ISG Provider Lens™

Cybersecurity — Solutions and Services

A research report evaluating solutions and service providers' capabilities across cybersecurity portfolios and key differentiators

Customized report courtesy of:

claranet

QUADRANT REPORT | JULY 2022 | U.K.

Table of Contents

Page 1 of 2

Page 2 of 2

Report Author: Arun Kumar Singh

Cybersecurity – Bedrock for UK's digital economy

Year 2022 marks the beginning of the UK's fourth ground breaking cybersecurity strategy in which the emphasis moves from cybersecurity to cyber power to boost the UK's digital economy and protect itself in the fast-evolving digital world.

The current National Cyber Security Strategy claims major progress collectively achieved by 1,400 UK cybersecurity businesses, contributing £8.9 billion in revenues last year, with 46,700 skilled jobs and opportunities for foreign investments. The UK government's budget for the National Cyber Security Programme was increased by £114 million, with a planned investment of £2.6 billion in cyber and legacy IT over the next spending review period.

The UK government is pumping incentives and devising programmes (e.g. LORCA, CyLon, and secure by design, etc.) for startups to solve key cybersecurity challenges. This results in an ecosystem of technology players, investors, academia, startups, industries, and government organisations to drive growth and innovation in the UK cybersecurity sector.

Rising Data Breaches and Associated Costs

According to NCSC's 2022 cybersecurity breach study, 39 percent of UK businesses experienced a cybersecurity breach in the last 12 months. The average cost of data breaches for a business is £8,460. For large and midmarket businesses, the cost rises to £19,400.

The UK government is building a **cyber-resilient economy.**

2022 UK CISOs' Priorities

Top three priorities for UK chief information security officers (CISOs) are:

- Establishing cybersecurity strategy for cloud models (IaaS, PaaS, SaaS, and hybrid)
- Driving a holistic resilience approach by communicating, training, and upskilling their employees and external stakeholders
- Become an enabler and align with organisation's business goals

Trust No One – Zero Trust (ZT)

With the US government's adoption of the ZT security model, the UK government is focusing on de-risking its digital transformation efforts. In the post-pandemic world, the growing adoption of the hybrid work model, increasing IT complexity, becoming an agile organization, and many more reasons will be driving board-level discussions to accelerate ZT security model adoption. Implementing the ZT model would result in reduced security costs and risk exposure, greater CISO confidence, and uniform security across an organisation.

ZT security elements such as network segmentation; security, information, and event management (SIEM); security orchestration, automation, and response (SOAR); endpoint detection and response (EDR); and multi-factor authentication (MFA) are crucial for mitigating IT and operational technology (OT) vulnerabilities.

Identity and Access Management (IAM) Trends

Passwords are the all-time favourite channel among malicious actors to get easy access to an enterprise network. According to a 2021 Verizon Data Breach Report, 81 percent of the confirmed data breaches involved leveraging weak, stolen, and default user passwords. Organisations are increasingly extending their budgets for two-factor authentication, password-less authentication, and privileged access management (PAM) to protect their virtual workforces amid the growing threat landscape. With a growing emphasis on automation to achieve process efficiency and productivity, organisations turn to RPA tools, virtual machines, and IoT devices, leading to demand growth for IAM tools for machine identities in the ZT framework (with hybrid and multicloud environments). IAM tool vendors are pursuing acquisitive strategies to offer integrated and cloud-based solutions with a wide range of features.

Data Leakage/Loss Prevention (DLP) and Data Security Trends

Businesses are wary of the stringent data protection laws, such as General Data Protection Regulation (GDPR), which impose hefty penalties for data breaches or being non-compliant. DLP will continue to remain the first step towards keeping data safe and reducing human touch surface. The increasing amount of unstructured data is pushing organisations to look at dynamic DLP tools that can monitor, evaluate, and analyse user behavioural patterns and secure workflows to avoid data leakage and exfiltration.

CIOs and CISOs are planning and implementing the zero trust security model to keep any threat at the bay, for which DLP and data classification services are essential. Secure email gateways, secure web gateways, and endpoint security solutions with native DLP capabilities to support multiple business use cases will be in demand to meet legal and compliance standards.

Advanced Endpoint Threat Protection, Detection, and Response (AETPDR) Trends

Alert overloads and false positive security alerts continue to trouble cybersecurity professionals. According to Critical Start, almost 50 percent of all security operations centre (SOC) analysts said that they turn off high-volume alerting features when there are too many alerts for analysts to process, creating the potential for a serious alert to be missed. Thus, platform-based endpoint detection and response tools, which allow organisations to have a proactive security posture and avoid the aftermath of skipping alerts, see an increase in demand.

Organisations are building large data lakes under EDR tools to store the collected endpoint telemetry data to identify and analyse potential threats and to provide real-time visibility of malicious events and AI-based threat mitigation steps.

Technical Security Services (TSS) Trends

With operating environments increasingly becoming complex with fragmented tools deployment, low utilisation, and third-party risks, TSS providers continue to guide businesses through each stage of the implementation lifecycle and offer product-certified implementation expertise. Some organisations have deployed more than 50 security tools and technologies to remain cyber resilient to the ever-growing threats. This clearly indicates the dependency on managed security service providers (MSSPs) for implementation and integration expertise whenever a new tool is added to a complex IT infrastructure.

Strategic Security Services (SSS) Trends

UK public and private businesses have turned to cloud-based solutions to gain business continuity, resilience, agility, and safe return to workplaces with usual benefits like quick access to market, lower OpEx costs, high availability, and elastic computing power.

Some of the key trends we are witnessing in the consulting services domain are:

- Rising local regulatory and compliance pressure
- Cybersecurity becoming one of the key topics among boardroom discussions
- Digital transformation initiatives often neglecting cybersecurity aspects and avoiding regular security assessments for quick deployments
- Deficiency of internal resources to conduct regular risk assessments and testing
- Growing inclination towards the zero trust approach

Large and midmarket enterprises are engaging with consulting services to help them in understanding and identifying suitable technologies to fit into their existing infrastructure and drive the demand for TSS and MSS.

Managed Security Services (MSS) Trends

The proactive approach remains the key to predict, prevent, detect, identify, respond, and recover from security breaches. This approach is embraced by UK businesses to keep tabs on costs and improve security awareness among employees. MSSPs continue to see rapid demand for MSS from businesses with low-maturity security postures to keep their infrastructure secure.

With increasingly stringent UK and EU regulations and compliance requirements, UK businesses are expecting data centres, delivery centres, and SOCs to be onshore or nearshore and have appropriate resilience plans for data storage compliance. However, unless clients require a local presence many MSSPs are delivering cybersecurity services through virtual SOCs to lower their operational costs. Recently, MSSPs have been targeted by malicious actors for high-profile cybersecurity attacks to gain financial benefits from them and their customers.

MSSPs are investing in platforms to gain a single pane of glass for management and orchestration capabilities to reduce security analysts' fatigue and continue to offer them effective visibility into clients' environments. They are struggling to support data ingestion via API integrations in multicloud environments across the three leading hyperscalers for remediation efforts.

Managed detection and response (MDR) capabilities are helping organisations with threat hunting, intelligence, detection, and response. We have observed that some of the legacy MSS players are building MDR capabilities, for example, SecureWorks is slowly transitioning from a pure managed services player to an extended detection and response (XDR) solution provider, bundling XDR services.

MDR services, AI, machine learning, and analytics are becoming fundamental expectations.

Provider Positioning

Page 1 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Absolute Software	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Leader	Leader	Leader	Not In
AT&T Cybersecurity	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In
Atos	Product Challenger	Not In	Not In	Leader	Leader	Leader	Not In
BAE Systems	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Blackberry (Cylance)	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Leader	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Rising Star ★	Market Challenger	Leader	Not In

Provider Positioning

Page 2 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader	Not In
CGI	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In
Check Point	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Cisco	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Not In	Product Challenger	Not In	Leader
Cognizant	Not In	Not In	Not In	Contender	Market Challenger	Market Challenger	Not In
Comodo	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Computacenter	Not In	Not In	Not In	Contender	Product Challenger	Market Challenger	Market Challenger
CoSoSys	Not In	Contender	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In	Not In

Provider Positioning

Page 3 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In
Darktrace	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader	Not In
DXC Technology	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In
ECSC	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
ESET	Not In	Not In	Contender	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Product Challenger	Leader	Not In	Not In
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 4 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Forcepoint	Not In	Leader	Not In	Not In	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Contender	Market Challenger	Market Challenger
GBS	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Getronics	Not In	Not In	Not In	Contender	Contender	Not In	Contender
Google	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Happiest Minds	Not In	Not In	Not In	Contender	Contender	Not In	Product Challenger
HCL	Not In	Not In	Not In	Leader	Leader	Leader	Not In
HelpSystems	Not In	Leader	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 5 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Herjavec Group	Not In	Not In	Not In	Not In	Not In	Not In	Leader
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Not In
Ilantus Products	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Product Challenger	Product Challenger	Rising Star ★	Not In
ITC Secure	Not In	Not In	Not In	Contender	Contender	Not In	Contender
Ivanti	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Kaspersky	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Kudelski Security	Not In	Not In	Not In	Contender	Contender	Contender	Not In
Logicalis	Not In	Not In	Not In	Contender	Contender	Not In	Product Challenger
LTI	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger

Provider Positioning

Page 6 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Micro Focus	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Microland	Not In	Not In	Not In	Contender	Contender	Product Challenger	Product Challenger
Microsoft	Leader	Market Challenger	Leader	Not In	Not In	Not In	Not In
Mindtree	Not In	Not In	Not In	Contender	Not In	Not In	Contender
Mphasis	Not In	Not In	Not In	Not In	Not In	Contender	Contender
NCC Group	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★
Netskope	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Nettitude	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Nexus Group	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
NTT	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In

Provider Positioning

Page 7 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Omada	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger	Leader
Palo Alto Networks	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Persistent Systems	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In
Ping Identity	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Not In	Leader	Not In	Not In

Provider Positioning

Page 8 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Rackspace Technology	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
SentinelOne	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Shearwater Group	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger
SilverSky	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Sophos	Not In	Not In	Leader	Not In	Not In	Not In	Not In
TCS	Not In	Not In	Not In	Leader	Rising Star ★	Leader	Not In

Provider Positioning

Page 9 of 10

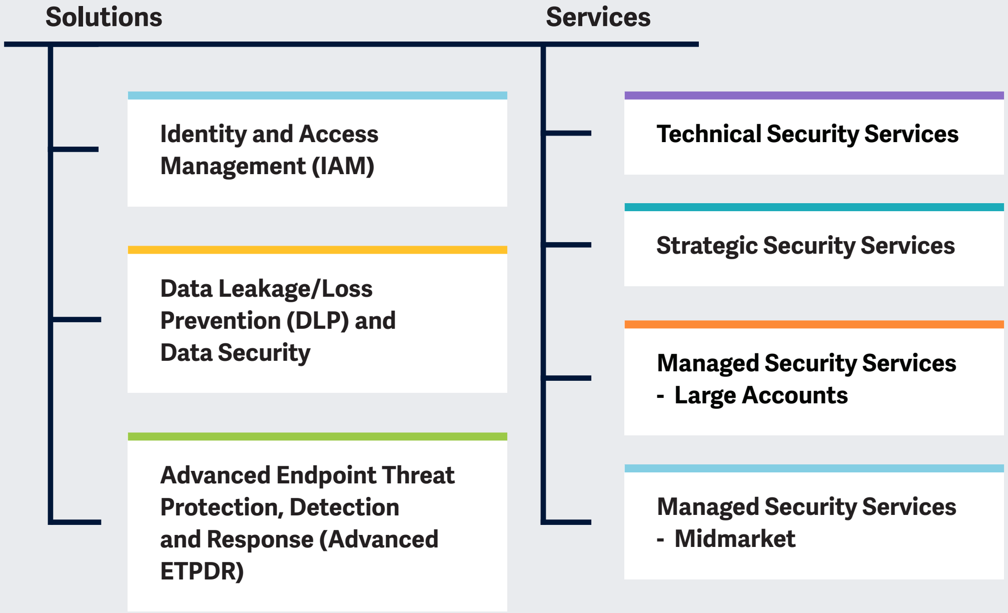
	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
Telstra	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Not In
Thales	Market Challenger	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Trellix	Not In	Leader	Product Challenger	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Rising Star ★	Not In	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Unisys	Product Challenger	Not In	Not In	Product Challenger	Contender	Product Challenger	Product Challenger
ValueLabs	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Verizon	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In

Provider Positioning

Page 10 of 10

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
VMware Carbon Black	Not In	Not In	Leader	Not In	Not In	Not In	Not In
WatchGuard	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Zensar	Not In	Not In	Not In	Contender	Contender	Contender	Contender
Zscaler	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In

This report has six quadrants on **cybersecurity solutions and services.**



Solutions

Identity and Access Management (IAM)

Data Leakage/Loss Prevention (DLP) and Data Security

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

Services

Technical Security Services

Strategic Security Services

Managed Security Services - Large Accounts

Managed Security Services - Midmarket

Simplified Illustration Source: 2022

Definition

Enterprises are adopting emerging technologies to embark on their digital transformation journeys to stay competitive. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has led to an increase in threat attack surface. With the ever-changing threat landscape and stringent regional regulations and compliances, enterprises need to take a detailed and inclusive approach to cybersecurity to safeguard their businesses by implementing a mix of security products and services across areas to achieve a robust, secure framework to reduce risk exposure. On the other hand, deploying adequate security tools does not imply that an enterprise will be immune to vulnerabilities; the human factor continues to remain the weakest link in the security wall.

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following six quadrants: Identity and Access Management (IAM), Data Leakage/Loss Prevention (DLP) and Data Security, Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR), Technical Security Services (TSS), Strategic Security Services (SSS) and Managed Security Services (MSS).

The ISG Provider Lens™ Cybersecurity – Solutions and Services 2022 study aims to support ICT decision makers in making the best use of their tight security budgets by offering the following:

- Transparency on the strengths and cautions of relevant providers.
- A differentiated positioning of providers by market segments.
- A perspective on local markets.

For IT providers and vendors, this study serves as an important decision-making basis for positioning, key relationships and go-to-market (GTM) considerations. ISG advisors and enterprise clients leverage the information from ISG Provider Lens™ reports while identifying and evaluating their current vendor relationships and potential engagements.

Provider Classifications

The provider position reflects the suitability of IT service providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT 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 IT 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 US$20 million and US$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 US$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 Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

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

Provider Classifications: Quadrant Key

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

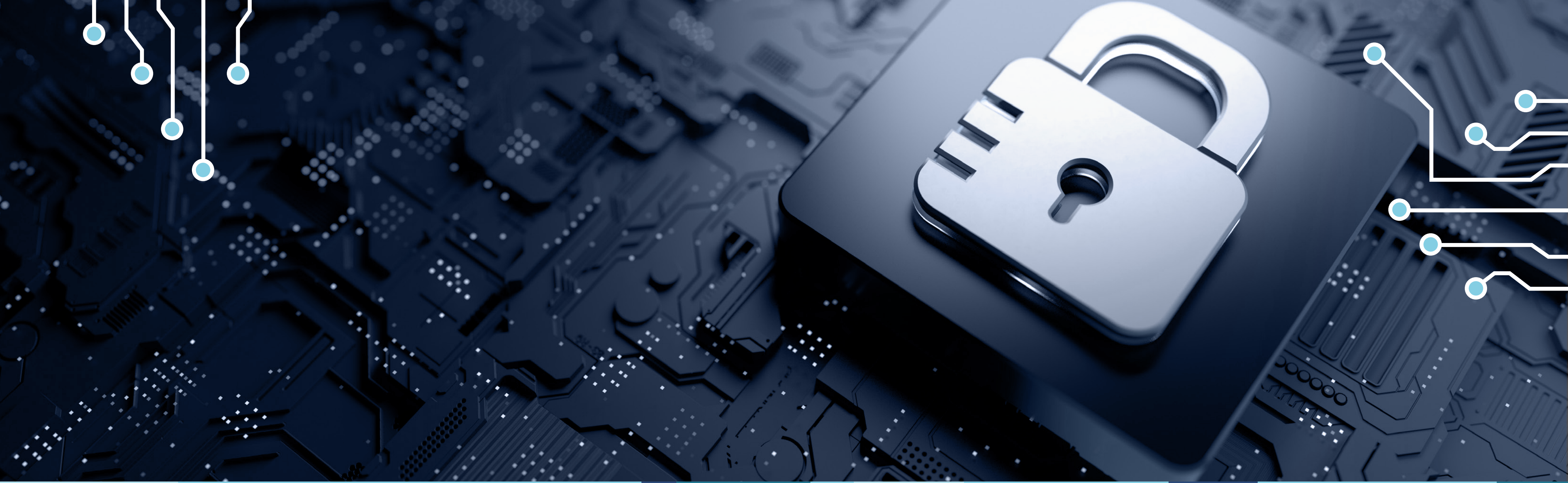
Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength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

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

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

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

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



Identity and Access Management (IAM)

Who Should Read This

This report is relevant to enterprises across industries in the U.K. for evaluating providers that offer solutions that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant report, ISG highlights the current market positioning of providers of identity and access management solutions that reduce security threats for enterprises in the U.K., and how each provider addresses the key challenges in the market.

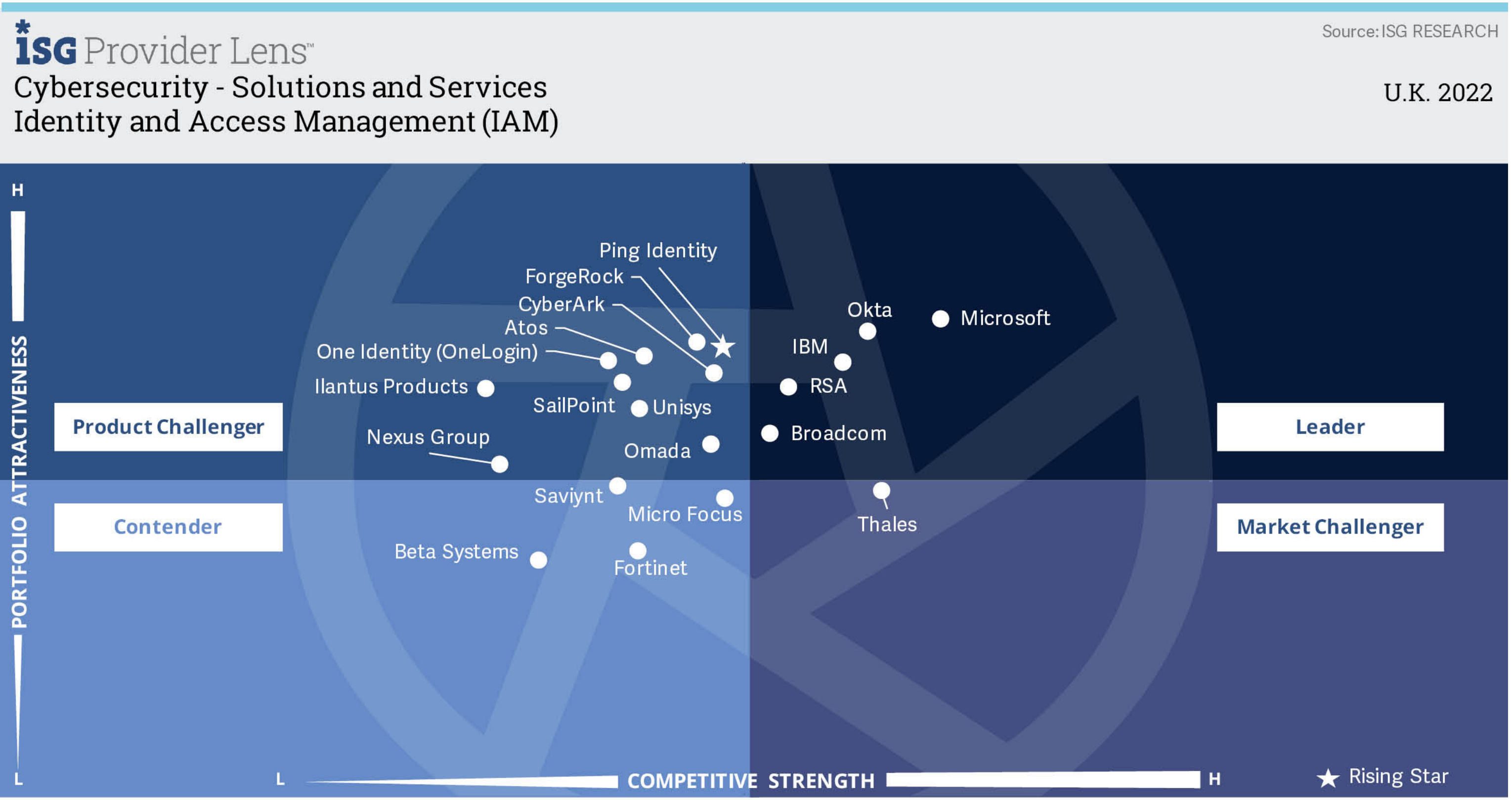
Enterprises are migrating to modern architectures, encompassing components such as the cloud, mobile and APIs, requiring a modern, integrated and open digital IAM architecture to enable them to securely fulfil their business objectives, while managing risks and complying with regulations.

As privileged access management (PAM) evolves, enterprises in the U.K. are seeking a change of PAM use cases from basic privileged account and session management (PASM) capabilities to advanced security management, especially cloud, DevOps and application-to-application password management (AAPM). With the expansion of of the number of endpoints and the need of protection, the demand for privileged elevation and delegation management (PEDM) capabilities have also increased.

Chief information security officer should read this report to understand how IAM solution providers address the significant challenges of compliance and security, while maintaining a seamless experience for enterprise clients

Chief data officers and data privacy officers should read this report to understand how the providers offer information protection and privacy, information governance, data quality and data lifecycle management.

Chief strategy officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



This quadrant assesses the IAM software providers that are characterised by their ability to offer proprietary software and associated services for **securely managing enterprise user identities and devices.**

Arun Kumar Singh

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services for securely managing enterprise user identities and devices. This quadrant also includes software as a service based on proprietary software. Pure service providers that do not offer an IAM product (on-premises and/or cloud) based on proprietary software are not included here. Depending on organizational requirements, these solutions could be deployed in several ways such as on-premises or in the cloud (managed by the customer), or as an as-a-service model, or a combination thereof.

IAM solutions are aimed at collecting, recording and administering user identities and related access rights, as well as specialized access to critical assets, including privileged access management (PAM). They ensure that access rights are granted based on defined policies. To handle existing and new application requirements, IAM solutions are increasingly embedded with secure mechanisms, frameworks, and automation (for example, risk analyses) within their management suites to provide real-time user and attack profiling functionalities. Solution providers are also expected to provide additional functionalities related to social media and mobile use to address their specific security needs that go beyond traditional web and context-related rights management. Machine identity management is also included here.

Eligibility Criteria

1. The solution should be capable of being deployed in **combination with an on-premises, cloud, identity-as-a-service (IDaaS), and managed third-party model.**
2. The solution should be capable of **supporting authentication by a combination of single-sign on (SSO), multifactor authentication (MFA), risk-based, and context-based models.**
3. The solution should be capable of **supporting role-based access and PAM.**
4. The IAM vendor should be able to provide access management for one or more enterprise needs such as cloud, endpoint, mobile devices, application programming interfaces (APIs), and web applications.
5. The solution should be **capable of supporting one or more legacy and newer IAM standards,** including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust, and SCIM.
6. To support through secure access, the portfolio should offer one or more of the following: **directory solutions, dashboard or self-service management, and lifecycle management** (migration, sync, and replication).

Observations

Organisations are shifting from manual processes and access configuration management to free up their resources to focus on critical tasks. The IAM software market continues to evolve, with organisations embarking on cloud transformation.

The IAM tools segment is witnessing consolidation. It is also undergoing the expansion of the capability portfolio related to identity governance and administration and privileged access management delivered as SaaS. Some of the recent IAM market consolidation events were Okta acquiring AuthO, OneIdentity acquiring OneLogin, Microsoft acquiring CloudKnox Security, and Ping Identity acquiring Singular Key. The adoption of the cloud model has triggered a fresh round of investments from IAM tool providers in establishing data centres and SOCs.

However, SaaS-delivered IAM solutions come with certain challenges in terms of scalability, availability, and reliability.

Zero trust is bringing identity and access to the machines and bots in organisations' hybrid cloud environments to mitigate risks. Cloud computing, distributed workforces, and remote connectivity also will accelerate the adoption of ZT network access.

Multi-factor authentication, in combination with the identity-based ZT framework, will help in improving identity authentication. This involves real-time prevention of identity-based threats by leveraging conditional access and risk-based policies enforced based on authentication patterns, end-user location data, IP addresses, end-user behaviour baselines, and end-user risk scores. AI will play a critical role in fraud minimisation and risk identification.

From the 95 companies assessed for this study, 20 have qualified for this quadrant, with five being Leaders and one Rising Star.

Broadcom

Broadcom's IAM suite provides comprehensive IAM capabilities in a unified and easy-to-use console to deliver productivity and increase audit and compliance efficiency.

IBM

IBM Security Verify, offered in on-premises, cloud, and appliance models, provides a robust solution aligned with the ZT model.

Microsoft

Microsoft's Azure AD product continues to bank on the bundling strategy. It's IAM capabilities have been expanded with added features such as FIDO2 support and an identity experience framework.

Okta

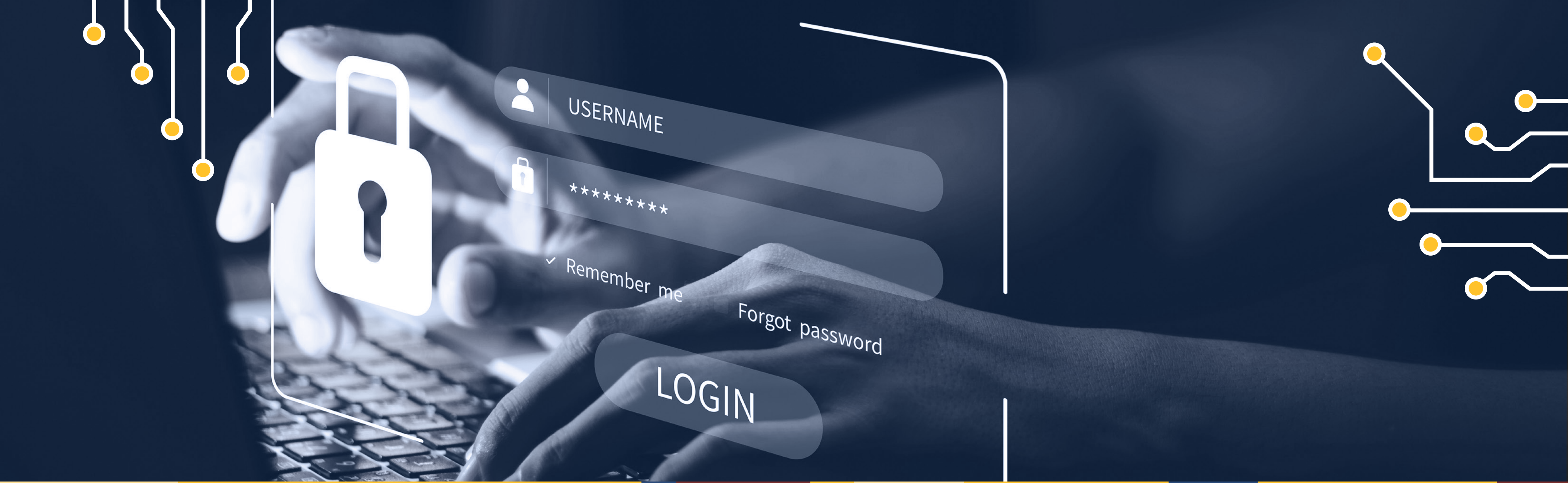
Okta offers simple identity verification options that support a broad set of authentication standards that can easily support heavy traffic loads. It expands developer- and customer identity and access management (CIAM)-oriented products through the acquisition of Auth0.

RSA

RSA SecurID helps organisations of all sizes easily manage access across cloud and on-premises environments, databases, and applications. RSA has easy-to-implement security and compliance policies and risk-based access certifications.

Ping Identity

Ping Identity (Rising Star) offers cloud-based IAM solutions to large enterprises to secure access to APIs, networks, cloud and on-premises applications, and other corporate resources. Its IAM utilises AI to track, detect, and block malicious activities to comply with regulations.



Data Leakage/Loss Prevention (DLP) and Data Security

Who Should Read This

This report is relevant to enterprises across industries in the U.K. for evaluating providers thar offer solutions that integrate multiple cybersecurity features, addressing security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant report, ISG highlights the current market positioning of providers of data leakage/loss prevention (DLP) and data security solution providers that help enterprises in the U.K. mitigate security threats, and how each provider addresses the key challenges.

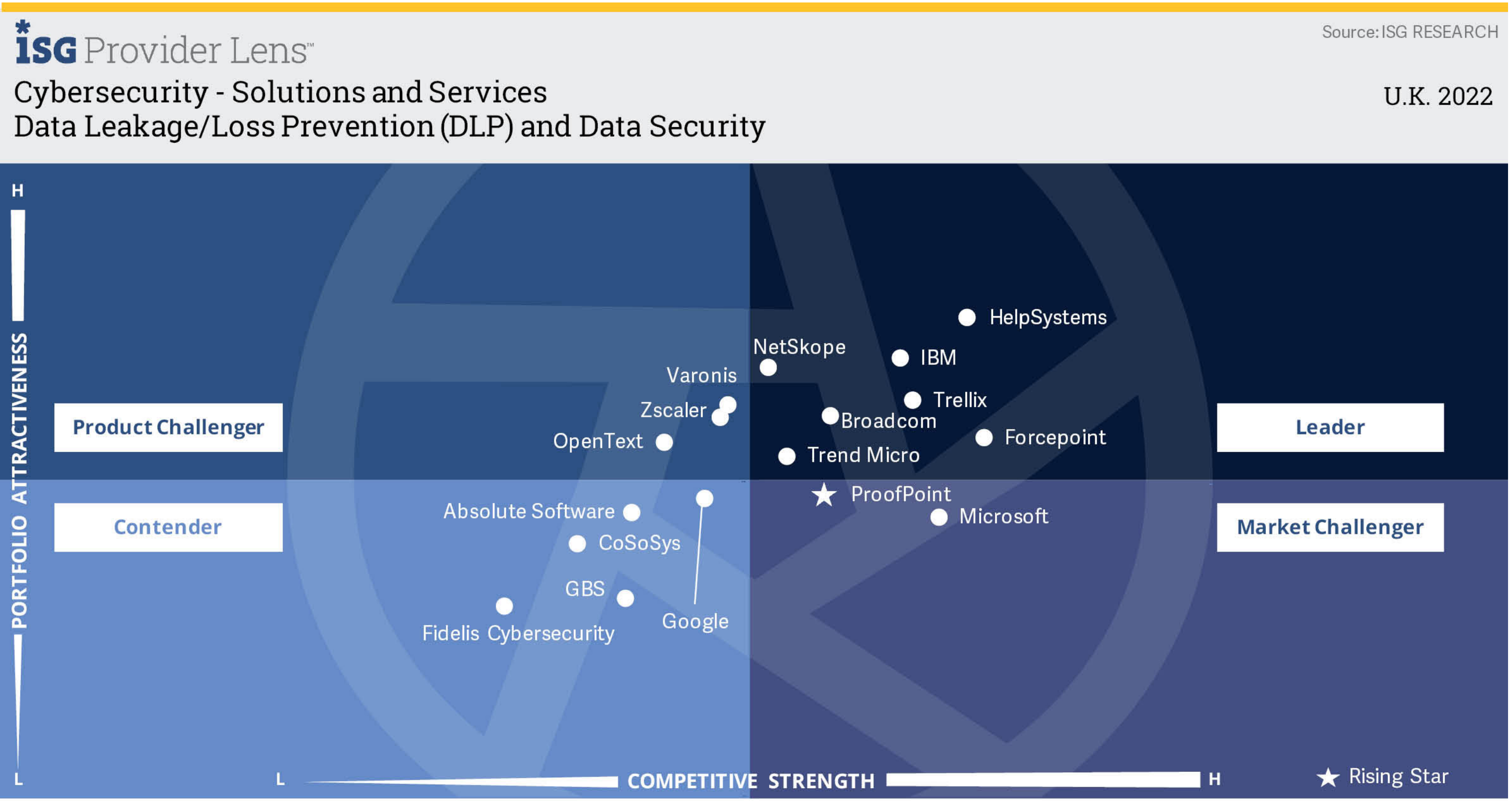
Prior to the COVID-19 pandemic, it was common practice for most employees to work from the office and in a controlled technological environment. This has now shifted in favour of remote work and is unlikely to revert completely to its original form. A large workforce working remotely implies that sensitive data is being accessed from different places, making it vulnerable to data leakage.

Several factors are driving enterprise adoption of DLP solutions, including increasing incidences of data breaches, along with other factors such as providers offering DLP as a service, DLP capabilities extending to the cloud, and the availability of advanced threat protection against these data breaches.

Chief information security officers should read this report to understand how DLP solution providers address the significant challenges of compliance and security, while maintaining a seamless experience for enterprise clients.

Chief data officers and data privacy officer should read this report to understand how the providers offer information protection and privacy, information governance, data quality and data lifecycle management

Chief executive officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



This quadrant assesses DLP software providers' offerings that can **identify and monitor sensitive data, provide access for only authorised users, and prevent data leakage.**

Arun Kumar Singh

Definition

DLP vendors and solution providers are characterised by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. Pure service providers that do not offer a DLP product (on-premises or cloud-based) based on proprietary software are not included here. DLP solutions are offerings that can identify and monitor sensitive data, provide access for only authorised users, and prevent data leakage. Vendor solutions in the market are characterised by a mix of products capable of providing visibility and control over sensitive data residing in cloud applications, endpoint, network and other devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile devices, that are being used to store data is increasing in companies. These are mostly equipped with an Internet connection and can send and receive data without passing it through a central Internet gateway. Data security solutions protect data from unauthorised access, disclosure, or theft.

Eligibility criteria:

1. The DLP offering **should be based on proprietary software** and not on third-party software.
2. The solution should be capable of **supporting DLP across any architecture** such as the cloud, network, storage, or endpoint.
3. The solution should be **capable of handling sensitive data protection across structured or unstructured data, text, or binary data.**
4. The solution should be offered with a **basic management support, including, but not limited to, reporting, policy controls, installation, and maintenance and advanced threat detection** functionalities.
5. The solution should be able to identify sensitive data, **enforce policies, monitor traffic, and improve data compliance.**

Observations

Data continues to remain sensitive, which can be compromised by human factors, resulting in financial and brand image damage to an organisation. The trend of working from anywhere anytime across the globe will be pushing organisations to strengthen their DLP policies, device security, productivity optimisation, and collaboration. The DLP tools market is mature already and seen as the second important point for implementing the SASE framework, after zero trust network access (ZTNA).

To support the ZT approach, organisations are looking for robust data leak prevention platforms with built-in data classification capabilities as table stakes, along with data obfuscation capabilities (encryption, tokenisation, and data masking) and controlled access. To minimize the operational burden, organisations are seeking for capabilities that can enhance tool usability and improve end-user experience around policy creation using templates and automate workflows. AI and machine learning emerge to be an underlying catalyst for DLP utilisation. AI-based user and entity behaviour analytics has been proven effective in anomalous behaviour and activity identification. AI is helpful in orchestrating the configuration of adjacent and impacted systems to reduce the propagation and scope of breaches.

With the growing adoption of SaaS-based applications, organisations are turning to cloud-based DLP solutions, which offers: agentless deployment; API-driven, agnostic platforms, endpoints, and networks; automated policies; and accurate data leak identification (using machine learning).

From the 95 companies assessed in this study, 17 have qualified for this quadrant, with seven being Leaders and one Rising Star.

Broadcom

Broadcom, with its comprehensive and sophisticated DLP solution covering cloud, endpoints, networks, and storage, can become the frontrunner in the DLP market. The company supports its customers through centralisation and standardisation and has a strong presence in the UK.

Forcepoint

Forcepoint offers behaviour-based DLP solutions to cover critical channels like cloud applications, endpoints, networks, web, and email. Forcepoint's DLP can identify and protect data at rest, in motion, and in use. In January 2021, it was acquired by Francisco Partners and appointed a new CEO to drive the ZT edge growth.

HelpSystems

HelpSystems acquired Digital Guardian (a SaaS DLP tool) and Clearswift (deep inspection tool) in 2021. Digital Guardian will be integrated with HelpSystems' powerful security solutions, such as Titus, Boldon James, and Vera, to extend data security capabilities and further enhance its ability to categorise, classify, and protect data.

IBM

IBM combines its significant market presence in the UK with a future-oriented DLP solution and its expertise in AI.

Netskope

Netskope has SASE-ready advanced DLP capabilities that are based on a machine-learning-based DLP engine for SaaS, IaaS, email, and web environments. Netskope received more than $300 million funding to expand its SASE platform and go-to-market strategies. It has expanded its DLP capabilities to protect cloud-based email solutions.

Trellix

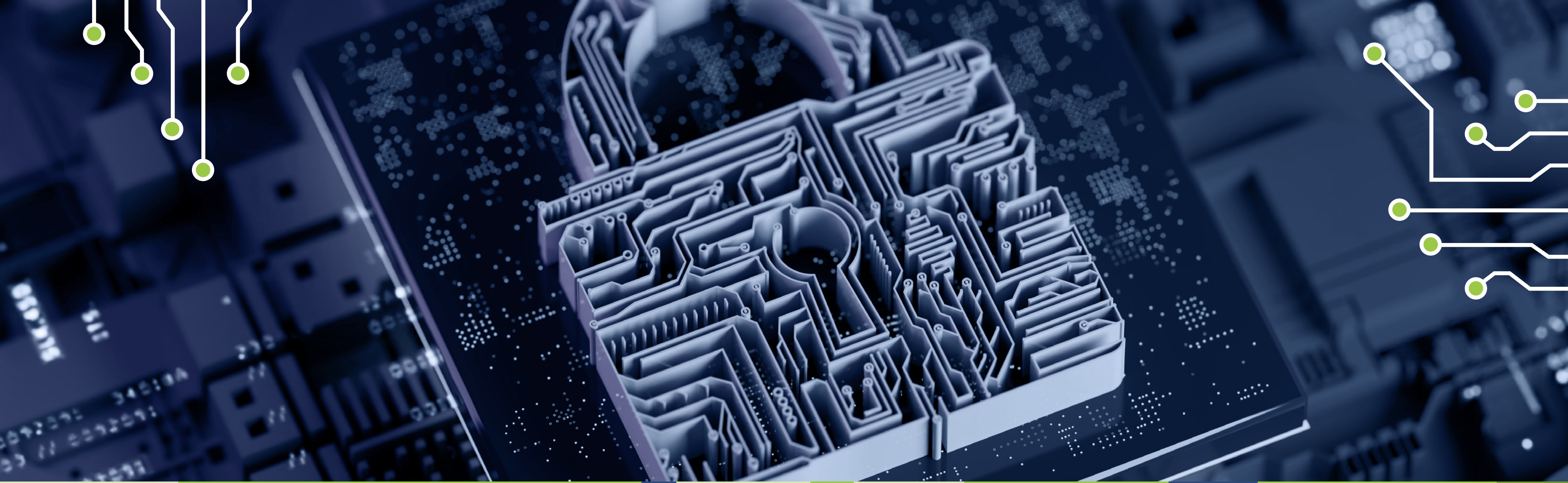
Trellix was formed by the merger of McAfee and FireEye. With its capabilities in data discovery, content-aware protection, and unified centralised reporting, it offers a robust DLP functionality. DLP is a core component of MVISION Unified Cloud Edge, which converges CASB, DLP, and web technologies to help businesses protect data.

Trend Micro

Trend Micro is primarily recognised for its ability to integrate and the ease of deployment and application of its DLP solutions, strengths which are made more effective through its partner network in the UK.

Proofpoint

Proofpoint's integrated DLP solution with threat management offers visibility into the threat landscape, along with broad alert coverage through pre-defined libraries. In 2021, it acquired Dathena (AI-powered data protection) and InteliSecure (DLP managed services). It witnessed significant growth through its product bundling programme. This makes the company a Rising Star.



Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)

Who Should Read This

This report is relevant to enterprises across industries in the U.K. for evaluating providers that offer solutions that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant, ISG focuses on the current market positioning of providers offering advanced endpoint security products to enterprises in the U.K., and how each provider addresses the key challenges faced in the region.

Endpoint devices are points of vulnerability, allowing attacks to reach the network. With advanced endpoint security, enterprises can seal off attack points, giving organisations valuable protection.

Endpoint threat detection combines real-time monitoring, automated responses and analytical capabilities to prevent attacks. Technologies such as AI, machine learning, security analytics and real-time threat intelligence go a step further to identify potential or complex threats.

Due to lack of skilled personnel to maintain standard security measures, small and midsize enterprises are increasingly being targeted by determined threat actors. With end point security, security operations personnel can obtain a consolidated view of suspicious behaviour across an enterprise through the use of various security tools.

Chief information security officers should read this report because it presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats, the capabilities needed to combat them, and assists in making the related strategic business decisions.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security service providers in the U.K. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to comprehend the changing security landscape. In addition to setting strategic objectives and adopting security platforms in accordance with their needs.

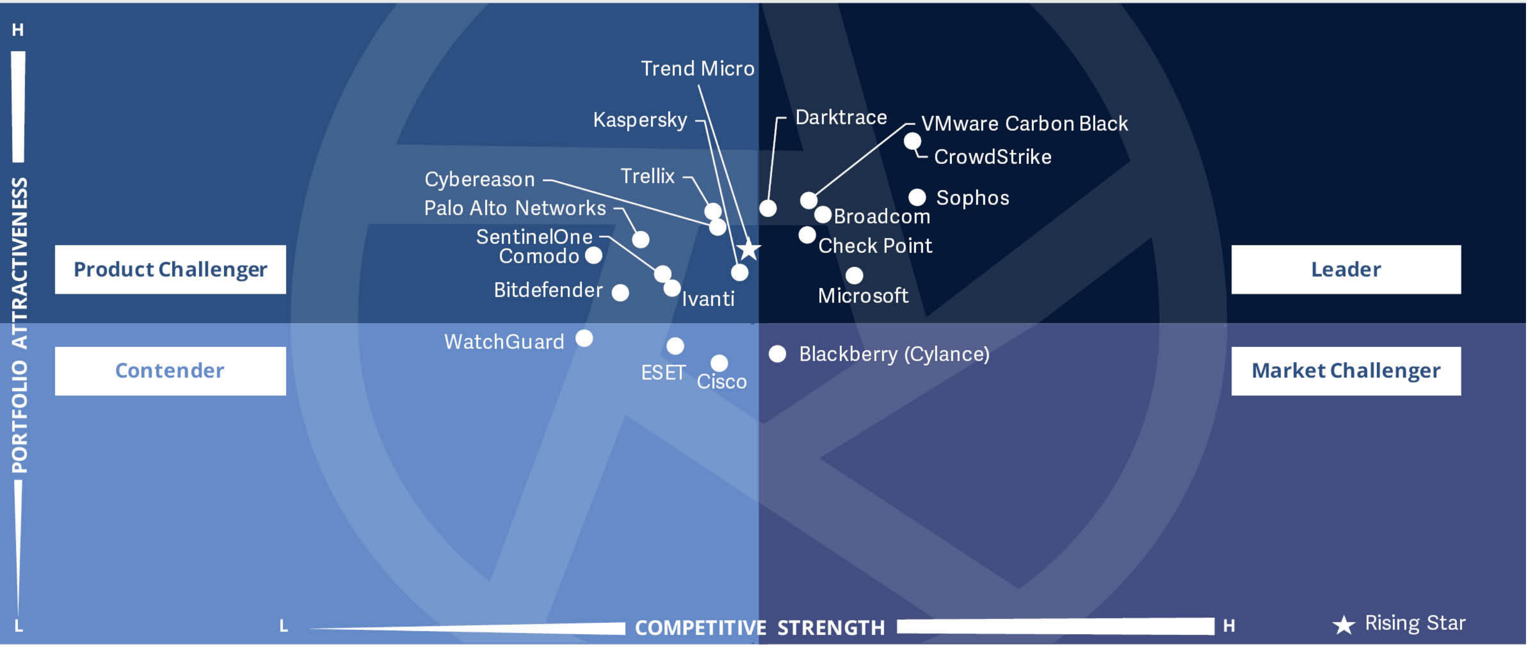
ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity - Solutions and Services

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

U.K. 2022



This quadrant assesses the providers of advanced endpoint threat protection, detection, and response software that can provide **continuous monitoring and total visibility of all endpoints and can analyse, prevent, and respond to advanced threats.**

Arun Kumar Singh

Definition

Advanced ETPDR vendors and solution providers are characterised by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. Pure service providers that do not offer an advanced ETPDR product (on-premises or cloud-based) based on proprietary software are not included here. This quadrant evaluates providers offering products that can provide continuous monitoring and complete visibility of all endpoints and can analyse, prevent, and respond to advanced threats. Endpoint security solutions that integrate secure access service edge (SASE) are also included here.

In our consideration, endpoint security also includes the corresponding protection of operational technology (OT) solutions. These solutions go beyond plain, signature-based protection and encompass protection from risks such as ransomware, advanced persistent threats (APTs) and malware by investigating the incidents across the complete endpoint landscape. The solution should be able to isolate the compromised endpoint and take the necessary corrective action or remediation. Such solutions comprise a database, wherein the information collected from a network and endpoints is aggregated, analysed, and investigated, and the agent that resides in the host system offers the monitoring and reporting capabilities for the events.

Eligibility Criteria

1. The solution provides comprehensive and **total coverage and visibility of all endpoints in a network.**
2. The solution demonstrates **effectiveness in blocking sophisticated threats** such as advanced persistent threats, ransomware, and malware.
3. The solution **leverages threat intelligence and analyses and offers real-time insights on threats** emanating across endpoints.
4. The solution **includes automated response features** that include, but are not limited to, deleting malicious files, sandboxing, ending suspicious processes, isolating infected endpoints, and blocking suspicious accounts.

Observations

AETDR software is designed to help organisations proactively detect malicious activities and trigger quick and appropriate responses. AETDR tools help in detecting incidents, confirming, and prioritising risks, and preventing attacks on IT infrastructure. These tools store telemetry data, such as endpoint-system-level behaviours and events (for example, file, registry, process, memory, and network events). The AETDR market is seeing a surge in demand due to an increase in the uniqueness of cyber threat techniques and the cyber threat landscape.

With the deployment of ADETR tools, organisations are looking to increase their visibility into endpoint events and reduce threat detection and response times. Cloud-based ADETR tools are seeing higher demand from organisations compared to on-premises solutions, as enterprises adopt the policy of work from anywhere and anytime due to the COVID-19 pandemic.

ISG has observed that endpoint threat detection and response tool providers are increasingly offering managed detection and response services to help organisations (especially from the SMB segment) that are struggling to handle and interpret complex telemetry data-laced alerts and have a security talent shortage. These providers are increasingly partnering with MSSPs and pureplay MDR service providers to compete in the market. In turn, MSSPs are building automated response and remediation capabilities around endpoint threat detection and response tools to cater to clients' requirements.

From the 95 companies assessed in this study, 20 have qualified for this quadrant, with seven being Leaders and one Rising Star

Broadcom

Broadcom utilises Symantec's platform to protect all traditional and mobile endpoint devices for on-premises, hybrid, and cloud-based solutions. It provides advanced endpoint protection, pre-attack, and attack surface reduction, breach prevention, and response and remediation functionality. It is supported by a broad network of partners in the UK.

Check Point Software

Check Point Software's Harmony Endpoint security portfolio offers data security, network security, advanced threat prevention, forensics, EDR, and remote access VPN through a single management console**.**

CrowdStrike

CrowdStrike is a publicly traded firm and offers Falcon endpoint protection, SaaS-based workload security, endpoint security, threat intelligence, incident response, and cyberattack response. The company enhanced its log management capabilities by acquiring Humio in 2021. It also acquired SecureCircle to improve its data protection capabilities by extending ZT security.

Darktrace

Darktrace went public in 2021. It offers a unique self-learning-AI-based endpoint security product that can disrupt any ongoing cyberattacks, such as ransomware, in split seconds.

Microsoft

Microsoft offers advanced EDR solutions under the Windows Defender brand. It can be easily managed by Microsoft's security centre console, which is integrated into the complete enterprise Microsoft environment.

Sophos

Sophos offers a series of endpoint security solutions integrated with Sophos Central to businesses of different sizes. It is supported by SophosLabs and leverages deep learning, which extended detection and response (XDR) capabilities strong, and addresses key security threats such as ransomware.

VMware Carbon Black

VMware Carbon Black offers an endpoint and workload security platform that leverages big data and analytics capabilities to help customers build proactive risk posture. Its cloud-based offering consolidates multiple endpoint security features to help customers investigate and prevent threats.

Trend Micro

Trend Micro is a Rising Star, considering its growth in the UK market. It offers the Apex One endpoint security platform with extended detection and response capabilities.

Technical Security Services

Who Should Read This

This report is designed to help companies, across industries in the U.K., evaluate providers that are not exclusively focused on their respective proprietary products, but can implement and integrate other vendors' products or solutions. This report covers integration and implementation of IT security services.

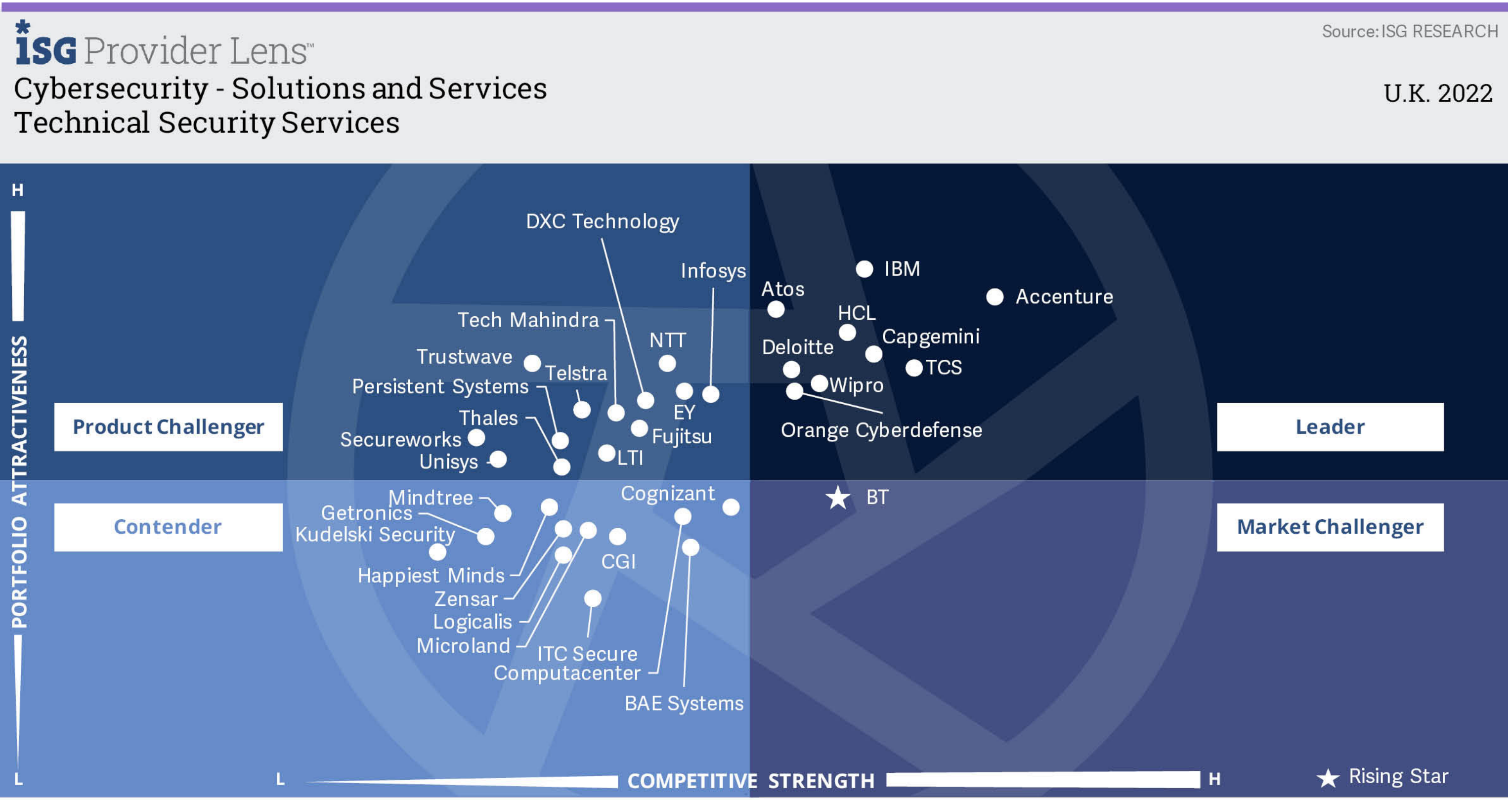
In this quadrant, ISG defines the current market positioning of providers of technical security services, offering implementation and integration services, and highlights how each provider addresses the key challenges in the U.K. With these services, organisations can defend themselves against cyberattacks and respond swiftly to threats that intending to access and misuse their sensitive information.

In this context, the key implementation or integration tasks include ransomware and malware protection. Considering the volatile security landscape, technical security services are in high demand in the U.K. compared with other European countries. However, each enterprise customer has their own priorities in terms of frameworks, security and scalability. Both enterprises and providers face challenges during the process of implementing technical security solutions. Therefore, enterprises prefer service providers with a talented workforce, expansive capabilities and a global presence.

Chief information security officers should read this report because, with digital transformation at the forefront of businesses today, they need find a balance between data security, customer experience and privacy. They need to have a thorough understanding of the leading service providers in the market that assist with integrating IT security services, and they need deep insights on providers' capabilities.

Chief strategy officers should read this report to understand the relative positioning and capabilities of service providers and collaborate with them to develop an effective cyber security service. This report contains information that can be used to implement a security solution.

Security analysts should read this report to understand how providers adhere to the security and data protection laws in the U.K., to stay abreast with market trends and to prepare themselves to utilise all available services.



This quadrant assesses the technical security service providers **offering integration, maintenance, and support services** for IT security products or solutions.

Arun Kumar Singh

Definition

TSS covers integration, maintenance, and support for both IT and operational technology (OT) security products or solutions. DevSecOps services are also included here. TSS addresses all security products, including anti-virus, cloud and data centre security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, and SASE. This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.

Eligibility Criteria

1. Demonstrate **experience in implementing cybersecurity solutions** for companies in the respective country.
2. Authorised by security technology vendors (hardware and software) **to distribute and support security solutions.**
3. Providers should **employ certified experts** (vendor-sponsored, association- and organisation-led credentials, government agencies) capable of supporting security technologies.

Observations

According to Trend Micro Research's Zero Day Initiative™ (ZDI), 2021 had the most zero-day exploits, and 1,604 vulnerabilities were detected (a 10 percent increase compared to 2020). Malicious actors use unique techniques to exploit the patch gaps in a system. Organisations are implementing the security-as-a-service model in their existing and new IT infrastructure. The consumption-based model pushes organisations to shift from their perimeter-based approach to user- and application-based security models, which is a time-consuming and resource-intensive task.

There is a growing trend of CIOs and DevOps teams working together to build "security by design" into their products throughout the development and operation cycles to address zero-day vulnerabilities. DevSecOps helps organisations build a security-aware mindset compared to offering a set of rules and tools. With DevSecOps, development teams are keeping security as a priority in the initial design and development phase.

The convergence of IT and OT environments challenges IT teams to manage the OT infrastructure. In pursuit of efficiency and connectivity, IT-OT convergence expands the attack surface, enabling malicious actors to take advantage of vulnerabilities and increases risks.

Common IT-OT security concerns that organisations face include a lack of in-house security expertise, access to sensitive information, connected smart devices, the inability to contain and isolate breaches, and the rising regulatory pressure for ICS/SCADA.

From the 95 companies assessed in this study, 35 have qualified for this quadrant, with nine being Leaders and one Rising Star.

accenture

Accenture's large partnership ecosystem, strong technical domain understanding, cyber labs, and threat intelligence expertise make it a leading player in the TSS domain.

Atos

Atos leverages its proprietary AIsaac® cloud-ready AI platform for deep detection and a faster response time. It also has a strong partner base to deliver integration services.

Capgemini

Capgemini's strengths lie in its diverse portfolio of technical security services. It also offers tool expertise for integration, maintenance, and support, and the ability to manage scale across implementation and integration engagements.

Deloitte

Deloitte has comprehensive customised solutions, thought leadership in cybersecurity, and a large partner base, making it a dominant TSS player.

HCL

HCL has a well-established practice, backed by a large pool of skilled cybersecurity professionals. It has a strong innovation roadmap and strategic partnerships with OEMs.

IBM

IBM's global presence, partnership ecosystem, and ability to offer scalable integration and technological leadership give it a leading position in this domain.

Orange Cyberdefense

Orange Cyberdefense takes an intelligence-led approach to cybersecurity. The company has invested significantly in innovation and holds numerous certifications and partnerships.

TCS offers a wide integration portfolio of cybersecurity services. It has a strong focus on resource development and innovation through alliances with leading security players.

Wipro has developed homegrown frameworks for identity, data privacy, risk governance, and vulnerability management. The company focuses on strengthening its ties with partners and offers a spectrum of technical security services.

BT

BT is expanding its presence in the UK and executing its TechCo transformation strategy. It leverages its telco experience to serve its cybersecurity customer base. In July 2021, it invested in SAFE security to improve their trust scores. It is identified as a Rising Star in this domain.

Strategic Security Services

Who Should Read This

This report is relevant to enterprises across industries in the U.K for evaluating providers offering services that integrate multiple features that address cybersecurity concerns arising from changes in work patterns and increased digitalisation.

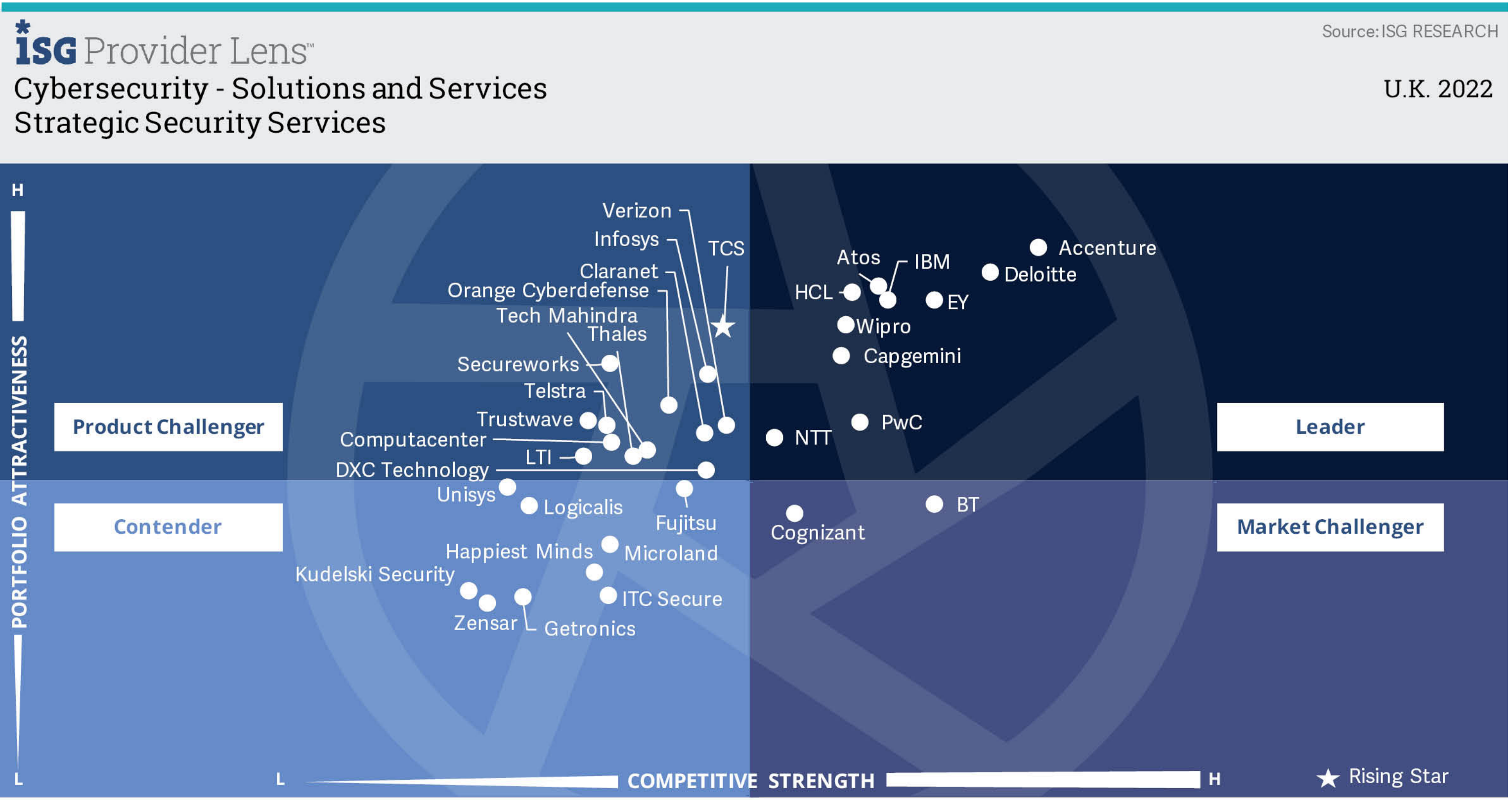
In this quadrant, ISG focuses on the current market positioning of strategic security service providers that reduce security threats for enterprises in the U.K., and how each provider addresses the key challenges in the market.

Strategic security services help organisations build security programs that are relevant to the needs of the business and have a lasting impact. The demand for strategic security services is rising in the U.K. with companies seeking them as an add-on to management services or technical services. To meet enterprise needs, strategic service providers are building up their capabilities by hiring industry experts and acquiring consulting firms.

Chief information security officers should read this report because it presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats and the capabilities needed to combat them, and it assists in making strategic business decisions. This report provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to stay apace with the changing security landscape. In addition to setting strategic objectives and developing security platforms in accordance with marketing needs.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of strategic security service providers in the U.K. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.



ISG Provider Lens™

Cybersecurity - Solutions and Services
Strategic Security Services

Source: ISG RESEARCH

U.K. 2022

This quadrant assesses strategic security service (SSS) providers **offering security audits, compliance and risk advisory services, security services, security assessments, security solution architecture consulting, and awareness and training services.**

Arun Kumar Singh

Definition

Strategic security services primarily cover consulting for IT and OT security. Services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategy for enterprises (tailored to specific requirements). This quadrant examines service providers that do not exclusively focus on proprietary products or solutions. The services analysed here cover all security technologies, especially OT security and SASE.

Eligibility Criteria

1. Service providers should demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, architecture consulting, and risk advisory.**
2. Service providers should offer at least one of the above strategic security services in the respective country.
3. Execution of security **consulting services using frameworks** will be an advantage.
4. **No exclusive focus on proprietary products** or solutions.

Observations

The COVID-19 pandemic had a tremendous impact on how organisations engaged with security services providers. Customers and security consulting partners were able to collaborate remotely to engage over outcome-based and risk-sharing pricing models in exchange of value delivery. However, SSS providers are very cautious in fully adopting these pricing models, considering a significant impact on their revenue streams. At the same time, customers' procurement teams find it more challenging to compare service providers. ISG believes that customers and service providers must come together to build a customised outcome-based or risk-sharing pricing model that suits their requirements.

The pandemic made a dent on innovation-related initiatives across industries. Organisations should be demanding strategic security services providers develop and/or collaborate to create unique and impactful IP.

There is a growing trend of establishing and expanding consulting capabilities around secure edge secure access (SASE), OT security, and zero trust. To leverage the growing benefits of SASE, customers are engaging in a consulting-led approach to understand SASE and its impact on architecture (including integration, identifying gaps and overlaps, and key technologies), identify and evaluate SASE solution vendors, and slide into the design and implementation phase.

Customers continue to get confused because SASE vendors are creating noise around providing full-scale SASE solutions, whereas no single vendor has a complete SASE solution. This is where SSS providers are leveraging their existing vendor relationships and helping the customers with successful SASE framework implementation.

From the 95 companies assessed for this study, 34 have qualified for this quadrant, with ten being Leaders and one a Rising Star.

accenture

Accenture has a presence in the security-led strategy, risk, and advisory services space, with strong capabilities to address enterprises' SSS requirements. In 2021, Accenture acquired Sweden-based Sentor to expand its MSS and security consulting services.

Atos

Atos is known for its broad services portfolio and understanding of emerging technologies. With its large ecosystem of partners and broad services range, it is a leading company in the UK for SSS. In 2021 it acquired Motiv to strengthen its MSS and SOC capabilities by adding more than 180 cybersecurity experts.

Capgemini

Capgemini has a strong base of skilled resources, coupled with evolving security consulting expertise and a focus on strategic security advisory.

Deloitte

Deloitte offers UK-based enterprises a balanced mix of technical, strategic, and risk-based cybersecurity solutions, backed by its extensive strategic consulting and risk advisory expertise. In 2021, Deloitte acquired various cybersecurity providers to add technologies around industrial cybersecurity, zero trust network access, digital risk protection, cloud security posture management, and threat hunting.

Ernst & Young (EY)

Ernst & Young (EY) provides a wide range of cybersecurity services along with strong GRC and audit capabilities, making it one of the leading providers in the SSS market.

HCL

HCL will be rebranding its security consulting division to Fortius. It offers a mix of proprietary assets along with innovation and cost-efficient delivery to reduce the risk posture of enterprises in the UK.

IBM

IBM leads in security and related strategy areas with its technical proficiency in AI, services-led frameworks, and innovative technologies. In 2021, IBM acquired ReaQta for threat detection and response capabilities.

NTT

NTT leverages innovative, proprietary tools along with a threat-intelligence-driven approach and platform. These are backed by a strong partner network to deliver strategic transformation services in the region.

PwC

PwC has a well-established advisory and consulting practice. It also has extensive M&A expertise and a network of cybersecurity facilities to deliver SSS. It is establishing a cybersecurity hub in Cardiff.

wipro

Wipro has a strategic focus on cybersecurity services, demonstrated through investments in developing proprietary assets and expanding dedicated resource bases. In 2021 Wipro acquired Edgile to develop the Wipro CyberTransform™ platform to improve governance, invest in security strategies, and deliver value. It also acquired Capco to strengthen its BFSI sector security consulting.

tcs TATA CONSULTANCY SERVICES

TCS witnessed 3X growth in security deals in 2021 and expects further growth. It provides a wide range of cloud-based platforms, such as the Cyber Vigilance platform, the threat intelligence platform, Identifence™, and a consent management solution to deliver SSS. It is identified as a Rising Star in this domain.

Managed Security Services – Large Accounts

Who Should Read This Section

This report is relevant to enterprises across industries in the U.K for evaluating providers offering services that integrate multiple cybersecurity features, addressing security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant, ISG focuses on the current market positioning of managed security service providers that mitigate security threats for enterprises in the U.K., and how each provider addresses the key challenges in the market.

Security issues are taking a toll on enterprises, with new threats emerging continuously, requiring smart ways to improve security postures and manage related concerns. Enterprises are currently harnessing the latest developments in the security space to drive efficiency and effectiveness and mitigate risks.

The managed security services market in the U.K. is characterised by the increasing adoption of secure access service edge (SASE) and zero-trust networks in response to the growth in cyber threats. Over the last year, enterprises have increased their demand for cloud/DevSecOps security, cloud-based security operations centeres, and IoT/OT security to protect valuable data and resources. However, the high growth prospects of the managed security services market are adversely impacted by the shortage of skilled professionals and budget constraints faced bysmall and midsize enterprises in the region.

Chief information security officers should read this report because it report presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats, the capabilities needed to combat them, and assists in making the related strategic business decisions.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to comprehend the changing security landscape. In addition to setting strategic objectives and adopting security platforms in accordance with their needs.

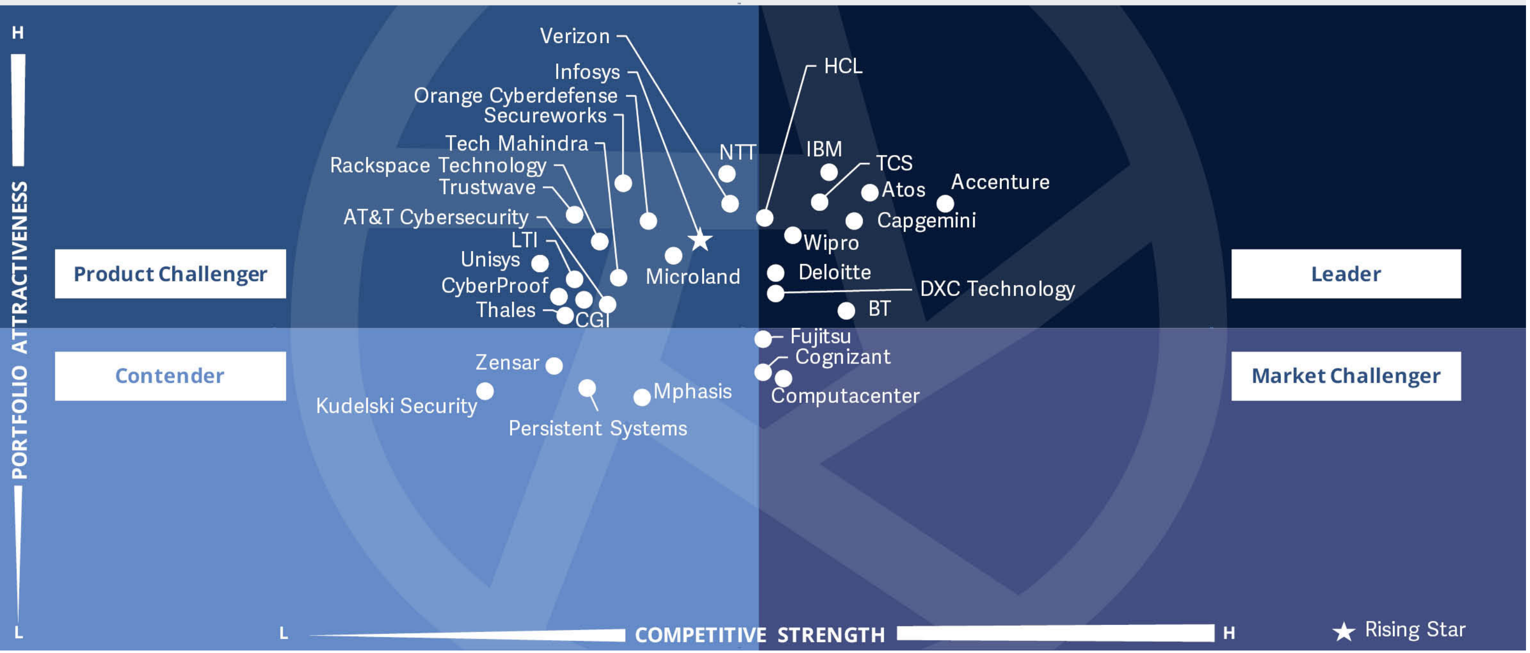
Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security service providers in the U.K. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity - Solutions and Services
Managed Security Services - Large Accounts

U.K. 2022



This quadrant assesses the providers of MSS that **comprise the operations and management of IT security infrastructure** for one or several clients by a security operations centre (SOC).

Arun Kumar Singh

Definition

MSS comprises the operations and management of IT and OT security infrastructure for one or several customers by a security operations centre. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.

Eligibility Criteria

1. Typical services include security monitoring, behaviour analysis, unauthorised access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations, and all other operating services to **provide ongoing, real-time protection, without compromising business performance.** In particular, secure access service edge (SASE) is also included.
2. Ability to **provide security services such as detection and prevention; security information and event management (SIEM); and security advisor and auditing support,** remotely or at the client site.
3. Possesses **accreditations** from vendors of security tools.
4. SOCs are **ideally owned and managed by the provider** and not predominantly by partners.
5. **Maintains certified staff,** for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Global Information Assurance Certification (GIAC).

Observations

MSS experienced growth in the UK across all organisation sizes, mainly due to the COVID-19 pandemic driving the adoption of the work-from-anywhere policies, an increase in cyber threats' 3Vs (volume, velocity, and variety), increased multicloud and hybrid cloud environments, and a security talent shortage.

Organisations are adopting the zero trust (ZT) model to strengthen IT infrastructure. While adopting this model, organisations are engaging with providers through consulting/advisory services, and slowly scale to implementation and managed support services.

MSSPs increasingly partner with extended detection and response (XDR) and EDR tool vendors to develop managed detection and response (MDR) services. This helps customers have a proactive and resilient approach toward threats and prevent the lateral movement of cybercriminals within their IT infrastructures. MSSPs are also building their technical and managed services expertise to help customers understand, plan, and implement the SASE framework.

Global MSSPs acquaint themselves with diverse European cultures and languages, build localised capabilities, and establish local/regional data centres and SOCs to align with the UK's data residency compliances and local regulations.

ISG witnesses a rapid expansion of Microsoft's Intelligent Security Association members and partner ecosystem for the sell-in of the Sentinel offering as part of broader Microsoft 365 E5 licensing. MSSPs are investing in resources and offerings to build Sentinel-focused practices even though pricing is an issue, especially for midmarket companies.

From the 95 companies assessed in this study, 32 have qualified for this quadrant, with 10 being Leaders and one Rising Star.

accenture

Accenture's strengths lie in its management consulting background, research-focused approach, and strong partner ecosystem. It expanded its MSS capabilities by acquiring Sweden-based Sentor.

Atos

Atos differentiates itself with the proprietary AI-driven AIsaac® platform, intelligence-led SOCs, and flexible delivery models for MSS. Atos acquired four security companies: Cloudreach (specialising in cloud application development and cloud migration), CV Cryptovision (advanced cryptographic products), In Fidem (cybersecurity consulting), and Motiv ICT security (MSS).

BT

BT is expanding in the UK and implementing its TechCo transformation strategy. It has 16 accredited global SoCs. It uses its telco experience to serve its cybersecurity customers. In July 2021, BT invested in SAFE security to use risk and predictive breach intelligence to help customers improve their trust scores.

Capgemini

Capgemini's strengths lie in its dedicated network of cyber defence centres (CDCs), flexible delivery model, and advanced threat hunting capabilities. It is investing in Europe by expanding partnerships, adding SASE solutions, and providing pricing flexibility.

Deloitte

Deloitte is a global consultancy firms with a thought leadership focus, 24/7 threat monitoring services, customised delivery capabilities, and strong acquisition strategies. It acquired five security businesses: aeCyberSolutions (industrial cybersecurity), TransientX (cloud-native application networking), Terbium Labs (digital risk protection tool), CloudQuest (cloud security posture management), and Root9B (cyber threat hunting).

DXC Technology

DXC Technology has a large base of skilled employees, a network of SOCs, and the DXC Security Platform, along with a wide range of services.

HCL

HCL takes a 360-degree approach to cybersecurity, with its MSS and consulting expertise. It delivers services through a series of frameworks, a network of cybersecurity fusion centres, and a large partnership network.

IBM

IBM leads in terms of applications, infrastructure, and acquisitions, and offers a research-led portfolio of cybersecurity services. It acquired ReaQta to add to its threat intelligence, detection, and response capabilities. It is a Level 1 AWS MSSP Competency Partner.

tcs TATA CONSULTANCY SERVICES

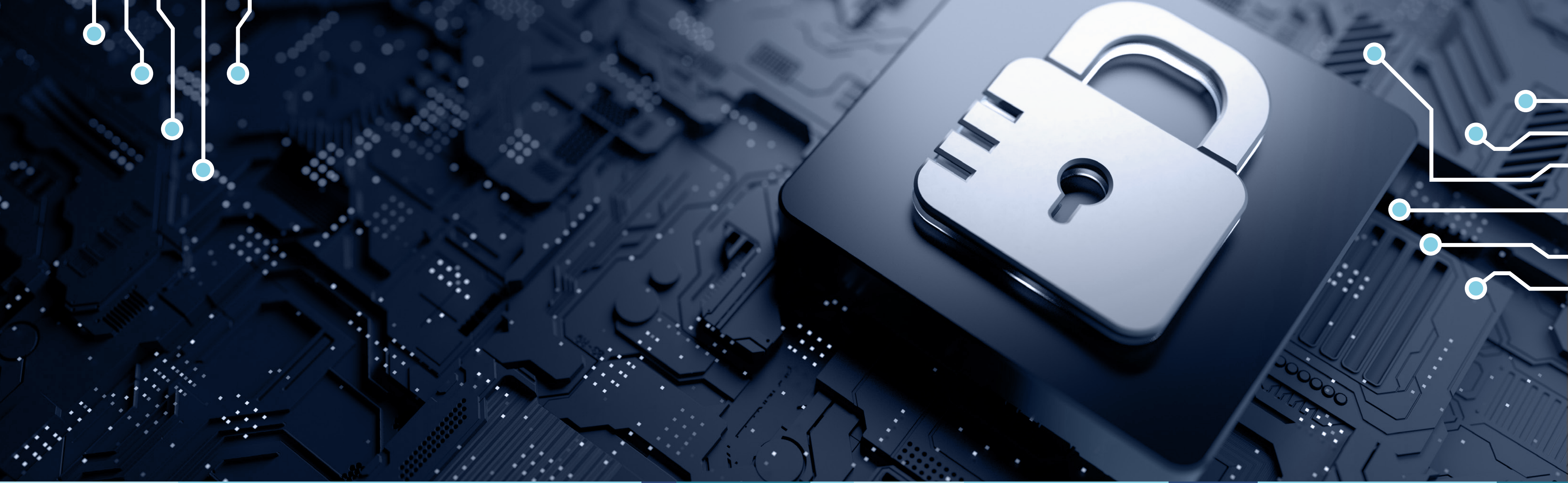
TCS has launched a series of SOC automation initiatives and has many unique proprietary assets for MDR, IAM, vulnerability management, and SOCs. It showcases its leadership through a network of 12 threat management centres, 200 SOCs, and IP-driven delivery for clients. TCS reports tremendous growth in its security deals pipeline.

wipro

Wipro's MSS portfolio combines HOLMES™-led SOC automation, a cyber defence platform, and analytics capabilities. It expanded its consulting capabilities by acquiring Edgile and Ampion. Wipro will be investing £16 million to set up an innovation centre in London. Cybersecurity startups remain a key focus area for Wipro Ventures.

Infosys

Infosys (Rising Star) offers a flexible MSS model that empowers organisations with people, processes, and technology to secure their critical assets and data. It is identified as a Rising Star in this domain.



Managed Security Services – Midmarket

Who Should Read This

This report is relevant to enterprises across industries in the U.K for evaluating providers offering services that integrate multiple cybersecurity features, addressing security concerns arising from changes in work patterns and increased digitalisation

In this quadrant, ISG focuses on the current market positioning of managed security service providers that mitigate security threats for enterprises in the U.K, and how each provider addresses the key challenges in the market.

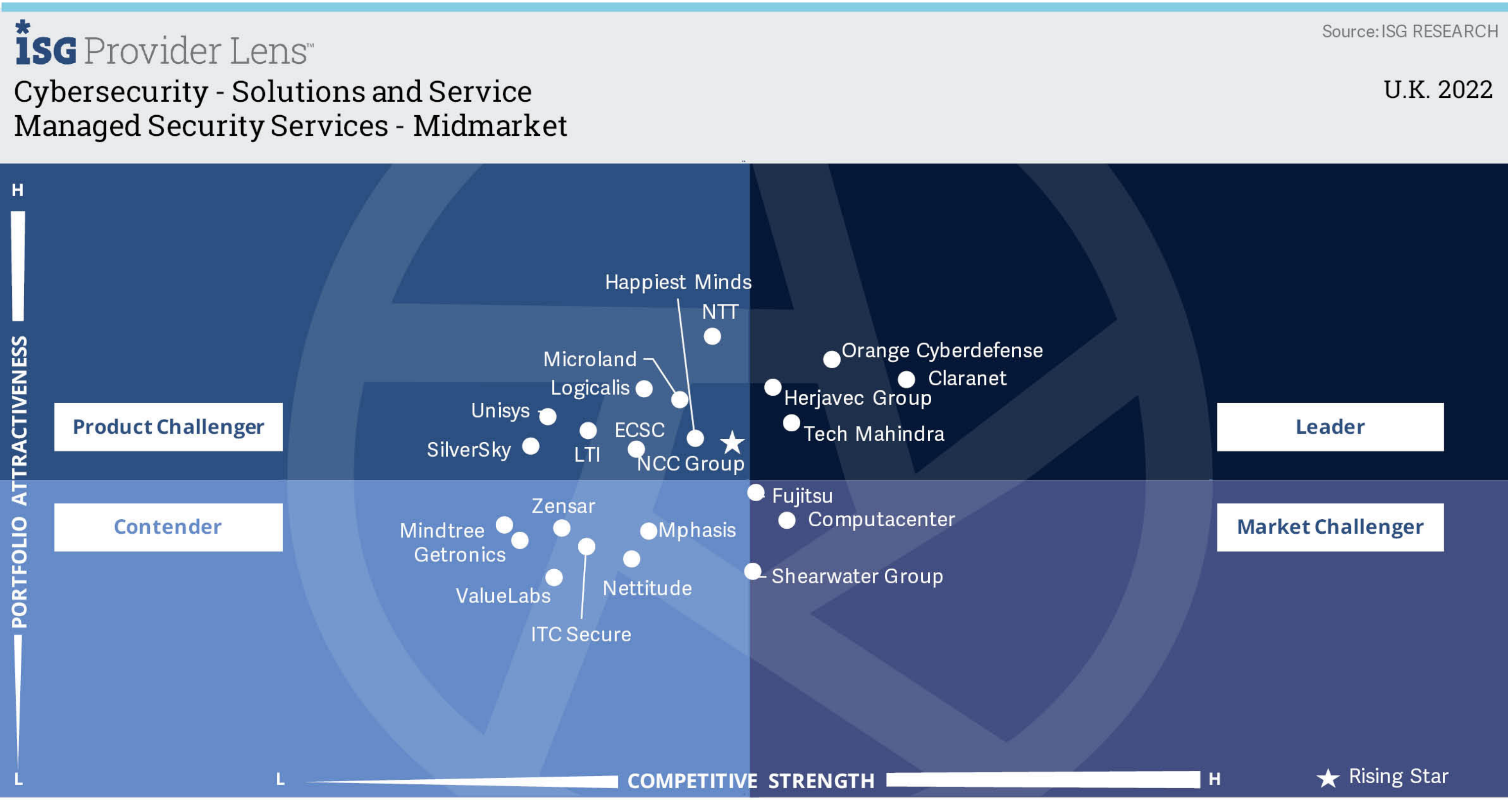
Unlike a few years ago, midmarket companies now are taking measures to adapt their services to respond to threats and cyber attacks, which are more debilitating for them. Phishing and malware attacks were the most common attacks before the pandemic. In the last two years, with the acceleration of digital transformation, midsize companies are unable to protect themselves with their current resources, budgets and expertise.

Over the last year, enterprises have increased their demand for cloud/DevSecOps security, cloud-based security operations centres, and IoT/OT security to protect valuable data and resources. However, the high growth prospects of the managed security services market are adversely impacted by the shortage of skilled professionals and budget constraints faced bysmall and midsize enterprises in the region.

Chief information security officers should read this report because it presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats and the capabilities needed to combat them, and it assists in making the related strategic business decisions. This report provides valuable insights on enhancing productivity and reducing complexity of enterprise security operations.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to comprehend the changing security landscape. In addition to setting strategic objectives and adopting security platforms in accordance with their needs.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security service providers in the U.K. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.



Cybersecurity - Solutions and Service
Managed Security Services - Midmarket

U.K. 2022

Source: ISG RESEARCH

This quadrant assesses the providers of managed security services (MSS) that **comprise the operations and management of IT security infrastructure for one or several clients by an SOC.**

Arun Kumar Singh

Definition

MSS comprises the operations and management of IT and OT security infrastructure for one or several customers by an SOC. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.

Eligibility Criteria

1. Typical services include security monitoring, behaviour analysis, unauthorised access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations, and all other operating services to provide ongoing, real-time **protection, without compromising business performance.** In particular, SASE is also included.
2. Ability to provide security services such as **detection and prevention, security information and event management (SIEM), and security advisory and auditing support,** remotely or at the client site.
3. Possesses **accreditations** from vendors of security tools.
4. SOCs **ideally owned and managed by the provider** and not predominantly by partners.
5. **Maintains certified staff,** for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

Observations

As midmarket organisations are expanding their presence and challenging their enterprise counterparts, their technology footprints are also expanding, with limited IT budgets and a low focus on securing the business and customers. Recently, for malicious actors, midmarket businesses have prime targets, as they are mostly underserved by cybersecurity solution and service providers.

Cybersecurity solution providers are engaging with the midmarket segment by leveraging remote selling strategies and creating subscription-basis pricing for tier-based security packages.

MSSPs are taking a similar approach where they are offering virtual CISO capabilities to help midmarket businesses plan, design, and implement the required components of security infrastructure. Besides, MSSPs handle procurement and manage security technologies and offer them on the basis of the per-seat or consumption-based model. To justify the ROI, MSSPs can provide KPIs indicating the number of threats prevented/mitigated, mean time to detect (MTTD), mean time to resolve (MTTR), peer comparisons, etc.

ISG has witnessed another emerging trend among midmarket-segment players; they are aligning their MSS around hyperscalers such as AWS and Microsoft. Google remains behind in terms of engaging the MSP community to address cloud security challenges.

From the 95 companies assessed for this study, 22 have qualified for this quadrant, with four being Leaders and one Rising Star.

claranet

Claranet envisions to be an end-to-end security services provider in the midmarket to help in implementing the "security by design" approach. With local presence, it has MSS offerings supported by certified analysts and partnerships. It is aligning its managed services with AWS and Microsoft and expanding its development team.

Herjavec Group

Herjavec Group offers 24/7 MSS certified for SOC 2 Type 2 and enabled by technical and human intelligence, AI remote SOC operations, and threat intelligence expertise. In 2021, Herjavec Group was merged with Fishtech Group, adding managed detection and response services to its MSS portfolio.

Orange Cyberdefense

Orange Cyberdefense's strength is its extensive base of proprietary assets, most of which are developed in-house. The company takes an intelligence-led approach to security, backed by a strong base of certified analysts.

Tech Mahindra

Tech Mahindra offers SOC 2 Type 2-compliant SOCs as a service, and managed network and endpoint security services. It plans to achieve $500 million cybersecurity revenue by 2025 and to be a top MSSP by developing cybersecurity offerings and intellectual property by leveraging alliances. It plans to expand its security team and customer accounts.

NCC Group

NCC Group (Rising Star) offers broad MSS, covering security information and even management (SIEM), managed detection and response (MDR), and extended detection and response (XDR) with strong global partnerships. In 2021 it invested £3 million to launch a new remediation proposition. It supports 58 Fortune 500 and 85 FTSE 350 clients.

Claranet

Leader

“Claranet has a quantitative risk-based approach to offer MSS, with local expertise.”

Arun Kumar Singh

Overview

Claranet is headquartered in London and has a strong global footprint, with more than 2,500 employees to serve over 10,000 clients. It has more than 20 years of experience in cybersecurity and training. Its MSS offering covers four key areas: MDR, endpoint detection and response, continuous testing services and managed firewalls, and network and denial of service (DoS) protection. Its MSS portfolio witnessed strong growth in 2021 and is expected to grow by 20 percent in the next year.

Strengths

Expanding portfolio and sales function: In 2021, Claranet expanded its portfolio by adding a range of managed services around AWS and Azure Sentinel. It has launched the CST penetration testing portal and cloud and ransomware risk assessment services. It is investing in expanding sales and business development functions to drive new businesses and inbound leads.

Certification-led expertise: Claranet is one of only 12 companies worldwide that have attained the CREST accreditation for SOCs. Its SOC staff have BSc, MSc, and SANS certifications, plus Azure certifications. It is working toward CREST certifications for analyst training.

Partnership with key vendors: Claranet has been recognised as one of the six Level 1 MSSP AWS Partners in Europe and achieved managed MDR on Azure Sentinel. Through these partnerships, the company offers a strong technology-backed portfolio of MSS to enterprises.

SOC automation: Claranet has invested in a security operations centre in the UK to offer next-generation SIEM services, endpoint protection, and network traffic analysis by leveraging the capabilities of AWS, AT&T, SentinelOne, and Lacework.

Caution

Claranet should expand its focus on verticals other than finance, retail, and technology.

Appendix

The ISG Provider Lens 2022 – Cybersecurity — Solutions and Services 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

Lead Author:
Arun Kumar Singh

Editors:
Dona George, John Burnell

Research Analyst:
Monica K

Data Analyst:
Rajesh Chillappagari

Consultant Advisor:
Doug Saylors

Project Manager:
Ridam Bhattacharjee

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 programmes, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of June 2022, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The study was divided into the following steps:

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

Author & Editor Biographies

Lead Author

Arun Kumar Singh

Senior Manager and Principal Analyst

Arun is principal analyst and senior research manager at ISG Research. He has more than 16 years of experience as a technology analyst and advisor with strong product strategy, industry research, and consulting skills. He has worked closely with multiple stakeholders in the technology domain delivering projects around product development and strategy, go-to-market strategy, patent (intellectual property) research, competitive intelligence, and M&A advisory. He has published multiple research studies on enterprise applications, security, and managed workplace services. Based out of ISG's Bengaluru office, Arun is responsible for delivering the ISG Provider Lens studies on Cybersecurity Solutions and Services and the Oracle ecosystem for the UK and Nordics regions. He regularly writes about the latest cybersecurity industry trends and works closely with ISG advisors to deliver on ad-hoc research requirements related to market, competitive intelligence, location analysis.

Research Analyst

Monica K

Research Specialist

Monica K is a research specialist and a digital expert at ISG. She supports and co-authoring Provider Lens studies on the Internet of Things (IoT), digital business transformation, blockchain, enterprise application as a service, and cybersecurity. She has created content for the aforementioned Provider Lens studies, as well as content from an enterprise perspective, and she is the author of the global summary report. Monica K brings more than eight years of experience and expertise in technology, business, and market research for ISG clients. Prior to ISG, Monica worked for a research firm specialising in technologies such as IoT and product engineering, as well as vendor profiling and talent intelligence. She has also been in charge of delivering end-to-end research projects and collaborating with internal stakeholders on various consulting projects.

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 analysing 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.

About Our Company & Research

ISG Provider Lens™

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

ISG Research™

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

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

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ISG Provider Lens™

JULY 2022

REPORT: CYBERSECURITY — SOLUTIONS AND SERVICES