ISG Provider Lens™

Cybersecurity – Solutions and Services

Managed Security Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

Infosys®

QUADRANT REPORT | JUNE 2023 | EUROPE

Table of Contents

Managed Security Services - SOC (Large Accounts) – U. K.

Report Author: Arun Kumar Singh

Cyber resiliency and data sovereignty are the two key themes integral to U.K. enterprises.

U.K. – Continuous push to become cyber power

Following the COVID-19 outbreak, businesses' digital transformation needs evolved and experienced an increase in cloud adoption, which peaked during the pandemic. The widespread demand for hybrid work culture led to rise in cyberattacks and sowed uncertainty among business decision-makers. Due to an expanded attack surface, it is now challenging for security experts to monitor strategic initiatives essential for business success while still protecting and securing IT infrastructure and applications.

To bolster vulnerability management, cloud, email and endpoint security, enterprises will be fighting and expanding their cybersecurity budget to invest in tools and frameworks such as zero trust, XDR and automated threat intelligence in the coming years. According to a CyberEdge report, the average security spending as a percentage of an enterprise's IT budget is approximately 11.3 percent in the U.K.

In 2020, the U.K. lost its leadership position in International Telecommunication Union (ITU) Global Cybersecurity Index to the U.S.. Although it had improved its cybersecurity capabilities, the U.K. lost on technical measures and capabilities to detect and respond to cyberattacks. The evaluation also factored in its heavy reliance on foreign-manufactured telecom and IT infrastructure hardware.

According to MIT Technology Review, which ranks the top 20 economies based on their cybersecurity assets, cyber resiliency practices, organisational capabilities and policy commitment to promote a secure and digital economy, the U.K. is ranked at the seventh position. Adopting a *whole of society* approach to implement its cybersecurity strategy, the U.K. government has created a Cyber Security Advisory Board to incorporate perspectives from industry and academia.

Cybersecurity is becoming **a business enabler** and a **key differentiator for enterprises' GTM strategy.**

The current National Cyber Strategy 2022 stands on major progress collectively achieved by 1,838 U.K. cybersecurity businesses (product and service providers, resellers and managed security service providers (MSSPs) contributing £10.1 billion (14 percent growth) in revenue last year, with 52,727 skilled jobs and foreign investments.

According to the Digital Economic Council, U.K.'s technology sector continues to move ahead of U.S. and China with excellence in science and technology to create a value-led innovation ecosystem in the wake of the global recession. In 2022, U.K. tech enterprises raised £24 billion compared to their neighbours, such as France (£11.8 billion) and Germany (£9.1 billion).

U.K. cybersecurity startups – Advancing through a tumultuous phase

According to Crunchbase, U.K.'s cybersecurity sector stood fourth in securing funding from VCs. In 2021, global investors invested £1.01 billion in 84 deals in the U.K. cybersecurity sector. Select few startups and product-based companies, vis-à-vis service providers, with a proven growth record secured most funding. Investors kept their hands tightly clenched while spending on early-stage startups despite the relevance and soaring support from the U.K. government.

However, during this period, the U.K. cybersecurity sector was heavily crowded, making high visibility, strong sales and marketing crucial.

Most cybersecurity businesses are based in London and the Southeast regions. There is a growing demand for security consulting services, especially from organisations pursuing digital transformation efforts to improve and develop sustainable and secure infrastructure. Regionally, London remains the sweet spot for global investors and cybersecurity talent seekers. However, other hubs are rising in Gloucestershire, Belfast, Wales, Scotland and Manchester.

Cost of data breach

According to IBM Security, the average total cost of a data breach reached $5.05 million in 2022. The cost of a data breach in the U.K. jumped to 8.1 percent. The average total cost of a data breach in the U.K. continues to climb, bagging fourth place globally, beating France, Japan and Germany.

According to the Sophos State of Ransomware Report, the average cost of a data breach for U.K. organisations was $1.08 million. However, this is still a substantial decrease from the $1.96 million reported in 2021.

Unforgiving and expanding threat landscape

State-sponsored attacks peaked in 2022, primarily dominated by the Ukraine-Russia war, followed by China, Iran and North Korea. According to the Department for Culture, Media and Sport (DCMS), of the U.K. businesses that identified a cyberattack, 83 percent of enterprises were targeted by a phishing attempt, making this the most common threat vector. About a fifth (21 percent) reported more sophisticated attack types, including denial of service, malware or ransomware attacks.

Despite its low prevalence, many U.K. enterprises still consider ransomware a major threat. The National Cyber Security Centre (NCSC) continues to see increased use of ransomware as a service (RaaS), where ransomware variants are leased to less-skilled affiliates that can launch cyberattacks without building the ransomware themselves. However, 56 percent of enterprises have implemented policies and frameworks to prevent paying for ransomware attacks.

Cloud security threats, IT-OT threats and ransomware attacks will continue to haunt U.K. enterprises, encouraging leader personas, such as CEO, CISO, CIO, CTO, CDO (chief digital officer) and CRO (chief risk officer), to collaborate and respond to take a proactive stance against cyber threats. According to State of Malware, a Malwarebytes report, enterprises should be wary of five types of common malware families frequently leveraged by the cybercrime ecosystem worth billions of dollars. These include LockBit ransomware, Emotet botnet, SocGholish drive-by download, Android droppers and macOS Genio adware.

U.K. IT decision makers see ChatGPT's potential (ability to write malicious source code and phishing emails and detect vulnerabilities and social engineering attacks) to be used for malicious purposes in cyberspace.

With the growing proliferation and easy accessibility of commercial cybersecurity technologies, the threat landscape in the U.K. and worldwide will continue to expand. In the future, the vast and complex cybersecurity tools landscape leveraged by cyber adversaries will include off-the-shelf cyber surveillance products and supporting services, the vulnerability and exploit marketplace, hackers-for-hire services and publicly available malware. These tools continue to lower the entry barrier for cyber adversaries to extort U.K. enterprises.

Data sovereignty compliance

The U.K.'s exit from Brexit in January 2020 demanded more collaboration between the country, the European Union (EU) Europol and ENISA, the EU's cybersecurity agency. This pushed the U.K. to evaluate its future cybersecurity approach to continue collaboration (including cybersecurity-related trade) with the EU or take a contract approach to open the door to opportunities in the global marketplace at the risk of sacrificing existing relationships (and trade) with the EU.

Data sovereignty is a top priority for national government regulators. Ongoing trends such as hybrid workforce and dynamic compliance landscape are reshaping enterprises looking at data privacy laws and protecting themselves from probable financial fines for not complying with data sovereignty regulations such as GDPR (£18M or 4 percent of annual revenue — whichever is greater), PCI-DSS ($5,000-$10,000 per month), HIPAA ($50-$50,000 per record) and GLBA (up to $100,000 per violation).

U.K.'s National Cyber Strategy 2022 emphasises data sovereignty to identify and catalogue critical information and control where the data is stored. However, when data is migrated to the cloud, this control is often lost, exposing organisations to significant gaps in data governance. As a result, organisations that fail to meet regulatory frameworks may be fined.

U.K. business challenges and priorities

Based on ISG advisors' interaction with enterprise leaders, it is evident that business leaders are concerned and cautious about high inflation, continued geopolitical tensions and rise in cost of living in 2023. They are decisive about increasing strategic investments around talent (upskilling, recruitment and retention) and technology for business transformation, new business models and achieving long-term growth. These investments would help U.K. business leaders to stay ahead of the competition, tackle industry challenges and create long-term value.

U.K. business leaders struggle to take a holistic approach to cyber threats, which includes a better understanding and visibility of all the network assets (especially container-based applications and SaaS deployed at large scale and faster pace), the associated risks they face and running business operations amid simultaneous risks. They are still focused on isolated risk scenarios and recovery plans instead of taking a proactive and preventive approach that embeds resilience capabilities to withstand disruption.

Onboarding new technologies and applications with frequent update release cadences and imposing rigorous pen-testing and red teaming on the source code are challenges for the internal security team of U.K. businesses.

Lastly, businesses need help to onboard experienced cybersecurity talent and retain them in the current market conditions where talent shortage has become an industry-wide challenge.

U.K. businesses can easily leverage the following:

1. Leadership influence to drive changes and reduce barriers to C-level collaboration
2. Analytics to improve threat detection and risk identification for a proactive stance toward cyber threats
3. Employee awareness of cyber risks and implications

CISO's key priorities in 2023

In 2022, the U.K. cybersecurity market experienced challenges with delayed cybersecurity budget spending. Managed security service providers expect clients to be continually cautious with rising economic and market volatility concerns in 2023. ISG expects the U.K. cybersecurity industry to grow flat or record negligible growth over 2022 while keeping its undeterred focus on protecting the industry from cyber adversaries. U.K. industries are expected to prioritise their IT spending

on zero trust, network security and cloud security (with a surge in demand for cloud migration services).

In 2023, we expect the below key CISO priorities for U.K. enterprises of prime importance:

- **Maintain a secure hybrid workplace environment:** The COVID-19 pandemic pushed enterprises to devise new policies to adopt hybrid workforce culture. This imparts tremendous pressure on security teams to ensure secure remote work infrastructure and invest in their talent to secure the system.
- **Cybersecurity enabling digital transformation initiatives:** Businesses continue to invest in their digital transformation efforts by adopting cloud, IoT, analytics and other enabling technologies to drive business value and improve customer experience. Security leaders are expected to become enablers of these business efforts to keep security a part of technology evaluation, design, implementation and support and contribute to innovation and organisational growth.
- **Comply with regulatory changes and industry compliances:** Security leaders are expected to stay on top of the ever-expanding regulatory and compliance requirements to fulfil governance and audit purposes.
- **Invest in advanced cybersecurity technologies:** With the growing availability of cyber tools among cyber adversaries, it becomes imperative for enterprises to leverage zero trust architecture, AI-based cybersecurity and quantum computing.
- **Security by design:** DevSecOps adoption will offer a cultural and mindset change to identify vulnerabilities in the early stages to create secure applications.

Enterprises struggling to transform cybersecurity into cyber resilience

Cybersecurity listed as a fairly high priority for the board members of U.K. enterprises. Enterprises are investing in identifying cyber risks and leveraging advanced technologies to proactively monitor threats and prevent breaches. However, when boardroom members allocate and approve the budget, the narrative lacks clarity around RoI. Boardroom members have a limited understanding of cyber risks and depend on external advisors such as third-party providers, cyber insurance providers and internal subject matter experts to manage threats.

U.K. cyber insurance still evolving

The Ukraine-Russia war is fuelling cyber threat (IT systems interruptions, data breaches and ransomware or cyber extortion) fear among U.K. enterprises, prompting them to look for cyber insurance as an option to stay protected or comply with U.K. government regulations.

According to the U.K. Department for Culture, Media, and Sport (DCMS), only 43 percent of U.K. businesses have an insurance policy that protects them against cyber risks. Further, only a tiny fraction (5 percent) of these enterprises has specific cyber policies catered to their needs. Most companies with cyber protection benefit from coverage within more general policies. Some U.K. businesses took insurance as it was necessary to comply with accreditations such as Cyber Essentials or ISO 27001. According to the European Union Agency for Cybersecurity (ENISA), coverage in case of an incident is the driving reason to purchase cyber insurance. Requirements by law and pre-incident and post-incident coverage are other lesser significant reasons. Businesses that did not have insurance were interested in various types of coverage, including business continuity, expert support during an incident and ransomware coverage.

According to Marsh's Q3 2022 pricing index, cyber insurance pricing increased 66 percent in the third quarter, following a peak increase of 102 percent year-over-year in the first quarter of 2022. The rise is faster in the U.K. than in any other regional market. According to ENISA, U.K. enterprises consider cyber insurance less attractive due to increasing prices and decreasing coverage. Some challenges that the U.K. cyber insurance industry face include:

- Lack of incident-related data impacting the cyber risks involved and proper insurance coverage
- Lack of formalised cyber risk quantification services adoption is low

- Frequent change in risk profile due to new systems being added, and obsolete ones being removed
- High mean time to detect (MTTD) any breach within the enterprise network

Widening cybersecurity skill gap

According to Harvey Nash Group's study, U.K.'s cyber skills shortage has surged by over a third in the past 12 months, and cybersecurity is the leading tech skill required in the U.K.. The U.K. cybersecurity sector is expected to attract approximately 10,500 people annually to meet new demands and lost talent. The U.K. government is collaborating with academic institutions to provide more than 130 masters programs in cybersecurity to develop the talent pipeline. The U.K. enterprises are set to increase security budgets for security staffing and employee training.

Zero trust (ZT) adoption

The U.K. government has accelerated its efforts in adopting digital services across ministries, from modernising the welfare system or legal system and improving citizen services to deliver efficiency and better citizen experience. However, this would require a high level of integration of systems and generate digital data, which would lead to an increase in cyberthreat surfaces.

Last year, NCSC published a strategic guidance document for the public sector and large businesses in the U.K. to implement their own zero trust security model. U.K. businesses are still in the early stage of adopting the zero trust security model. They will continue to face cultural barriers, impacting budget provisioning in coming years, if not for the longer term.

ISG expects U.K. enterprises to increase their security budgets for zero trust strategies and initiatives while facing challenges in addressing talent shortage, improving awareness and investing in new cybersecurity technologies implementation. U.K. enterprises in financial services and healthcare sectors are heading towards adopting zero trust architectures.

OT devices, such as industrial control, hospital monitoring and water management systems, are lagging in adopting and implementing cybersecurity standards. Some ZT security elements, such as network segmentation, SIEM, SOAR, endpoint detection and response and multifactor authentication (MFA), are crucial for mitigating IT and OT vulnerabilities.

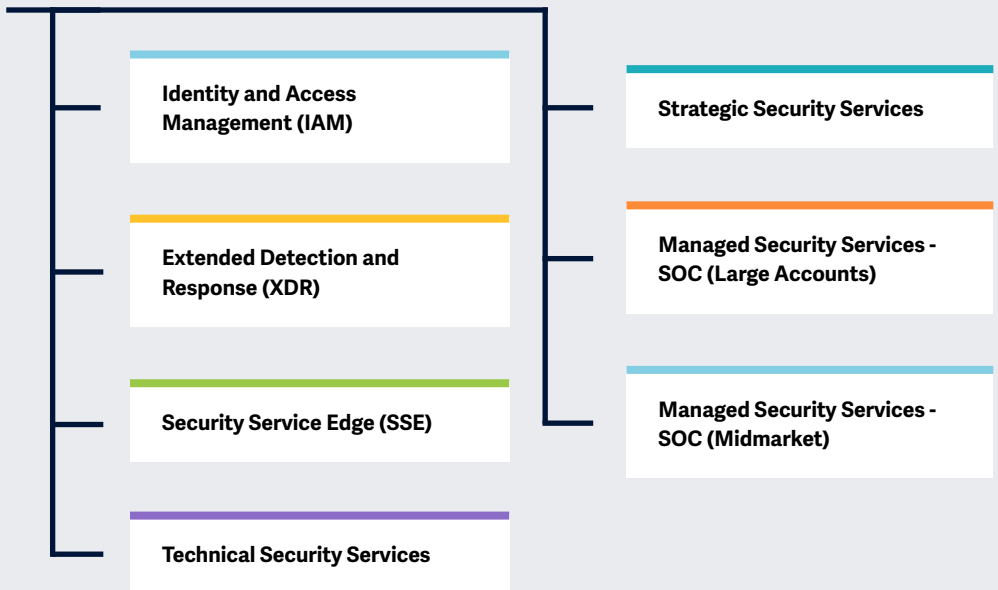
AI and automation in cybersecurity

AI and automation are critical tools in the cybersecurity industry to mitigate security threats, gather threat intelligence and detection and alert triage leveraging ML and advanced analytics. However, the industry continues to face talent shortage to develop, maintain and operate AI and automation tools for cybersecurity functions. These drive managed security service providers and managed service providers to invest in AI and automation tools to support their clients, offering immense opportunities to tap into.

Cyber resilience is the second of the five pillars of the U.K. National Cyber Strategy 2022-2030. The U.K. government has invested heavily in building and improving cyber resilience through NCSC and implementing NIS regulations, GDPR and Data Protection Act 2018. The strategy targets to make businesses, public services and critical national infrastructure more resilient and reduce cyber risks with more effective cybersecurity actions.

Key focus areas for **Cybersecurity Solutions and Services** 2023

Simplified Illustration; Source: ISG 2023



Definition

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritised relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

From an enterprise perspective, even small businesses understood the impact of cyber threats and realised that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident. Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

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

Scope of the Report

In this ISG Provider Lens™ quadrant report, ISG covers the following 6 (number of quadrants) quadrants for services/solutions: Identity and Access Management (IAM), Extended Detection and Response (XDR), Security Service Edge (SSE), Technical Security Services (TSS), Strategic Security Services (SSS) and Managed Security Services - SOC.

Vendors offering Security Service Edge (SSE) solutions are analyzed and positioned from a global perspective, rather than by individual regions, as the market is yet in the early stages of maturity.

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

- Transparency on the strengths and weaknesses of relevant providers/software vendors
- A differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on different markets, including the U.S., the U.K., Nordics, Germany, Switzerland, France, Brazil, Australia, Singapore & Malaysia, and the US public sector. The SSE topic will be analysed for the global market.

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

Provider Classifications

The provider position reflects the suitability of IT 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 $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have 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).

Who Should Read This Section

This report is relevant to enterprises across industries in the U.K. for evaluating providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. This report covers the operations and management of IT and OT security services.

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.

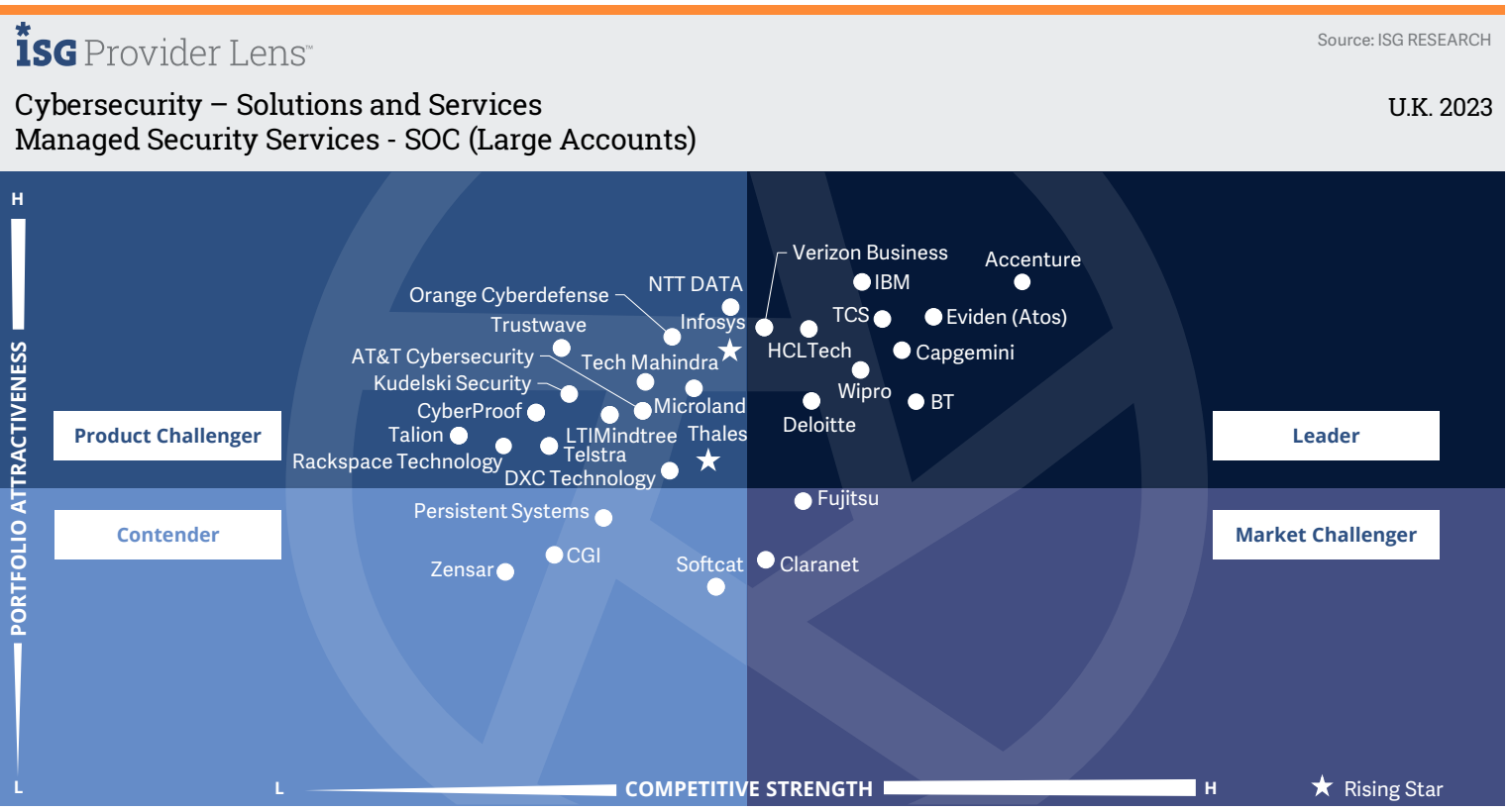
In this data-driven era, enterprises are keeping themselves updated with the transforming taxonomy of cyberattacks. Businesses are harnessing the power of AI and ML platforms to detect and respond to the bottleneck of a cyberattack rapidly. Large enterprises are on the lookout for providers with integrated toolsets capabilities such as anomaly detection, incident risk prediction, early threat identification, and incident filtering that decreases the Mean time to detection & response (MTTD & MTTR) through the use of advanced AI/ML.

As data loss due to the modern threat of ransomware and other pervasive attacks poses significant disruption and financial loss, enterprises are pivoting towards regaining access to mission-critical applications swiftly post-cyberattacks. Enterprises Many enterprises in the U.K. are transitioning from detection and response to recovery strategy in security operations centres (SOCs) and expect security providers to offer heightened cyber threat preparedness and build a cyber-resilient framework.

Cybersecurity professionals should read this report as it showcases emerging trends and immediate threats. It aids in strategic decision-making, enhancing productivity and reducing security complexity.

Technology professionals should read this report as it highlights emerging trends, insights into tailored security platforms and strategic objectives to keep pace with the changing security landscape.

For **business professionals**, it's a must-read report as it gives valuable insights into simplifying security operations. It offers practical solutions for reducing complexity and enhancing efficiency.



This quadrant examines service providers that are not exclusively focused on proprietary products. They can **manage and operate the best-of-breed security tools and handle the security incident lifecycle**, from identification to resolution.

Arun Kumar Singh

Definition

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

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximising the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS (SOC) providers must combine traditional managed security services with innovation to fortify their clients with an integrated cyber defence mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies, infrastructure and experts skilled in threat hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs should support expert-driven security intelligence response, while offering clients a holistic and unified approach to advanced-level security.

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 on business performance. In particular, secure access service edge (SASE) is 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 a client's site
3. Possesses **accreditations** from security tools vendors
4. **SOCs ideally owned and managed by the provider** and not predominantly by partners
5. Maintains **certified staff**, for example, with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Global Information Assurance Certification (GIAC)

Rising Star

"Infosys stands out in MSS through its as-a-service packaged security offerings powered by Cyber Next."

Arun Kumar Singh

Infosys

Overview

Infosys is headquartered in Bengaluru, India and operates in 54 countries. It has more than 346,800 employees across 247 global offices. In FY22 the company generated $16.3 billion in revenue, with financial services as its largest segment. Infosys' integrated managed protection, detection, and response(MPDR) solution was built with the Cyber Next platform and security controls. It has multiple platforms, such as Cyber Gaze, Cyber Hunt, Cyber Compass and Cyber Central. Infosys has been recognised as AWS Security Competency Partner for showcasing its technical expertise around AWS and cloud security.

Strengths

Partner ecosystem: Infosys has strategic partnerships with more than 25 leading partners that help them build joint solutions and go-to-market plans. Its partnerships with academic institutions, both national and international, allow it to develop and nurture talent at scale.

Underlying automation: The company's dedicated automation team helps build use cases, bots and accelerators. It has built more than 100 reusable use cases spanning across IAM, infrastructure security and data security, more than 200 reusable bots, automation platforms (Infosys IPs) for identity operations and infrastructure operations and support for SOX governance, patch management and vulnerability management.

Continuous innovation:
Infosys cybersecurity, along with Infosys Centre for Emerging Technology Solutions (ICETS), constantly innovates, validates and launches new solutions to enable customers to be risk resilient.

Cybersecurity CoE: Infosys' CoE develops capability and capacity to enable business growth by competency development via trainings and academic collaborations, partner-led certifications, solution labs, and automation for delivery excellence.

Caution

Infosys is heavily dependent on clientele in the BFSI and retail sectors. It should slowly consider expanding its presence in other verticals in the U.K.

The company must continue to invest in local talent and business development.

Managed Security Services - SOC – Germany

Report Author: Frank Heuer

Current crises and the SME segment are driving the German cybersecurity market

Currently, companies are facing various challenges in terms of cybersecurity. Increased cyberthreats due to the Ukraine war, the upheavals caused by the COVID-19 pandemic, which have been overcome, and the long-term trend of digitization have created vulnerabilities for cyberattacks in Germany, requiring appropriate countermeasures. On the other hand, the weakened economy presents further financial challenges.

As businesses undergo digital transformation, more processes are being shifted to IT. Digital representation of intellectual corporate property is also increasing. Protecting IT and communication systems has become essential for corporate security. The COVID-19 crisis has further heightened the need for IT security, as remote work and external connectivity of employees have increased the susceptibility of IT systems to attack. With remote work likley to continue even after the pandemic, this challenge will persist.

> The shortage of skilled workers is driving the demand for external cybersecurity service providers in Germany.

The increased use of cloud resources, hybrid work and the vulnerability it brings to IT systems have emphasized the relevance of the zero-trust approach. The principle of *never trust, always verify* means, among other things, mutual authentication and continuous network monitoring.

Cybercriminals are developing new, sophisticated and complex methods to bypass companies' and authorities' cyber defense systems at shorter intervals than ever. In the past year, there have been notable cyberattacks, including ransomware attacks, causing significant trouble for businesses. Accordingly, cybersecurity measures must be seamlessly up to date. More companies and public authorities

Cybersecurity challenges are increasing for businesses in various ways.

are struggling with this, particularly due to the shortage of IT specialists, especially in the cybersecurity market. As a result, IT managers and executives are increasingly turning to external service providers, such as managed security service providers, that employ proactive rather than reactive methods based on AI to safeguard against such threats.

Cybersecurity providers seeking above-average growth in Germany should prioritize the needs of SMEs and effectively communicate with this segment.

In addition to the company's own protection, legal regulations such as the General Data Protection Regulation (GDPR) in the EU also require companies to implement stronger security measures to prevent cyberattacks. Compliance with these regulations remains a major challenge for midsize companies in particular.

On the other hand, SMEs present an interesting market segment for cybersecurity providers. As they upgrade their less mature IT security systems, as compared to large enterprises, driven by the factors described above, there is an above-average growth in the demand for cybersecurity solutions among SMEs. Having a balanced customer structure for both midsize and large companies is advantageous for providers to leverage the budgets of large accounts. Despite the economic slowdown, the demand for cybersecurity solutions remains unaffected among SMEs, making it an increasingly attractive market segment and the one that needs to be addressed adequately. The services meant for large customers cannot simply be offered to SMEs. Rather providers should tailor their entire go-to-market strategy, including products, prices and communication, to suit the needs of SMEs. Providers must understand that communication and cultural aspects are particularly important to be accepted by SMEs.

Despite the great importance of cybersecurity, IT managers are increasingly struggling with justifying IT security investments to stakeholders, especially the CFOs. Unlike other IT projects, it is not always easy to prove the return on investment or quantify threat risks. However, executives are increasingly aware that cyberattacks can lead to significant financial and reputational damage. Consequently, cybersecurity is gaining importance within companies, and senior management is becoming more involved in cyber risk management.

Furthermore, technical factors alone do not contribute to the vulnerability of IT systems. Careless user behavior, such as falling victim to Trojan and phishing attacks, play a key role in facilitating cyberattacks. Therefore, in addition to updated security equipment, user training and consulting also play an important role.

Looking ahead, there are future technical threats to consider, such as quantum-based attacks that target the encryption of confidential data. Some service providers have already started adapting their consulting services to address this new challenge.

Identity and Access Management (IAM)

In terms of cybersecurity topics, IAM holds significant importance, especially with the increasing digitalization of all areas and the need to protect not only users but also machines and certain areas within companies, such as Industry 4.0.

The growing number of users, devices and services necessitates effective management of digital identities, especially considering the rise in remote work due to the pandemic. Many employees are accessing corporate resources remotely, making regulation and control of access to data and systems even more important.

Data Leakage/Loss Prevention (DLP) and Data Security

DLP solutions have witnessed increasing demand in Germany in the recent past due to various factors affecting data security within organizations. The importance of data, IP and corporate assets has significantly increased, making protection against unwanted data leaks, especially from private end devices used for business purposes, a major challenge for companies.

Extended Threat Detection and Response (XDR)

XDR solutions have gained prominence and traction over the past two years as organizations aim to better understand and contextualize (correlate) information gathered from various security tools deployed in their IT infrastructure. Automation plays a central role in this, and leading providers offer behavioral and contextual analytics modules, as well as open integration with other endpoint and network detection and response products.

Security Service Edge (SSE)

SSE solutions are still in the early stages of maturity and adoption by enterprises. SSE includes solutions that enable enterprises to securely access the cloud, facilitate remote work, secure edge computing and support digital transformation. The increasing number of remote and hybrid workers and the transition to the cloud have created the need for SSE solutions.

Strategic Security Services

Amidst the acute crises arising from the Ukraine war and the effects of the COVID-19 pandemic, companies in Germany are facing several challenges concerning IT security and data protection. The growing threat landscape and resource scarcity create a greater need for orientation.

As cyberattacks become more intense and sophisticated, companies must protect their IT systems from damage. This challenge extends beyond well-known large companies and public authorities to small and midsize companies. However, the shortage of IT specialists further complicates this situation, especially for midsize companies. The midmarket is thus a segment that is growing at an above-average rate and is consequently becoming increasingly attractive.

Technical Security Services

In the face of increasingly sophisticated cyberattacks and a shortage of skilled workers, companies and public authorities in Germany are relying more on external service providers to keep their IT security systems up to date.

Cybercriminals are taking advantage of careless user behavior, and thus incidents of Trojan, phishing and ransomware attacks are becoming more common. Along with having updated security equipment, user training continues to play an important role.

IT security projects are often demanding and multifaceted, so service providers that offer a wide range of technical security services from a single source have an advantage here.

Managed Security Services (SOC)

The increasing frequency and complexity of cyberattacks, along with the challenges posed by the current crises, have created a demand for managed security services in particular. The scarcity of qualified resources and the need for updated specialist knowledge are driving German companies to focus on these services.

> Managed security services providers rely on AI and automation to combat cyberattacks, but human expertise remains indispensable.

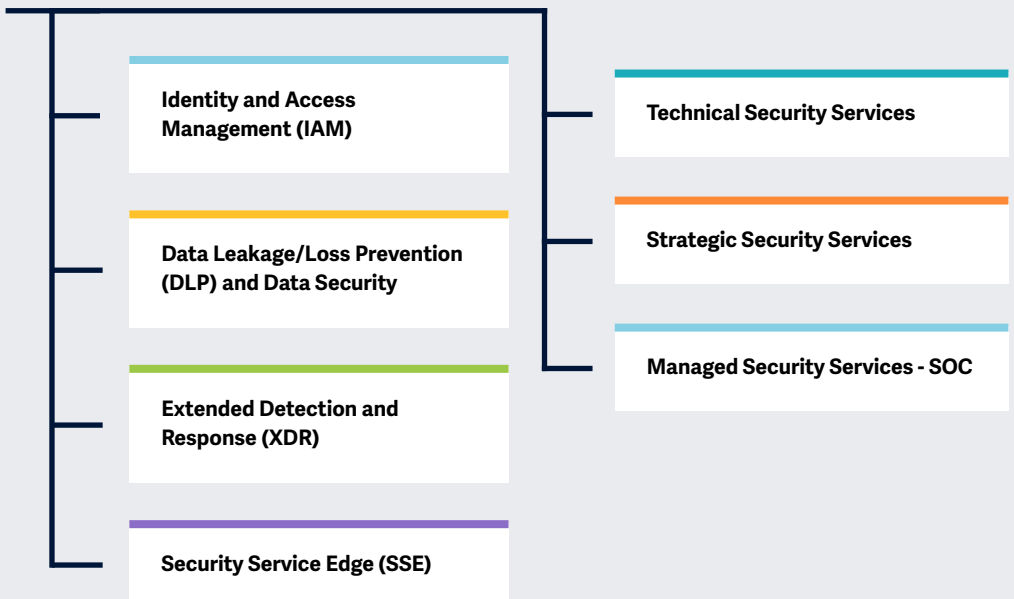
Both large and midsize customers prefer SOCs located in Germany due to the increasing importance of data protection. End-to-end security services, integrated solutions comprising IT and related security solutions, and innovation are crucial for staying ahead of cybercriminals.

Managed security services providers are increasingly using AI and automation to combat cyberthreats, combining machine efficiency with human expertise.

> In the future, cybersecurity service providers must equip their customers to defend against quantum-based attacks.

Focus areas of the **Cybersecurity – Solutions & Services** 2023 study.

Simplified Illustration Source: ISG 2023



Definition

From a cybersecurity perspective, 2022 could be described as turbulent; despite declining data breaches, attacks this year were significantly more sophisticated and severe. In 2022, companies increased their investment in cybersecurity and placed a high priority on corresponding initiatives to prevent attacks and improve their security posture. They had learned their lesson from the 2021 attacks; executives and companies of all sizes and industries invested accordingly in measures to respond to and weather cybersecurity threats and cyberattacks.

Even small businesses are now aware of the dangers posed by cyberthreats and have realized that they are actively targeted and highly vulnerable to cyberattacks. This has increased the need for (managed) security services and cyber resiliency services that enable companies to quickly resume operations after a cyber incident. Service providers and vendors are therefore offering services and solutions to support recovery and business continuity.

Cybercriminals exploited major vulnerabilities such as Log4shell and continued to disrupt business activities with ransomware; the healthcare, supply chain, and public sectors were particularly targeted.

Enterprises responded by investing in capabilities such as identity and access management (IAM), data loss prevention (DLP), managed detection & response (MDR), and securing the cloud and endpoints. The market is shifting toward integrated solutions such as Security Service Edge (SSE) and Extended Detection & Response (XDR); using best-of-breed tools, staff expertise, and complementary behavioral and contextual intelligence and automation to improve security posture.

Scope of the Report

In this ISG Provider Lens™ Quadrant Report, ISG covers the following seven quadrants for services/solutions: Identity and Access Management (IAM), Data Leakage/Loss Prevention (DLP) and Data Security, Extended Detection and Response (XDR), Security Service Edge (SSE) , Strategic Security Services, Technical Security Services, Managed Security Services - SOC. Security Service Edge (SSE) solution providers are initially analyzed and positioned from a global perspective in this year's study, rather than from the perspective of individual countries and regions, as the market is currently still in its early stages and maturing process.

The ISG Provider Lens™ study Cybersecurity - Solutions and Services 2023 offers business and IT decision makers the following benefits:

- Transparent presentation of the strengths and weaknesses of relevant providers
- A differentiated positioning of suppliers by segment, based on competitive strengths and portfolio attractiveness
- Focus on regional markets

The study thus provides an essential decision-making basis for positioning, relationship and go-to-market considerations. ISG Advisors and enterprise clients also use information from these reports to evaluate their current and potential new vendor relationships.

Provider Classifications

The provider position reflects the suitability of IT 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 $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have 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).

Who Should Read This Section

This quadrant is relevant to enterprises across industries in Germany for evaluating service providers specializing in managed security services (MSS) and thus helping enterprises combat security threats. It also provides insights into how each provider addresses critical market challenges.

In this quadrant, ISG defines the current positioning of MSS providers, offering a comprehensive overview of the competitive market landscape.

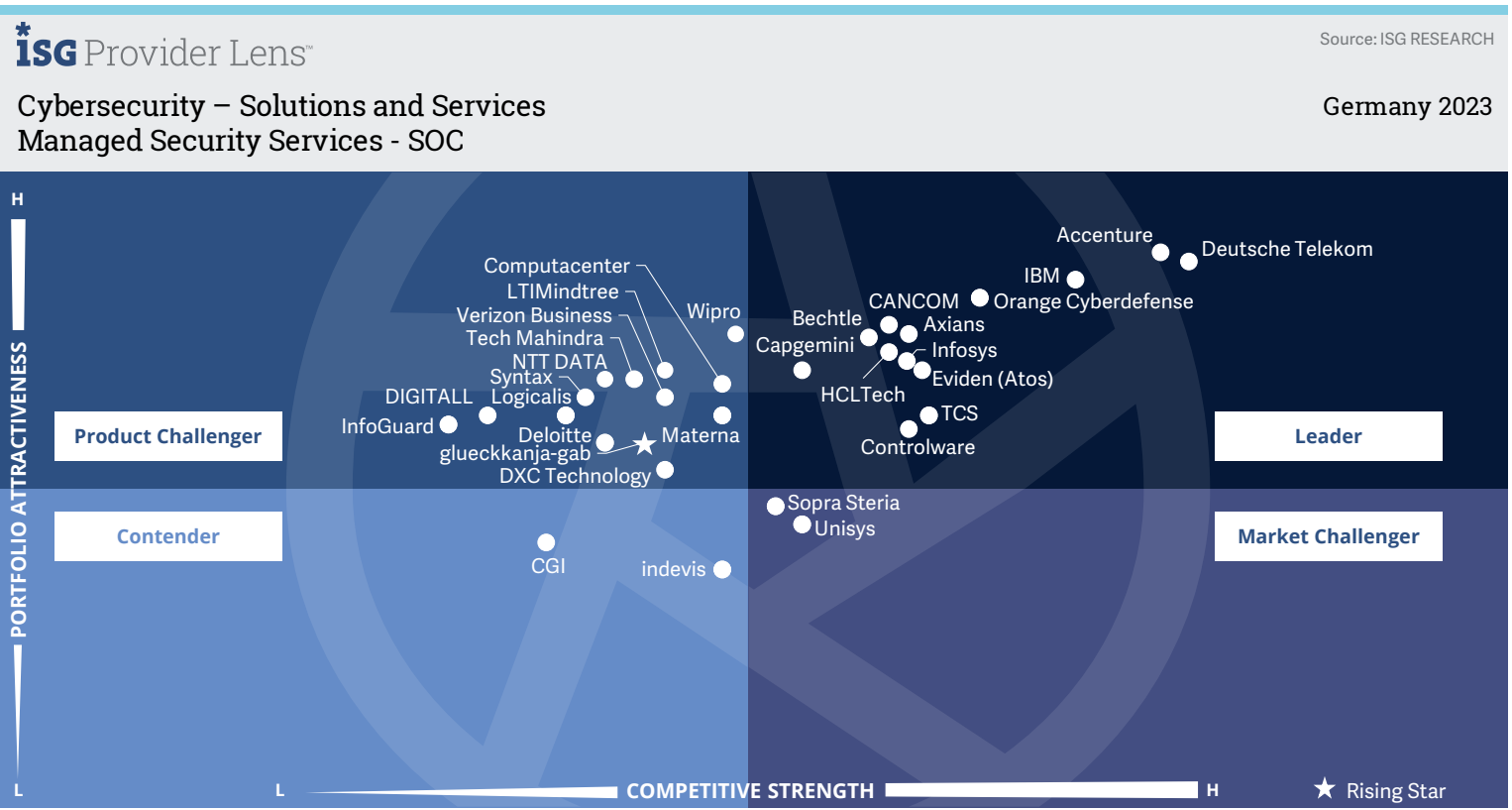
Businesses have become more vulnerable to cyber-attacks with the shift to remote work and the increased use of cloud-based applications and services. Managed detection and response (MDR) services provide a critical layer of protection against these threats, ensuring that remote workers and cloud-based assets are secure. Enterprises need continuous monitoring, advanced threat detection capabilities, incident response and remediation support to help prevent data breaches and ensure business continuity.

The importance of compliance regulations and data privacy laws drives the demand for MDR services. Ransomware detection and readiness are still high on the agenda as enterprises seek to protect their valuable data and systems from being compromised by malicious actors. It allows enterprises to prepare for the ransomware threat proactively. Advanced analytics, AI, ML and deep learning techniques for behavior-based threat analysis are gaining interest. Threat intelligence feeds allow proactive risk identification, monitoring and accurate detection and threat intelligence as a service is picking up. With the increasing adoption of zero trust and SASE and the scarcity of qualified resources and expertise, the need for managed services is increasing.

Cybersecurity professionals should read this report to understand the emerging trends and immediate threats to aid their strategic decision-making, enhance productivity and reduce security complexity.

Business professionals should read this report to gain valuable insights on simplifying security operations. It also offers practical solutions to reduce complexity and enhance efficiency.

Technology professionals should read this report to keep pace with the changing security landscape, as it provides insights on emerging trends, tailored security platforms and strategic objectives.



This quadrant evaluates the **most relevant** managed security service providers in Germany, excluding those providers that do not solely rely on their own products. The demand for external operations by **SOCs** is on the rise.

Frank Heuer

Definition

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

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximizing the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS (SOC) providers must combine traditional managed security services with innovation to fortify their clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies, infrastructure and experts skilled in threat hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI and machine learning. These sophisticated SOCs should support expert-driven security intelligence response, while offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, 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 on business performance. In particular, secure access service edge (SASE) is 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 a client's site
3. Possesses **accreditations** from security tools vendors
4. **SOCs ideally owned and managed by the provider** and not predominantly by partners
5. Maintains **certified staff,** for example with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)

Leader

"Infosys has established itself as a leader in the German market for managed security services and is consolidating its position through strong growth in this segment in this country."

Frank Heuer

Infosys

Overview

Infosys is headquartered in Bengaluru, India, and operates in 54 countries. In Germany, it has offices in nine locations. The company employs more than 346,800 people in 247 offices worldwide. In FY22, it generated revenue of $16.3 billion. In addition to strategic security services and technical security services, Infosys offers managed security services. These include "Cyber Next - Platform Powered Services," designed to provide visibility into security events, automated response capabilities and proactive vulnerability management, among others.

Strengths

Wide range of services: Infosys offers a full range of managed security services. The services include a broad spectrum of security technologies. This aspect particularly attracts large companies that have a diverse security landscape. Infosys also continues to further develop its managed security services portfolio; the roadmap is extensive. Infosys Cyber Security and the Infosys Center for Emerging Technology Solutions are constantly innovating, validating and bringing new solutions to the market.

Active in Germany: Infosys has a significant presence in Germany and is strongly positioned in terms of its managed security services in the region. In addition, it has a SOC in Düsseldorf, Germany. Infosys' business in Germany is growing strongly.

Up-to-date information for customers: Infosys helps its customers stay up-to-date and supports them in continuously improving their cybersecurity maturity. To achieve this, Infosys leverages its global network of Cyber Defense Centers spread across the U.S., Europe and India.

Caution

An expansion of the client base could be advantageous. Infosys mainly focuses on the needs of its demanding large companies and hardly on the specific needs of midsize companies that are yet to catch up in terms of managed security services and, thus, represent a large market potential.

Managed Security Services - SOC – Nordics

Report Author: Arun Kumar Singh

Cyber resiliency and data sovereignty continue to remain top priorities

During the COVID-19 pandemic, Nordic chief information security officers (CISOs) were compelled to develop novel solutions to keep businesses secured and operational. They discovered hidden strengths and resilience in their business strategies and teams. Cybersecurity gained renewed attention from organizations' leadership, board members and customers.

CISOs and their teams were considered business enablers within organizations instead of barriers impacting the delivery of products and services to the market. Most CISOs believe they were not adequately funded for security before the COVID-19 pandemic. The CISO community collaborates internally and externally for information exchange and continuous awareness about cyber hygiene to combat cybercriminals.

Digital Transformation = Increased Attack Surface

Enterprises adopt new technologies to embark on their digital transformation journeys to stay competitive and align with the evolving needs of end users. Digital technologies enable enterprises to expand their portfolios and market presence and improve CX. Nordic enterprises pursue security-focused digital transformation projects where security strategy, road mapping and risk assessment are top priorities for digital transformation. However, a few enterprises struggle to execute their efforts toward threat monitoring, hunting, alerting and response services due to cybersecurity skill shortages in the market. This shortage presents broad opportunities for service providers with consulting and managed services expertise to become strategic partners of enterprises. Leveraging managed security service providers (MSSPs) is becoming a trend to safeguard the value they would gain from digital transformation projects with embedded security.

Rising geopolitical conflicts and joint efforts toward unified cyber defense strategies.

According to the International Institute for Management Development (IMD), Denmark, Sweden and Finland held three of the top 10 positions in the global digital competitiveness ranking for 2022.

According to the Digital Economy and Society Index 2022, three Nordic countries, namely, Sweden, Denmark and Finland, emerged as leaders in integrating digital technologies into business processes. These three countries in the EU score very high on the Digital Intensity Index, signifying how enterprises leverage different technologies for their advantage, competitiveness and contribution to the national economy.

Most enterprises in Sweden, Finland and Denmark adopt sophisticated or intermediate cloud services. Sectors such as IT businesses and media and broadcast are leaders in adopting cloud models, whereas the construction, transportation and storage sectors lag with respect to cloud adoption, indicating their low reliance on technologies to drive businesses.

Cybersecurity Collaboration Among Nordic Countries is of Prime Importance

With the ongoing Russia and Ukraine conflict, in late 2022, Nordic countries collaborated to support the Nordic Defence Cooperation (NORDEFCO) — an interstate, military-led joint action coordination agency — for strengthening cybersecurity measures and spearheading the strategy to evaluate and deliver technical solutions, information exchange cadence and joint responses to handle cyber threats.

Besides collaborating, Nordic countries mainly focus on strengthening and investing in their cybersecurity infrastructure to safeguard critical national infrastructure, banking and financial services, and manufacturing industries from cyber threats.

- The Swedish government has commissioned key defense and security agencies to establish a National Cybersecurity Center (NCSC). This center will be critical in implementing the long-term goal of preventing, identifying and responding to the surge of cyber threats for protecting the IT infrastructure. Sweden will invest an additional $130 million in its military budget for 2023-2024 to expand cybersecurity capabilities.
- Finland has established the Network Security Advisory Board (NSAB) to help state governments and municipal departments implement and integrate security technologies with advanced cyber risk and threat monitoring capabilities. By 2023-2024, Finland is anticipated to spend $80 million as part of its cybersecurity budget, which will double compared to the previous fiscal year. The Finnish government has issued grants worth €115K (~$125K) to help enterprises of all sizes bolster their cyber defense program.
- Norway's National Security Authority (NSM), responsible for preventing, detecting and coordinating the handling of cyberattacks, will receive NOK 200 million (€21m) in funding to protect the government against cyberattacks. It also received NOK 40 million for introducing cyber threat alerts to NSM and plans to allocate another NOK 50 million to fortify its cybersecurity expertise for municipalities. The Norwegian Center for Information Security (NorSIS) has allocated NOK 10 million to improve communication systems, drive national crisis management efforts, establish a digital security portal for authorities and upgrade security clearance processes. Additional funding worth NOK 5 million is given to the Norwegian Civil Security Clearance Authority to assess the risk of a breach caused by insiders.
- The Danish government launched a new cyber and information security strategy in late 2021, with implementation scheduled between 2022 and 2024. This strategy will strengthen Denmark's digital security posture to deal with malicious attacks. The Danish government has allocated $226 million to invest in cybersecurity by 2023.

3Vs (Variety, Volume and Velocity) of the Cyber Threat Landscape in the Nordics

Nordic countries witnessed a series of cyberattacks in 2022 due to the Russia-Ukraine conflict and Finland and Sweden joining NATO forces. During this period of conflict, there was a significant increase in hacktivist mobilization and their activities, cyberattacks in sync with military actions, cybercrime and a rise in nation-state groups. Government entities

remain the prime focus of this cyber warfare. Cyber threats and cyberattacks on state assets continue to grow.

According to Google, the targeting of users in NATO countries increased by more than 300 percent in the same period. Cyber adversaries and hacktivists used malware as a primary tool to attack government websites, collect intelligence and organize disinformation campaigns to change public opinion.

Some of the significant cyberattacks that took place in the Nordic countries leading to business disruption are listed as follows:

1. Sweden:
   - In early 2023, distributed denial-of-service (DDoS) attacks by the hacker group *Anonymous Sudan* targeted several educational institutions, such as Karolinska Institute, Swedish University Network (Sunet) and the Luleå University of Technology, and Sweden's national TV broadcasting company SVT.
   - In September 2022, three DDoS cyberattacks targeted the Election Authority website (val.se) in less than 24 hours. These attacks impacted the reporting from municipalities and regional governments.
2. Norway:
   - The Norwegian newspaper Verdens Gang reported that its customers were logged into incorrect user accounts and had access to other individuals' personal details.
   - The Norwegian municipal pension fund's CEO was subjected to a phishing attack using the EvilProxy tool. This attack could have led to the transfer of NOK 3.5 billion (€322m) to a hacker's account, but it was apparently ceased on time.
3. Finland:
   - In August 2022, Finland's parliament experienced DDoS attacks leading to a temporary shutdown of its website.
   - OP Financial Group experienced a cyberattack on its website, impacting its login process.
4. Denmark
   - In early 2023, Denmark's central bank and seven other private lenders, namely, Jyske Bank, Sparekassen Sjælland-Fyn, Skjern Bank, Ringkjøbing Landbobank, Djurslands Bank and Kreditbanken, experienced DDoS attacks.
   - Cybersecurity threat actors targeted the OT systems of DSB, Denmark's largest train operating company, resulting in trains coming to a halt. Supeo, a mobile application provider that offers apps used by DSB train drivers, was the target of a ransomware attack.

Data Sovereignty Compliance

Data sovereignty is a top priority for national government regulators. Businesses are wary of the stringent data protection laws. Ongoing trends such as a hybrid workforce and dynamic compliance landscape are reshaping enterprises exploring data privacy laws and protecting themselves from probable financial fines for failing to comply with data sovereignty regulations. These regulations include the General Data Protection Regulation (GDPR; £18M or 4 percent of the annual revenue, whichever is greater), Payment Card Industry Data Security Standard (PCI-DSS; $5K-$10K per month), Health Insurance Portability and Accountability Act (HIPAA; $50-$50K per record) and Gramm-Leach-Bliley Act (GLBA; upto $100K per violation), among others.

The cybersecurity strategy of Nordic countries emphasizes data sovereignty, which implies identifying and cataloging critical information and controlling where essential data is stored. However, when data is migrated to the cloud, this control is often lost in the process, exposing organizations to significant gaps in data governance. Such gaps can result in failure to meet regulatory frameworks, which, in turn, will lead to penalties for organizations.

Nordics Business Challenges and Priorities

Based on ISG advisors' interaction with enterprise leaders, it is evident that business leaders are concerned and cautious about increased inflation, continued geopolitical tensions and a rise in the cost of living in 2023. Enterprises are decisive about increasing strategic investments

around talent (upskilling, recruitment and retention), technologies for business transformation and new business models, and achieving long-term growth. These investments would help business leaders stay ahead of the competition, tackle industry challenges and create long-term value.

Enterprises struggle to undertake a holistic approach to cyber threats, which entails a better understanding and visibility of all network assets (especially container-based applications and SaaS, which are deployed at a large scale and faster pace), associated risks faced by them and techniques to execute business operations amidst simultaneous risks. Business leaders in the Nordics focus on isolated risk scenarios and recovery plans instead of adopting a proactive and preventive approach that embeds resilience capabilities to withstand disruption.

Onboarding new technologies and applications with frequent update release cadences and imposing rigorous pen-testing and red teaming on the source code become a challenge for the internal security team of businesses. Lastly, Nordic enterprises require assistance in onboarding experienced cybersecurity talent and retaining them in the current market conditions where talent shortage is an industry-wide challenge.

Enterprises Struggling to Transform Cybersecurity Priority into Cyber Resilience

Nordic enterprises' board members consider cybersecurity a fairly high priority. They invest in identifying cyber risks and leverage advanced technologies to proactively monitor threats and prevent breaches. However, there is a lack of clarity around ROI when allocating and approving the budget by boardroom members. The members have a limited understanding of cyber risks and depend on external advisors, such as third-party providers, cyber insurance providers or internal subject matter experts, to manage threats.

Nordics Cyber Insurance Market Remains Challenging

The Russia-Ukraine conflict is fueling apprehension regarding cyber threats (IT systems interruptions, data breaches, and ransomware or cyber extortion) among Nordic enterprises, leading them to consider cyber insurance to safeguard themselves and comply with local government regulations. It is to be noted that coverage in case of an incident drives the purchase of cyber insurance. Requirements by law, pre- and post-incident coverage, to a lower degree, are other important reasons. Businesses without insurance are also interested in various types of coverage, including business continuity, expert support during an incident and ransomware coverage.

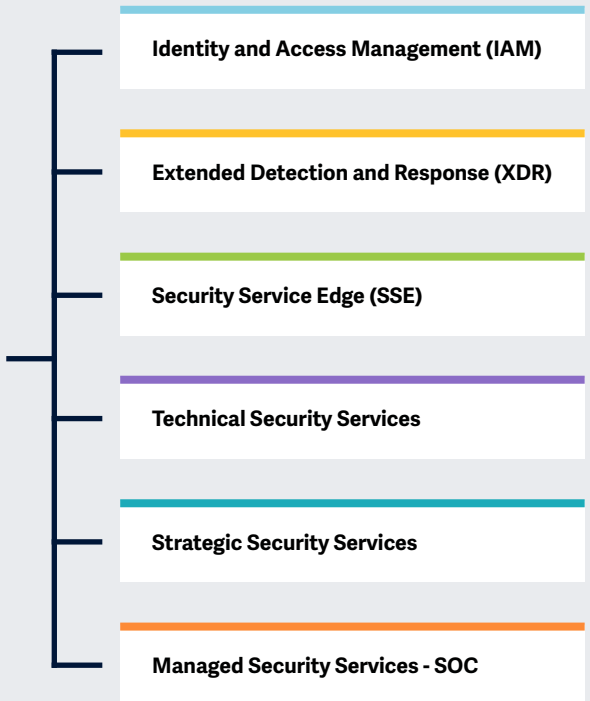
AI and Automation in Cybersecurity

AI and automation tools are becoming a highly critical component of the cybersecurity industry. These tools help mitigate security threats, gather threat intelligence and detection, and alert triage leveraging ML and advanced analytics. However, the industry continues to face a talent shortage to develop, maintain and operate AI and automation tools for cybersecurity functions. This shortage propels MSSPs and managed service providers (MSPs) to invest in AI and automation tools to support their clients, offering immense growth opportunities.

Nordic countries are ahead in terms of leading digital transformation efforts compared to other countries, The ongoing Russia-Ukraine conflict has compelled Nordic governments to enhance their regulatory, incident response efforts and cybersecurity budgets and strengthen their resilient posture to overcome the rapidly growing cyber threat landscape and reduce cyber risks.

Key focus areas for **Cybersecurity Solutions and Services 2023**

Simplified Illustration; Source: ISG 2023



Definition

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritized relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

From an enterprise perspective, even small businesses understood the impact of cyber threats and realized that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident. Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of the cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

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

Scope of the Report

In this ISG Provider Lens™ quadrant report, ISG covers the following five quadrants for services/solutions: Identity and Access Management (IAM), Extended Detection and Response (XDR), Security Service Edge (SSE), Technical Security Services, Strategic Security Services and Managed Security Services - SOC.

Vendors offering Security Service Edge (SSE) solutions are analyzed and positioned from a global perspective, rather than by individual regions, as the market is yet in the early stages of maturity.

This ISG Provider Lens™ study offers IT decision makers with the following:

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on the Nordics market

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

Provider Classifications

The provider position reflects the suitability of IT 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 $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have 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).

Who Should Read This Section

This report is relevant to enterprises across industries in the Nordics for evaluating providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. This report covers data on operations and management of IT and OT security services.

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

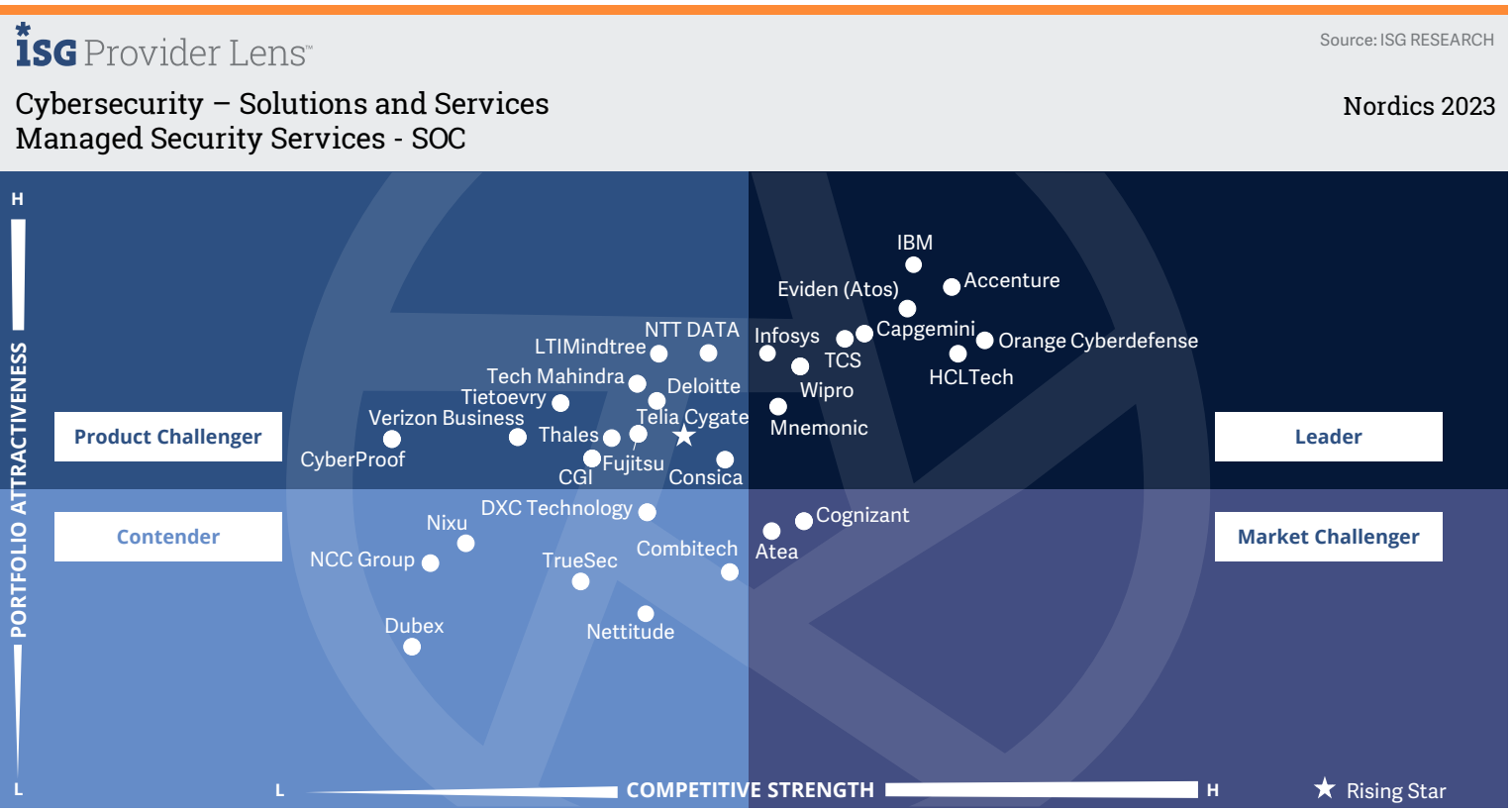
The nature of security operations center-as-a-service (SOC-as-a-service) is becoming competitive in Nordic countries. Enterprises seek service providers with robust technological expertise in AI, ML and behavior analytics to provide real-time threat intelligence while lowering the risk of data breaches or other cybersecurity incidents that could impact an organization's reputation and bottom line.

Recently, as the use and dependence on technologies continue to rise, there has been a corresponding increase in cyberattacks. Enterprises are looking for service providers with next-generation cloud-based managed detection and response (MDR) services equipped with advanced threat detection and analysis capabilities, adding an extra layer of protection while having robust cybersecurity measures in place. In contrast, to stay ahead of the curve, service providers substantially invest in developing in-house cloud-based MDR solutions with a few security stacks through technological partnerships, enabling scalability tailored to meet organizations' specific needs.

Cybersecurity professionals should read this report because it showcases emerging trends and immediate threats. It aids in strategic decision-making, enhancing productivity and reducing security complexity.

Business professionals should read this report because it offers valuable insights into simplifying security operations. It also provides practical solutions to reduce complexity and enhance efficiency.

Technology professionals should read this report because it highlights emerging trends and provides insights into security platforms and strategic objectives to keep pace with the changing security landscape.



This quadrant examines service providers that are not exclusively focused on proprietary products. They can **manage and operate the best-of-breed security tools and handle the security incident lifecycle**, from identification to resolution.

Arun Kumar Singh

Definition

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

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximizing the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS - SOC providers must combine traditional managed security services with innovation to fortify their clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies, infrastructure and experts skilled in threat hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI and machine learning. These sophisticated SOCs should support expert-driven security intelligence response, while offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, 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 on business performance. In particular, secure access service edge (SASE) is 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 a client's site.
3. Possesses **accreditations** from security tools vendors.
4. **SOCs ideally owned and managed by the provider** and not predominantly by partners.
5. Maintains **certified staff**, for example with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Global Information Assurance Certification (GIAC).

Leader

"Infosys emerges as a Leader through its as-a-service packaged security offerings powered by Cyber Next."

Arun Kumar Singh

Infosys

Overview

Infosys is headquartered in Bengaluru, India and operates in 54 countries. It has more than 346,800 employees across 247 global offices. In FY22 the company generated $16.3 billion in revenue, with Financial Services as its largest segment. Infosys' integrated managed protection, detection and response (MPDR) solution was developed with the Cyber Next platform and security controls. It has multiple platforms, such as Cyber Gaze, Cyber Hunt, Cyber Compass and Cyber Central. Infosys has been recognized as an AWS Security Competency Partner for showcasing its technical expertise in AWS and cloud security. It has more than 280 MSS FTEs in the Nordics.

Strengths

Underlying automation: The company's dedicated team for automation helps build use cases, bots and accelerators. It has developed more than 100 reusable use cases spanning IAM, infrastructure security and data security; over 200 reusable bots; automation platforms (Infosys IPs) for identity operations; and infrastructure operations and support for Sarbanes-Oxley Act (SOX) governance, patch management and vulnerability management.

Robust partner ecosystem: Infosys has strategic partnerships with more than 25 leading partners that help them build collaborative solutions and go-to-market plans. Its partnerships with academic institutions, both national and international, allow it to develop and nurture talent at scale.

Cybersecurity CoE: Infosys' CoE develops capability and capacity to enable business growth by competency development through training and academic collaborations, partner-led certifications, solution labs and automation for delivery excellence.

Continuous innovation: Infosys Cyber Security, along with Infosys Centre for Emerging Technology Solutions (ICETS), constantly innovates, validates and launches new solutions to enable customers to be risk-resilient.

Caution

Infosys is increasingly reliant on its clientele in the BFSI and retail sectors. The company should consider gradually expanding its presence in the midmarket and other verticals. It should also continue investing in SOC automation.

Appendix

Methodology & Team

The ISG Provider Lens™ 2023 – Cybersecurity – Solutions and Services report analyzes the relevant software vendors/service providers in the global 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:
Priyanka Richi and Sajina B

Research Analyst:
Deepika B

Data Analysts:
Rajesh Chillappagari and Shilpashree N

Consultant Advisor:
Roger Albrecht

Project Manager:
Donston Sharwin

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research™ programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of April 2023, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The study was divided into the following steps:

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

Lead Author

Arun Kumar Singh

Sr. Research Manager and Principal Analyst

Arun is a 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. 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.

Author

Gowtham Kumar Sampath

Assistant Director and Principal Analyst

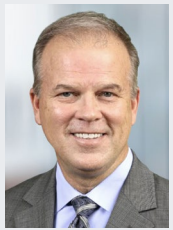
Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Research Analyst

Deepika B
Senior Research Analyst

Deepika is a Senior Research Analyst at ISG and is responsible for supporting and co-authoring Provider Lens™ studies on Cybersecurity - Services and solutions. She works closely with the Lead Analysts from diverse regions in the research process. She also authors enterprise context reports. She has over 4 years of experience in the technology research industry and has carried out various client-facing ad-hoc projects across industries such as Automotive, BFSI, and Retail & Consumer Goods. She was also accountable for maintaining a constant eye on the technology market and providing insightful quantitative and strategic analysis to clients through market sector reports. Her expertise spans a wide range of technologies, including IoT, AI, Big Data, and RPA.

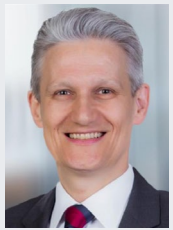


IPL Product Owner

Jan Erik Aase
Partner and Global Head – ISG Provider Lens™

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor. Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

Author



Frank Heuer
Principal Analyst

Frank Heuer is Principal Analyst at ISG Germany. His focus is on cybersecurity, digital workspace, communication, social business & collaboration, and cloud computing.

His main responsibilities include advising ICT vendors on strategic and operational marketing and sales.

Mr. Heuer is a speaker at conferences and webcasts on his main topics and is a member of the IDG expert network. Mr. Heuer has been active in the IT market as an analyst and consultant since 1999.

Author

Gowtham Kumar Sampath
Assistant Director and Principal Analyst

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Research Analyst

Bhuvaneshwari Mohan

Senior Research Analyst

Bhuvaneshwari is a senior research analyst at ISG responsible for supporting and co-authoring Provider Lens™ studies on Banking, Cybersecurity, Supply Chain, ESG and Digital Transformation. She supports the lead analysts in the research process, authors the global summary report and develops content from an enterprise perspective. Her core areas of expertise lie in Cybersecurity, Cloud & Data transformation, AI/ML, Blockchain, IoT, Intelligent Automation and Experience Engineering. She has 7 years of hands-on experience and has delivered insightful reports across verticals.

She is a versatile research professional having experience in Competitive Analysis, Social Media Analytics, Glassdoor Analysis and Talent Intelligence. Prior to ISG, she held research positions with IT & Digital Service Providers and was predominantly part of Sales Enablement teams.

Lead Author

Arun Kumar Singh

Sr. Research Manager & Principal Analyst

Arun is a 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. 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.

Author

Gowtham Kumar Sampath

Assistant Director and Principal Analyst

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Research Analyst

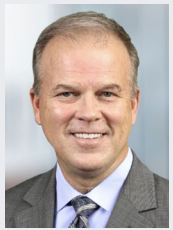
Deepika B

Senior Research Analyst

Deepika is a Senior Research Analyst at ISG and is responsible for supporting and co-authoring Provider Lens™ studies on Cybersecurity - Services and solutions. She works closely with the Lead Analysts from diverse regions in the research process. She also authors enterprise context reports. She has over 4 years of experience in the technology research industry and has carried out various client-facing ad-hoc projects across industries such as Automotive, BFSI, and Retail & Consumer Goods.

She was also accountable for maintaining a constant eye on the technology market and providing insightful quantitative and strategic analysis to clients through market sector reports. Her expertise spans a wide range of technologies, including IoT, AI, Big Data, and RPA.

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

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

ISG Provider Lens™

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

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

ISG Research™

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

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

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

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including 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 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.

ISG Provider Lens™

JUNE, 2023

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES