ISG Provider Lens™

Cybersecurity – Solutions and Services

Technical Security Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

pwc

QUADRANT REPORT | JUNE 2023 | U.S.

Table of Contents ⌂

Executive Summary

Report Author: Gowtham Kumar Sampath

CISOs will invest in eliminating threats and reducing costs, enhancing UX and risk posture

The year 2022 saw multidimensional challenges, which helped revolutionize the U.S. cybersecurity market from different perspectives. In that year, the U.S. witnessed more than 1,800 reported breaches, which was slightly lower than in 2021, which saw 1,862 incidents. However, the sophistication of the attacks was significantly higher in 2022, with more than 422 million individuals impacted compared with 298 million in 2021. The decline in breaches was partially due to federal laws that issued rulings to report only during actual damage and not for a potential one. While most large firms issued a breach notice, the notices had little to no information on the extent and impact of the attacks. Industry sources cite that the average time to identify a breach is about 207 days, which is almost half a year; the impact of the breaches is either unknown or not investigated further.

The second half of 2022 witnessed changes, with the U.S. government recognizing the need for strong regulations and policy changes that would encourage enterprises to invest in holistic cybersecurity solutions to protect their business and their clients. While the National Cybersecurity Strategy is aimed at prioritizing cybersecurity as a critical component of the economic prosperity and national security of the U.S., it also addresses the fundamental notion that the private sector holds the key to the public good of cybersecurity.

ISG is of the view that a large portion of the SMB market is invariably linked to large corporations directly and indirectly as part of a larger supply chain. Therefore, it is imperative for SMBs to invest in appropriate security measures to address all vulnerabilities and fill gaps in controls and policies; in short, approach security as a holistic responsibility across the business environment.

ISG's analysis indicates that U.S. enterprises continue to face challenges like their counterparts in other regions. However, the market shows a stark distinction in approach and investment, given the varied levels of

Cybersecurity initiatives must align with business priorities for strategic resilience.

digital transformation between large and small enterprises. Therefore, the approach to identifying challenges and the ensuing activities to ensure a secure environment is largely aligned with the enterprise's digital maturity, irrespective of its size.

ISG has identified the following challenges enterprises face:

- **Expensive attacks and threats:** U.S. enterprises continue to face increasingly sophisticated attacks, with cybercriminals employing complex and creative methods. Enterprises struggle to identify threats from unprotected devices and endpoints, vulnerabilities in applications and software, cloud misconfigurations and control policies, legacy infrastructure and internal threats. The cost of a data breach has increased over the years, with increasing expenses related to lost opportunities, regulatory fines and forensic investigation. Attackers are using sophisticated phishing techniques, malware and ransomware to target unsuspecting enterprises. In 2022, cybercriminals were specifically targeting enterprises in the healthcare and education

sectors. The cost of a breach, especially in the healthcare sector, is exponentially high in the U.S. with the loss of confidential patient data. Moreover, the healthcare sector is connected to several other critical industries, including banking, finance, payments and insurance, making it particularly attractive for malicious intent.

- **Supply chain attacks:** Cybercriminals have been attacking weak links in the enterprises' supply chains, such as their customers, third-party vendors and suppliers. Software supply chain attacks are expected to be the largest reason for compromised identities and data leakage. Enterprises can no longer remain satisfied with just securing their perimeters and plugging vulnerabilities but must also ensure that their partners and suppliers adhere to the highest standards of security. The situation becomes further complex as enterprises increasingly wish to adopt open-source software and develop applications in the cloud, prompting software developers to unintentionally use libraries available online. Threat actors have utilized these channels to embed malicious code

and exploit the entire chain of enterprises with targeted attacks. Enterprises are struggling to adopt policies and procedures to undertake continuous assessments and audits of their supply chain partners to ensure changes in behavior, detect vulnerabilities and deception techniques and develop agile isolation capabilities.

- **Government regulations and sanctions:** The announcement of the National Cybersecurity Strategy policy also indicates that the government and the public are aware of the importance of undertaking voluntary cyber hygiene programs and, at the same time, are aware of the recurring failures due to the soft enterprise measures. The strategy takes recourse in new regulatory frameworks that shift accountability, incentivizing enterprises to set up the appropriate defense against critical vulnerabilities. The U.S. Securities and Exchange Commission (SEC) also proposed cybersecurity measures in 2022 that came into effect in April 2023, once again highlighting the understanding among C-level executives of the criticality of security risks and the requirement for

increased transparency in dealing with breaches and threats. Enterprises will be required to disclose cybersecurity experience of board of directors on their 10-K and 8-K forms, governance methods and risk analysis and management processes and incidents deemed malicious within four days of determining that such a situation has occurred.

- **IoT and transformation initiatives:** Enterprise investments in digital technologies toward their transformation journeys, with IoT, AI and ML, have resulted in increased vulnerabilities that are unknown and inconspicuous. The adoption of IoT has increased the number of endpoints, with enterprises sometimes having little to no visibility of the entire network comprised of a large number of devices. Moreover, some IoT devices and deployments do not follow standard protocols, leaving them vulnerable to attacks, and the limited security integration capabilities make them impossible to protect. Apart from limited visibility, IoT poses other challenges arising from the use of open source software,

unpatched vulnerabilities, APIs and weak password protection. The increased sprawl of IoT devices also means that attackers will no longer exploit individual endpoints but the entire network to create botnets for extensive distributed denial of service (DDoS) attacks. These attacks, especially on critical infrastructure, will prove to be devastatingly costly from both a monetary and a socioeconomic perspective.

- **Skills and gap talent:** U.S. enterprises continue to face a shortage of cybersecurity talent and skillsets, with industry sources citing nearly 700,000 unfilled positions. Apart from the explosive growth of technology becoming a challenge for cybersecurity professionals, enterprises are also struggling to retain employees due to their requirements for multiple certifications and years of experience and the investments needed to keep skills up to date. Industry sources cite that the average experience for cybersecurity professionals is around six years across U.S. enterprises, further creating challenges with handling legacy security tools and solutions. Moreover, enterprises

are struggling to retain employees due to the change in work culture post-pandemic, and because of competition from technology startups offering attractive packages and career opportunities, which is triggering job hopping.

- **Remote and hybrid work:** Although enterprises are expecting and urging employees to return to work, the work culture and workplace have undergone a significant evolution with the adoption of emerging technologies. Enterprises are challenged by their expanded perimeter due to the investment in devices, endpoints, cloud and applications that are enabling remote and hybrid work. These factors have contributed to the increased attack surface and vulnerabilities because most of these investments were focused on attaining uninterrupted operations, but without the necessary diligence and control policies in place. Enterprises are also challenged by limited visibility across devices and applications and from complexities arising from insider threats.

Enterprises are taking necessary initiatives to reduce attack surface by focusing on the following

- **Focus on business resilience:** Since 2021, cyber resilience has been gaining mindshare among C-level executives across U.S. enterprises, with 2022 seeing the evolution of resilience widening to include business and operational aspects. While enterprises have been investing in intelligence-led detection and response solutions, they are also keen on investing in rapid recovery and business continuity capabilities. U.S. enterprises understand that investing in point solutions will not suffice; they need to take a holistic approach, assessing their risk appetite and maturity in implementing relevant solutions that mitigate business risks. Enterprises view resilience as a key factor in bolstering their ability to survive in the face of threats and for maintaining trust, responsibility and accountability, while ensuring high levels of CX.

- **Industry-aligned cybersecurity:** Enterprises are investing in identifying vulnerabilities and risks that are unique to their business

and ecosystem and are taking proactive measures to test and understand their threat landscape. With attackers targeting specific industries such as healthcare, utilities, automotive and education, enterprises are keen on investing in cybersecurity solutions that align better with their industry-specific regulations, threats and attack vectors. Besides compliance, controls and frameworks, attackers are exploiting similarities in unpatched vulnerabilities and backdoors to launch phishing campaigns that lead to breaches.

- **Zero trust and SASE:** As more enterprises invest in the cloud as a way to achieve digital transformation and support remote and hybrid workers, the Zero Trust framework has become an imperative investment. The framework's Never Trust, Always Verify tenet helps address multiple aspects, including perimeter-less enterprises, mutual authentication, explicit scrutinization, continuous monitoring and microsegmentation of the network. The framework requires a thorough understanding of existing security solutions

and requires phased investments to consistently deploy security measures deemed relevant for an enterprise. Security service edge (SSE) is another approach that supports their cloud migration journey and allows enterprises to start with small investments and progress rapidly.

- **Adhering to regulations:** Enterprises seek to undertake continuous and periodic risk assessments and audits across different areas, covering changes related to business strategy, supply chain, M&A and financial exposure. Apart from this, spending is focused on conducting periodic vulnerability scans and penetration tests to identify access points that are not secure and visible to security analysts. CISOs engage with providers that have red teams to simulate sophisticated cyberattacks to better understand vulnerabilities and weak access points and determine how adversaries can access sensitive data or disrupt networks. Enterprises are also adopting stricter measures and processes to thoroughly assess third-party vendors and software suppliers to minimize the

risk of attacks through the supply chain. From a prevention perspective, enterprises will become more cautious and invest in measures, including patching known exploits and deploying anomaly detection tools. As a comprehensive and overall strategy, they are investing in strong response and recovery plans to minimize the scale and impact of breaches.

- **Human-centric training and awareness:** Enterprises focus on providing awareness training to their employees to embed a cybersecurity-centric culture that would help reduce human errors and internal threats. Enterprises are also seeking innovative and user-oriented training that would help beyond just certification and instill a cybersecurity culture. Enterprises are willing to invest in multi-pronged security training to ensure a better understanding of sophisticated attack campaigns and vulnerabilities. Apart from addressing data breach, the trainings are expected to help address areas such as improved compliance, UX, employee well-being and customer assurance.

Considering there are challenges in aligning the CISO and overall enterprise objectives, ISG has analyzed CISO-specific challenges that hamper the effective security of an enterprise.

- **Recessionary fears impacting budgets:** CISOs are faced with constrained budgets, with the fear of a looming recession undermining their ability to defend their businesses against the ever-increasing frequency and sophistication of attacks. In some cases, budget reduction results in an executive board contemplating the right balance between ROI and the possibility of an actual attack. The economic headwinds have strained the ability of the CISO to invest in security solutions or hire relevant cybersecurity personnel. CISOs are struggling to allocate budgets and prioritize security solutions and services that would help drive value and enhance risk posture.

- **Fatigue and alerts:** Security teams are swamped with work related to alerts, tools, technologies and intelligence, and other challenges. While these teams must learn to adapt themselves to emerging security technologies, they also need to gain a better

context and understanding of the behavior of attackers and indicators of compromise (IoC), which would help them identify breaches and vulnerabilities. While most existing solutions offer alerts, the increased recurrence is likely to have an adverse impact on adherence to safety protocols. The market is also flooded with multiple tools and technologies claiming to have the ability to address security threats and attacks, making it difficult for security professionals to choose the optimal solution for their infrastructure. The market is also facing the challenge of incorrect information related to threat intelligence, which further puts a strain on security analysts, creating distrust and fatigue and affecting their morale and effectiveness.

- **Tool sprawl:** U.S. enterprises have an average of more than 25 security tools and solutions in place, according to industry sources. This volume complicates management and creates challenges in providing effective security. Apart from the challenges arising from legacy systems and related outdated and unpatched vulnerabilities, the lack

of technical support and tool sprawl lead to other issues, including difficulties in integration with other tools and operationalizing them. Tool sprawl is also identified as the cause of increased fatigue and burnout while enterprises struggle to find appropriate talent to offer support with these technologies.

- **Cloud security:** The unprecedented rate at which enterprises are adopting the cloud has prompted CISOs to quickly understand the security boundaries of their enterprises and determine responsibilities. Cloud misconfigurations have been cited as the most common area of security compromise, leading to the loss of data to cybercriminals. CISOs are also challenged with identifying where the data resides and when it is in motion to aid a better security posture throughout the data lifecycle.

CISOs are actively seeking the following solutions and services that will help them to improve the current situation.

- **Aligning with business objectives:** CISOs are looking for solutions and services that help them better prioritize their

cybersecurity initiatives and align them with enterprise business objectives. Apart from monitoring the threat landscape, CISOs are keen on educating board members on risk management capabilities relevant to an enterprise to ensure business resilience and growth. CISOs are looking to invest in solutions that can address industry-specific security threats, fostering a comprehensive security culture, creating awareness about insider threats and making cybersecurity a business problem rather than a technology problem.

- **Tool and vendor consolidation:** CISOs are looking for solutions that help address tool sprawl and technology rationalization. Cybersecurity services and solutions that enable better integration with existing tools and deliver intelligence to enable the appropriate response will gain traction. CISOs will invest in solutions that help them consolidate various tools and technologies, yet offer holistic detection and risk mitigation functionalities. They are no longer keen on investing in best-of-breed capabilities, but rather on integrated product

suites and single vendor platforms that will offer relevant risk management better suited for an enterprise's risk appetite.

- **Risk prioritization and quantification:** CISOs are investing in risk assessments and audits that help to better prioritize threats and risks specific to their business. Cybersecurity solutions and services that offer in-depth intelligence with industry-aligned assessments that consider supply chain risks are gaining traction. Although in the early stages, CISOs are investing in risk quantification solutions that allow them to engage and convince C-level executives to invest in appropriate security technologies. While the market is flooded with comparable scoring and benchmarking tools, CISOs are preferring solutions that can quantify risk in terms of monetary losses, which enables them to prioritize as well as educate board members to take appropriate security measures.

- **AI- and automation-driven intelligence:** Security teams are looking for solutions with the highest level of automation. AI that can sift through alerts and logs to provide

in-depth threat intelligence. Besides alert fatigue, CISOs are investing in human-centric solutions that leverage context- and behavior-led engines to detect threats and vulnerabilities. In addition to mitigating threats, these solutions offer intelligence to understand the kill chain and malicious behavior to prepare for and prevent such attacks in the future.

- **Utilizing outsourced services:** Managed services will become the new normal and de facto choice for enterprises, across different sizes, given the complex threat environment and lack of talent. CISOs will look for solutions that can integrate better with existing security tools or invest in integrated suites with extended detection and response (XDR) capabilities across the IT environment. CISOs will invest in MDR, XDR and MXDR solutions and services that consolidate intelligence across the IT infrastructure and security tools and prioritize them with remediation, including isolation of threats handled by security experts from an advanced SOC.

Executive Summary

Notes on quadrants: The Security Service Edge (SSE) quadrant is analyzed from a global perspective, given its early stages of maturity and because enterprises taking a phased approach to investing in these solutions.

Notes of quadrant positioning: In this study, several security services and solution providers that offer similar portfolio attractiveness in most quadrants are assessed. This reflects the relative maturity of the market, providers and offerings. It is a given that not all are equal in circumstances. The vertical axis positioning in each quadrant reflects ISG's analysis of how well the offerings align with the full scope of enterprise needs. Readers will also note similarities in portfolio axis (vertical axis) positioning with providers included in ISG's Provider Lens™ U.S. Public Sector Cybersecurity Solutions and Services study.

Cybersecurity can no longer be restricted to only preventing attacks and defending against cyber criminals with sophisticated malware and ransomware but needs to evolve to better understand cyber risks and recovery capabilities to ensure business resilience. As businesses increasingly shift to the cloud and adopt emerging technologies, enterprises will seek cybersecurity solutions/services that offer enhanced visibility and risk management.

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Accenture	Not In	Not In	Not In	Leader	Leader	Leader	Not In
AT&T Cybersecurity	Not In	Not In	Not In	Not In	Not In	Not In	Leader
Avatier	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Avertium	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
BlueVoyant	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger	Not In
Check Point	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cipher	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
Computacenter	Not In	Not In	Not In	Contender	Contender	Contender	Product Challenger
Critical Start	Not In	Not In	Not In	Not In	Not In	Not In	Leader
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
CyberArk	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Not In	Not In	Leader	Not In
CyberSecOp	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
Cyderes	Not In	Not In	Not In	Not In	Not In	Rising Star ★	Not In
Cynet	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader	Not In
DXC Technology	Not In	Not In	Not In	Product Challenger	Market Challenger	Product Challenger	Not In
Elastic Security	Not In	Contender	Not In	Not In	Not In	Not In	Not In
EmpowerID	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
eSentire	Not In	Contender	Not In	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Eviden (Atos)	Product Challenger	Not In	Not In	Leader	Leader	Leader	Not In
EY	Not In	Not In	Not In	Rising Star ★	Leader	Product Challenger	Not In
Fidelis Cybersecurity	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fischer Identity	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In
ForgeRock	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Fortinet	Market Challenger	Leader	Product Challenger	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Fortra	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Contender	Contender	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Happiest Minds	Not In	Not In	Not In	Contender	Contender	Not In	Contender
HCLTech	Not In	Not In	Not In	Leader	Leader	Leader	Not In
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Not In
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Infinite Networks	Not In	Not In	Contender	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Infosys	Not In	Not In	Not In	Leader	Leader	Leader	Not In
KPMG	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
Kudelski Security	Not In	Not In	Not In	Contender	Contender	Not In	Rising Star ★
Kyndryl	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Not In
Lookout	Not In	Not In	Contender	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Lumen	Not In	Not In	Not In	Market Challenger	Not In	Not In	Leader
ManageEngine	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Microland	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger
Microsoft	Leader	Leader	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 7 of 11

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Mphasis	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In
NetWitness	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In	Not In
OpenText	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Optiv	Not In	Not In	Not In	Not In	Not In	Not In	Leader
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Perimeter 81	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Persistent Systems	Not In	Not In	Not In	Contender	Product Challenger	Not In	Product Challenger
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Presidio	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Proficio	Not In	Not In	Not In	Not In	Contender	Not In	Leader
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In
PurpleSec	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
PwC	Not In	Not In	Not In	Leader	Leader	Not In	Not In
Rackspace Technology	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In
SecureAuth	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Leader	Not In	Not In	Market Challenger	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In
SilverSky	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
SLK Software	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In

Provider Positioning

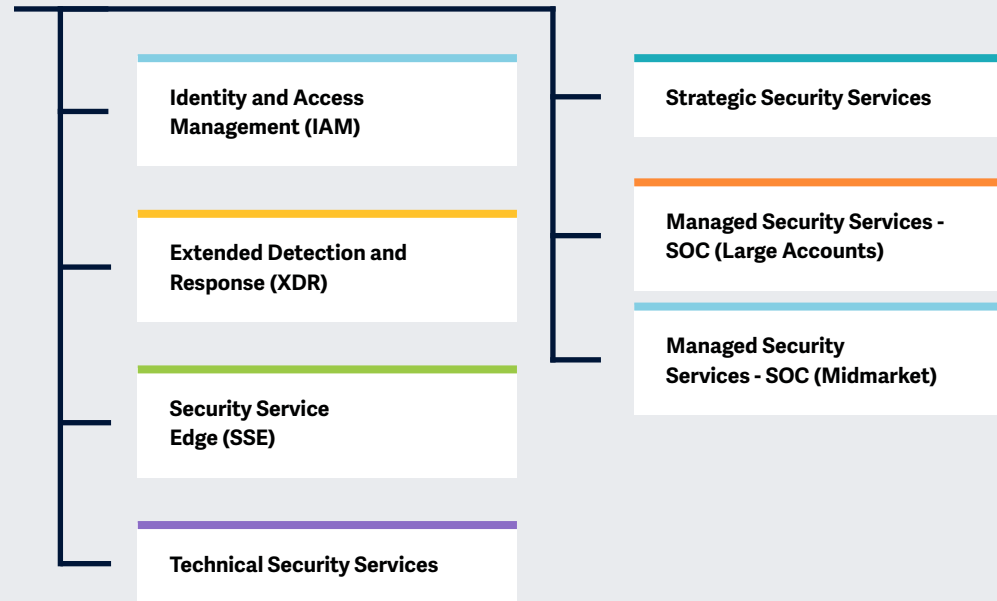|	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
TCS	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Thales	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★	Leader
Unisys	Not In	Not In	Not In	Leader	Contender	Product Challenger	Leader
ValueLabs	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Verizon Business	Not In	Not In	Not In	Leader	Rising Star ★	Leader	Not In

Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In
VMware	Not In	Contender	Contender	Not In	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Zensar	Not In	Not In	Not In	Contender	Product Challenger	Contender	Contender
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In

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

Simplified Illustration Source: ISG 2023

Identity and Access Management (IAM)

Extended Detection and Response (XDR)

Security Service Edge (SSE)

Technical Security Services

Strategic Security Services

Managed Security Services - SOC (Large Accounts)

Managed Security Services - SOC (Midmarket)

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.

Even small businesses understood the impact of cyberthreats 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), 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 six 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), the latter of which is divided into Large Accounts and Midmarket quadrants.

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 (quadrants)
- Focus on regional 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).

Provider Classifications: Quadrant Key

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

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

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

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

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

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

Technical Security Services

Who Should Read This Section

In this quadrant, ISG aims to assist U.S. enterprises in evaluating technical security service (TSS) providers that specialize in implementing and integrating security products or solutions. The report focuses on providers that integrate solutions offered by other vendors in addition to their proprietary products.

ISG defines the current market positioning of TSS providers and highlights how each provider addresses the key security challenges in the U.S. and helps clients with robust security practices.

Managing a mature cybersecurity program is becoming difficult for enterprises due to their long-term investments in numerous security tools and technologies. Subsequently, they are changing their focus from point solutions to a more holistic platform-based approach. Enterprises are seeking the help of providers for technology consolidation, which involves integrating multiple tools and technologies into a centralized platform for better visibility and control and for maximizing ROI. This approach

can help enterprises streamline their security operations, reduce complexity and improve their threat security posture. DevSecOps continues to mature as security is integrated earlier in the application development. As modern applications become increasingly complex and interconnected, enterprises find the task of securing their critical data and systems increasingly challenging, more so with the subsequent increase in potential attack surfaces. Furthermore, many applications now rely on third-party libraries and components, which represent additional security risks. Providers implement a combination of secure coding practices, vulnerability management, threat modelling and penetration testing for effective application security.

Technology professionals should read this report to understand providers' integration capabilities that reduce threat impact by using advanced technologies to transform legacy systems.

Security and data professionals should read this report to gain insights into how providers comply with security and data protection laws to stay abreast with market trends.
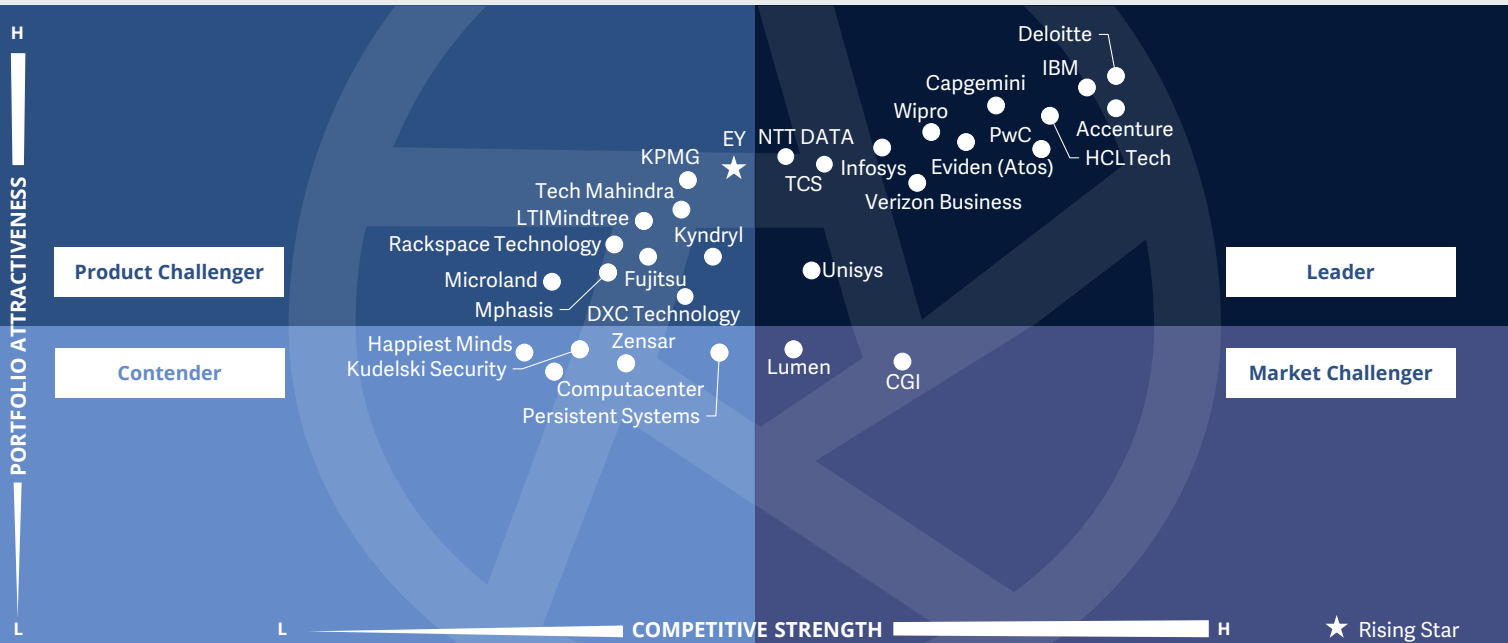
Business professionals should read this report to balance data security, customer experience and privacy amidst digital transformation at the forefront of businesses today.

ISG Provider Lens™

Cybersecurity – Solutions and Services
Technical Security Services

U.S. 2023

PORTFOLIO ATTRACTIVENESS

H

Product Challenger

Contender

Deloitte

IBM

Capgemini

Wipro

Accenture

EY   NTT DATA   PwC

KPMG   Infosys   Eviden (Atos)   HCLTech

Tech Mahindra   TCS   Verizon Business

LTIMindtree

Rackspace Technology   Kyndryl

Microland   Fujitsu

Mphasis   Unisys

DXC Technology

Happiest Minds   Zensar

Kudelski Security

Computacenter   Lumen   CGI

Persistent Systems

Leader

Market Challenger

L

L   **COMPETITIVE STRENGTH**   H   ★ Rising Star

This quadrant assesses service providers with capabilities and **specialized accreditations** to transform an existing security environment with **best-of-breed tools and technologies**, improving security posture and reducing threat impact.

Gowtham Kumar Sampath

Technical Security Services

Definition

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

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

implementation, validation, penetration testing, integration and deployment. The providers also leverage sophisticated solutions that enable comprehensive vulnerability scanning across applications, networks, endpoints and individual users to uncover weaknesses and mitigate external and internal threats.

TSS providers invest in establishing partnerships across security technology, cloud, data and network domains to gain specialized accreditations and expand the scope of their work and portfolios. This quadrant also encompasses classic managed security services, i.e., those provided without a security operations center (SOC).

This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.

Eligibility Criteria

1. Demonstrate experience in **implementing cybersecurity solutions** for companies in the respective country.

2. **Authorized by security technology vendors** (hardware and software) to distribute and support security solutions.

3. Providers should **employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies.

Technical Security Services

Observations

Traditional technical security services (TSS) are being increasingly integrated with consulting or managed services, leaving very few pure-play service providers in the market. Compared with the assessments in 2022, this year ISG has excluded service providers that have already integrated their TSS with other services.

Some of the other developments in this space are:

- Enterprises are looking for service providers with the ability to address tool sprawl and technology rationalization, can ease integration efforts and offer cost optimization benefits.

- TSS offerings are being designed to suit the special requirements of verticals such as manufacturing and automotive to enable standardized delivery. Services are also flexibly designed to be in sync with existing technologies and shift to emerging technologies.

- Providers are applying automated security controls and tests early in the development cycle; DevSecOps teams can minimize human errors, downtime and vulnerabilities. They are also investing in developing proprietary tools and leveraging third-party security tools to support the development of the integration pipeline.

- Providers are investing in establishing a large ecosystem of partners so they can take a vendor-agnostic approach and showcase best-of-breed capabilities. This network of partners and alliances is enabling providers to gain access to a wide range of technologies, implementation options and best practices.

- With the increased convergence of IT/OT environments, providers are investing to gain OT capabilities. They are also focusing on IT service management (ITSM) capabilities for enabling integration, convergence and standardization of infrastructure and security services.

From the 261 companies assessed for this study, 30 have qualified for this quadrant with 13 being Leaders and one a Rising Star

accenture

Accenture continues to invest in combining human and applied intelligence with digital technologies to drive operations. Its services also leverage analytics to collect relevant data and analyze the vulnerabilities of more than 71,000 products from over 1,000 vendors.

Capgemini

Capgemini utilizes cutting-edge technologies such as security, cloud automation, AI, analytics, data and threat intelligence, and its in-depth know-how of security products to offer its services. Its Factory Design and Setup takes an industrialized, factory approach to serve clients in specific industries.

Deloitte.

Deloitte's more than 8,600 dedicated cyber risk service practitioners support the customization of solution packages for clients, based on size, industry and business needs. It combines these services with a function-leading toolset from its partner network and proprietary solutions.

EVIDEN
an atos business

Eviden (Atos) has more than 6,000 cybersecurity specialists and has invested in a large ecosystem of technology partners. Eviden (Atos) also takes part in several working groups and is a thought leader across industry organizations within the cybersecurity community.

HCLTech

HCLTech relies on its large set of experts skilled in multiple security technologies, delivering its transformation and integration services through seasoned subject matter experts placed across the globe. HCL's Cybersecurity Fusion platform solutions and deep domain knowledge, along with Microsoft's range of security products, create a compelling suite.

IBM has a strong portfolio with its integrated security services aimed at protecting critical assets. It offers quick response and recovery from disruptions using assessment libraries and maturity models, customized to a client's industry, segment and geography.

Infosys relies on its comprehensive portfolio that includes the Cyber Next Platform, which includes pre-built, ready-to-use solutions and services for security monitoring, security analytics, threat intelligence and advanced security controls.

NTT DATA

NTT DATA provides customized offerings to suit the specific needs of enterprises across industry verticals. Decades of experience in handling complex industry challenges and localized expertise enable the company to create a compelling offering.

PwC uses a multidisciplinary team of specialists in digital technologies, people and organization, business resilience, forensics, financial crime and human-centric design. Its deep knowledge across industries helps clients build robust cybersecurity and privacy programs.

TCS invests heavily in alliances with technology vendors for service development and a GTM strategy, and positions them within its service model. Its cyber vigilance operations allow proactive scanning of security vulnerabilities and quick response to data breaches.

Unisys uses its understanding of how clients are targeted to create a security architecture to address these areas, with a strong focus on providing an ecosystem of solutions addressing specific threats.

Verizon Business leverages partnerships with many industry-leading and best-of-breed technology companies to increase bench strength and consulting service delivery. It is enhancing offerings in SASE, network security, cloud security and managed detection and response (MDR).

Wipro combines detection, triaging, orchestration and contextualized incident management and investigation into a seamless experience to reduce the mean time to respond (MTTR) for every incident. It optimally combines home-grown intellectual property and IP from partners.

EY

EY (Rising Star) has inherent risk management capabilities that help with security operations and response efforts. It has strong ties with leading product vendors and can provide vendor-agnostic threat management offerings.

Technical Security Services

PwC

"PwC delivers strong TSS competence with its core value of driving cybersecurity and risk management across enterprise transformation initiatives. It exhibits continuous innovation, a strong team of experts and intelligent threat response capabilities."

Gowtham Kumar Sampath

Overview

PwC is headquartered in London, U.K. and operates in 152 countries. It has more than 327,900 employees across 690 global offices. In FY22 the company generated $50.3 billion in revenue, with Advisory as its largest segment. PwC helps clients not only identify risks, but also measure and monitor the effectiveness and value of a security strategy. Its engagements are outcome driven and quantified to enable business leaders and technology leaders to make strategic, cost-feasible decisions based on risk.

Strengths

Comprehensive portfolio: PwC's Cybersecurity, Risk and Regulatory (CR&R) practice provides comprehensive TSS covering security architecture design and development, security and risk tech implementation, threat intelligence, vulnerability management and zero trust technical services. PwC offers integrated services in four specific areas: data trust, cyber resilience, cyber transformation and cyber risk management.

Innovative capabilities: PwC's Cyber Security Simulation Platform provides an environment that enhances security design and can assess and augment internal and third-party workforce security competency. The platform offers a controlled environment that mimics real-world networks, security technologies and cyberattacks to strengthen capabilities, including protection, detection and response.

Addresses business risk and resilience: PwC helps enterprises with their transformation initiatives by integrating security right from strategy design through implementation and management to better align business objectives and risks. Its offerings help enterprises adopt emerging technologies confidently by reducing risk exposure and operational cost while improving resilience to withstand cyberthreats.

Caution

PwC should continue promoting awareness and thought leadership in areas such as technology consolidation, security fabric and security mesh.

PwC should continue expanding its partner network and focus on players with native and out-of-the-box integration capabilities covering future-proof security solutions.

Appendix

The ISG Provider Lens™ 2023 – Cybersecurity – Solutions and Services report analyzes the relevant software vendors/service providers in the U.S. market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research™ methodology.

Lead Author:
Gowtham Kumar Sampath

Editor:
Ipshita Sengupta and John Burnell

Research Analyst:
Bhuvaneshwari Mohan

Data Analysts:
Rajesh Chillappagari and Shilpashree N

Consultant Advisor:
Doug Saylors

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 June 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

Author & Editor Biographies

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.

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™