint response processes
7. Present **reference cases** showing measurable improvements in detection coverage, response efficiency or operational resilience within the target region
8. **Do not** focus exclusively on proprietary products, but manage and operate best-of-breed security tools

Observations

In 2026, board-level accountability under FCA's operational resilience regime, DORA alignment and rapid adoption of AI-driven security operations shape the demand for next-gen SOC and MDR services among large enterprises in the UK.

Providers are moving beyond scale-based delivery towards intelligence-driven platforms that unify cloud, identity and end-point telemetry into a single analytics layer. GenAI copilots and automated investigation pipelines are embedded, reducing triage workloads, while federated threat intelligence across EMEA improves response precision against advanced threats.

Continuous control validation is now a baseline expectation. Enterprises require audit-ready evidence trails, making compliance-by-design a core SOC feature. The UK's requirements around data residency and regulatory oversight are reinforcing the demand for sovereign delivery models, supported by hyperscaler partnerships, regional SOC presence and customer-managed encryption controls.

Co-managed SOC models are becoming standard, with enterprises retaining oversight while outsourcing detection, threat hunting and response execution. This drives demand for shared visibility, integrated workflows and clear accountability between internal teams and providers.

Providers are differentiating through outcome-based SLAs linked to MTTR and risk reduction, alongside sector-specific accelerators. As hyperscalers expand native XDR capabilities, leading providers are focusing on orchestration maturity, AI explainability and cross-platform integration.

The shift is from reactive monitoring to predictive, increasingly autonomous security operations, where data residency, automation governance and business-risk correlation determine leadership.

From the 67 companies assessed for this study, 30 qualified for this quadrant, with 12 being Leaders.

accenture

Accenture delivers AI-driven SOC services through Cyber Fusion Centres, combining automation, threat intelligence and global scale to enable resilient, intelligence-led security operations.

Atos

Atos provides sovereign, intelligence-led SOC services through its TDIR model, integrating threat intelligence, proactive defence and regulatory alignment for critical and regulated environments.

BT Business

BT Business delivers network-integrated SOC services leveraging its Global Fabric and UK sovereign infrastructure, enabling real-time monitoring and response across distributed, connectivity-driven environments.

Capgemini

Capgemini delivers industrialised SOC services through its global Cyber Defense Centres, combining platform-led operations, automation and compliance alignment for scalable enterprise security operations.

Deloitte.

Deloitte delivers risk-aligned SOC services integrating detection, response and governance, enabling organisations to align security operations with compliance and enterprise risk frameworks.

EY

EY provides transformation-aligned SOC services integrating monitoring, response and risk governance, supporting organisations in aligning security operations with resilience and compliance objectives.

HCLTech

HCLTech delivers AI-driven SOC services through its Cyber Security Fusion Centres, leveraging automation, proprietary platforms and global delivery to enable scalable, intelligence-led operations.

IBM

IBM provides platform-led SOC services through its X-Force and QRadar ecosystem, combining threat intelligence, analytics and automation to deliver advanced detection and response capabilities.

NTT DATA

NTT DATA delivers globally scaled SOC services integrating AI-enabled detection, threat intelligence and automation, supporting resilient operations across complex enterprise environments.

pwc

PwC delivers automation-led SOC services focused on transformation and AI-enabled operations, supporting organisations in modernising security operations and improving response effectiveness.

TCS TATA CONSULTANCY SERVICES

TCS provides AI-infused SOC services through its Cyber Defense Suite, enabling scalable detection, response and automation across hybrid enterprise environments.

wipro

Wipro delivers AI-enabled SOC services using platform-driven operations and innovation, supporting proactive and scalable threat detection and response.

Next-Gen SOC/MDR Services – Midmarket

Who Should Read This Section

This report is valuable for service providers offering **managed detection and response (MDR)** services in the **UK** to understand their market position and for midmarket enterprises looking to evaluate these providers. In this quadrant, ISG highlights the key enterprise challenges of tackling advanced threats, minimising response times and combating alert fatigue.

Cybersecurity professionals

Cybersecurity professionals should read this report to understand how nextgeneration SOC and MDR providers align services with compliance requirements while supporting enterprise transformation. The analysis highlights approaches to building resilient security strategies, managing complex environments, and mitigating risk by combining AIdriven threat hunting and forensics with established security operations.

Technology professionals

Technology professionals should read this report to stay informed on SOC and MDR trends and evaluate providers offering tailored, scalable security platforms. Compliance leaders can identify SOCaligned providers that meet regulatory needs, while IT leaders gain insight into vendorneutral expertise that supports diverse infrastructures and strengthens security integration across enterprise systems.

Business professionals

Business professionals should read this report to gain practical insights into simplifying security operations without compromising effectiveness. The findings highlight how enterprises can reduce operational complexity, improve efficiency, and select providers that deliver measurable value by integrating advanced security capabilities into streamlined, cost effective operating models.

Cybersecurity professionals

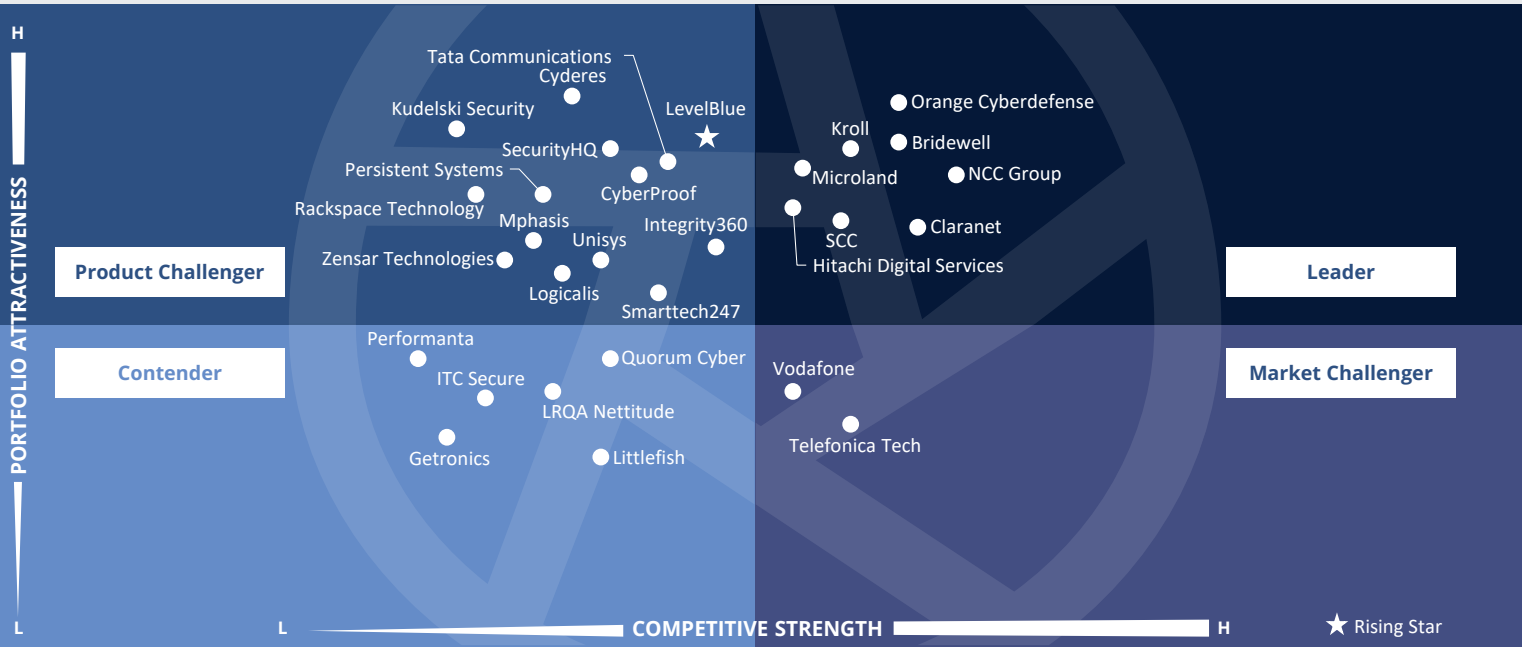
Cybersecurity professionals should read this report to understand how next generation SOC and MDR providers align services with compliance requirements while supporting enterprise transformation. The analysis highlights approaches to building resilient security strategies, managing complex environments, and mitigating risk by combining AI driven threat hunting and forensics with established security operations.

ISG Provider Lens®

Source: ISG RESEARCH

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

U.K. 2026



This quadrant assesses providers offering **MDR services, fast onboarding** and **cost-optimised security automation**, enabling **midmarket clients** to meet growing threats with **minimal internal overhead**.

Bhuvaneshwari Mohan

Definition

This quadrant evaluates service providers that deliver continuous monitoring and MDR services through SOCs. Their offerings span the entire incident lifecycle, including detection, triage, investigation, containment and coordinated remediation. Providers integrate and operate modern security technologies, apply threat intelligence and advanced analytics, and deliver human-led and automated threat hunting to strengthen enterprise resilience. Next-gen SOC/MDR services combine managed security operations with innovative AI-driven analytics, autonomous triage and security orchestration, automation and response (SOAR)-based orchestration to reduce response times and improve threat visibility across IT and OT environments. They support co-managed models and do not focus on strategic advisory or technology implementation, which fall within the scope of SSS and TSS, respectively.

Eligibility Criteria

1. Deliver 24/7 **monitoring, detection and response** services through owned SOCs, covering IT and/or OT environments
2. Provide **MDR-specific capabilities**, including behavioural analytics, large language model (LLM)-aware threat intelligence integration, human-led and automated threat hunting, and advanced detection engineering
3. **Operate and manage** Security Information and Event Management (SIEM), SOAR, endpoint detection and response (EDR), network detection and response (NDR) and other relevant security technologies, supported by OEM accreditations
4. Demonstrate a structured **incident response approach** covering triage, investigation, containment, remediation coordination and post-incident improvement
5. Use **AI-driven** analytics, autonomous triage agents and SOAR workflows to accelerate detection and reduce mean time to respond (MTTR)
6. Offer **co-managed** service models with enterprise teams, enabling shared visibility, analyst collaboration and joint response processes
7. Present **reference cases** showing measurable improvements in detection coverage, response efficiency or operational resilience within the target region
8. **Do not** focus exclusively on proprietary products, but manage and operate best-of-breed security tools

Observations

The Next-Gen SOC/MDR Services quadrant for the UK midmarket reflects a shift towards faster, intelligence-driven detection and response, alongside the growing demand for transparency, cost efficiency and regulatory alignment. Organisations are seeking services that can be deployed quickly and operated with minimal internal overhead, often within constrained security teams.

ISG's analysis highlights a move towards platform-enabled MDR, where AI-assisted enrichment, automated investigation workflows and integrated response orchestration are becoming the norm. Co-managed operating models are gaining traction, allowing organisations to retain oversight while relying on providers for monitoring, threat hunting and response execution. Ease of onboarding and integration with existing SIEM, XDR and identity platforms is a key buying factor.

Cloud-native SOC architectures, improved identity and SaaS telemetry coverage and the effective use of threat intelligence are shaping service maturity. However, midmarket buyers prioritise practicality over sophistication, favouring providers that can deliver clear response actions, simplified reporting and consistent detection engineering without excessive complexity.

The ecosystem is evolving through consolidation, increased automation and expansion of sector-specific threat models aligned to NIS2, DORA and UK frameworks such as CAF. Expectations are rising around measurable outcomes, especially reduced response time and improved risk visibility.

In this quadrant, the ability to deliver scalable, easy-to-consume MDR services that balance automation with clarity while aligning to UK regulatory requirements and operating constraints drives differentiation in the midmarket.

From the 67 companies assessed for this study, 30 qualified for this quadrant, with eight being Leaders and one Rising Star.

Bridewell

Bridewell differentiates through its UK-sovereign, intelligence-led MDR model, combining rapid co-managed SOC integration, **Microsoft** ecosystem depth and growing European scale to deliver highly contextualised, regulation-aligned security operations.

claranet

Claranet delivers cloud-integrated SOC and MDR services, combining managed infrastructure, proprietary automation platforms and vulnerability-led security operations to support midmarket organisations.

Hitachi Digital Services

Hitachi Digital Services delivers globally integrated SOC and MDR services, combining IT, OT and IIoT threat detection with advisory-led cyber resilience capabilities for midmarket and regulated sector organisations.

MICROLAND®

Microland delivers next-generation SOC and MDR services through its Assured Cyber Resilience Managed Security (ACRMS) model, combining AI-augmented detection, identity-led security and outcome-driven cyber resilience for midmarket and enterprise clients.

nccgroup

NCC Group distinguishes itself through its deep threat intelligence heritage and incident response pedigree, delivering highly contextualised MDR services that prioritise adversary insight and real-world attack disruption for UK midmarket clients.

Cyberdefense

Orange Cyberdefense delivers next-generation SOC and MDR services through its global security operations platform, combining network-native telemetry, advanced threat intelligence and large-scale managed security capabilities.

Kroll

Kroll delivers next-generation SOC and MDR services through its Redscan platform, combining incident response expertise, threat intelligence and continuous monitoring to support organisations with high-risk security environments.

SCC

SCC delivers next-generation SOC and MDR services through its UK-based operations, combining automation-led SecOps, Microsoft-native security capabilities and integration-driven delivery for midmarket and public sector organisations.

LevelBlue

LevelBlue (Rising Star) delivers next-generation SOC and MDR services through a unified platform approach, combining large-scale telemetry, multi-vendor integration and AI-augmented security operations to support global enterprises and midmarket clients.

Leader

"SCC differentiates through its automation-first SOC model, leveraging proprietary IP and Microsoft-aligned security operations to deliver fast, efficient and scalable MDR services tailored to UK mid-market and public sector clients."

Bhuvaneshwari Mohan

SCC

Overview

SCC is headquartered in the UK and operates across Europe as part of SCC Digital. The company employs over 7,000 people globally and supports cybersecurity operations through a growing team of specialists and certified professionals. SCC has expanded its cybersecurity capabilities in recent years through targeted investments. Its UK-based SOC in Birmingham, supported by a delivery centre in Romania, enables sovereign and hybrid delivery models aligned to public sector and regulated clients. Its MDR services leverage proprietary platforms such as Pulse for automation and Secure Vision for analytics and reporting.

Strengths

Automation-first SOC architecture: SCC's Pulse platform automates Level 1 SOC operations, including alert triage, enrichment and initial response, eliminating the need for manual L1 analysts. This significantly reduces response times and analyst workload while improving consistency and scalability of MDR operations.

Integrated Microsoft-native security stack: The provider demonstrates deep alignment with Microsoft security technologies, including Sentinel and Defender, enabling efficient integration, TDR across client environments. This ecosystem-driven approach supports rapid deployment and operational standardisation.

Proprietary visibility and governance platform: SCC's Secure Vision platform aggregates data across multiple tools and services, providing unified dashboards, executive reporting and compliance visibility. This enhances transparency and supports decision-making across operational, executive and board levels.

Flexible delivery and co-managed models: SCC supports fully managed, hybrid and co-managed SOC models, underpinned by its Aegis platform, allowing clients to retain internal capabilities while leveraging external expertise. This flexibility aligns well with mid-market and public sector organisations with varying maturity levels.

Caution

While SCC's automation-led and Microsoft-centric approach delivers strong operational efficiency, further investment in advanced threat intelligence, broader ecosystem depth and clearer differentiation beyond Microsoft-aligned services will be important to compete with more specialized and platform-driven MDR providers.

Appendix

The ISG Provider Lens 2026 – Cybersecurity – Services and Solutions study analyzes the relevant software vendors/service providers in the UK market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Author:
Bhuvaneshwari Mohan

Editor:
Sajina B

Research Analyst:
Monica K

Data Analysts:
Rajesh Chillappagari and Laxmi Sahebrao Kadve

Project Manager:
Smita S M

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.

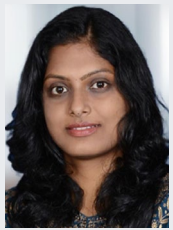
The research and analysis presented in this report includes research from the ISG Provider Lens® program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. The data collected for this report represent information that ISG believes to be current as of May 2026 for providers that actively participated and for providers that did not. ISG recognizes that many mergers and acquisitions may have occurred since then, but this report does not reflect these changes.

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

The study was conducted in the following steps:

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

Lead Author



Bhuvaneshwari Mohan
Lead Analyst

Bhuvaneshwari Mohan is a Lead Analyst at ISG Research, focusing on cybersecurity solutions and services, with primary responsibility for ISG Provider Lens® studies across the U.K. and U.S. public sector. She contributes to research and advisory insights spanning digital sustainability services and supply chain services, with a focus on market positioning, service evolution and enterprise adoption patterns.

With over a decade of industry experience, Bhuvaneshwari specializes in market intelligence, competitive benchmarking and enterprise-focused research. She contributes to thought leadership on cybersecurity, enterprise resilience and evolving service delivery models, and collaborates closely with ISG advisors to deliver strategic, client-specific research. Prior to ISG, she worked in research and enablement roles within IT and digital engineering services organizations, strengthening her expertise in translating market dynamics into actionable business insights.

Enterprise Context and Global overview analyst

Monica K
Research Analyst

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

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

Study Sponsor

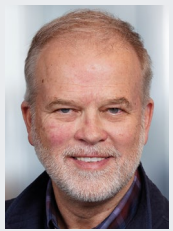
Heiko Henkes

Director & Principal Analyst, Global IPL Content Lead

Heiko Henkes serves as Managing Director and Principal Analyst at ISG, where he oversees the Global ISG Provider Lens® (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as strategic program manager and thought leader for IPL Lead Analysts. Additionally, Henkes heads the 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 renowned for his contributions as a keynote speaker on digital innovation, where he shares insights on leveraging 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. 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 and cities) and 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 AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth.

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

For more information, visit isg-one.com.

ISG Provider Lens®

JUNE, 2026

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS