ISG Provider Lens™

Cybersecurity – Solutions and Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

Infosys®

QUADRANT REPORT | JUNE 2023 | U.S.

Table of Contents

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.

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

Page 1 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)
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

Page 2 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)
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

Page 3 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)
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

Page 4 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)
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

Page 5 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)
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

Page 6 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)
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

	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

Page 8 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)
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

Page 9 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)
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

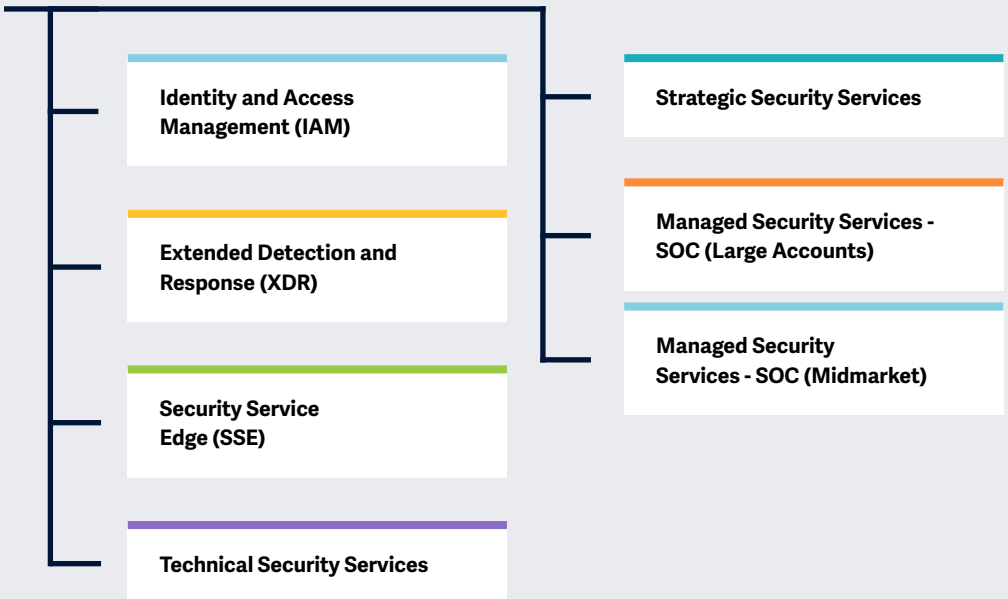
Provider Positioning

Page 11 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)
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



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.

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

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

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

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

Identity and Access Management (IAM)

Who Should Read This Section

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

ISG defines the current positioning of IAM players in the U.S., with a comprehensive overview of the market's competitive landscape.

For enterprises in the U.S., IAM is becoming the foundational layer in implementing a zero-trust security model that ensures that only authorized users can access sensitive data and applications. IAM solutions help enterprises centralize and automate the management of user identities and control access to enterprise resources from anywhere and everywhere. With attack surfaces becoming increasingly large and complex, enterprises find it a challenge to minimize cyber risks and secure their digital systems while, concurrently, provide a frictionless user experience. Enterprises expect IAM tools to provide a clear and intuitive user experience that can be empowering for their employees and customers. To keep up with the evolving market demands, IAM vendors are shifting their business focus to provide next-generation security capabilities for identity that include centralized, zero-trust IAM to fit cloud-oriented organizations. Advanced security capabilities such as biometrics for passwordless authentication, automated access approvals, risk-based authentication and user provisioning and de-provisioning based on behavior analytics for minimizing user friction and improving security are gaining momentum in the market.

Cybersecurity professionals should read this report to understand how providers use technologies to address compliance and security concerns while offering a seamless experience to enterprise clients.

Compliance and governance professionals should read this report to understand how to better manage user access to systems and data for ensuring regulatory compliance and streamlining audits.

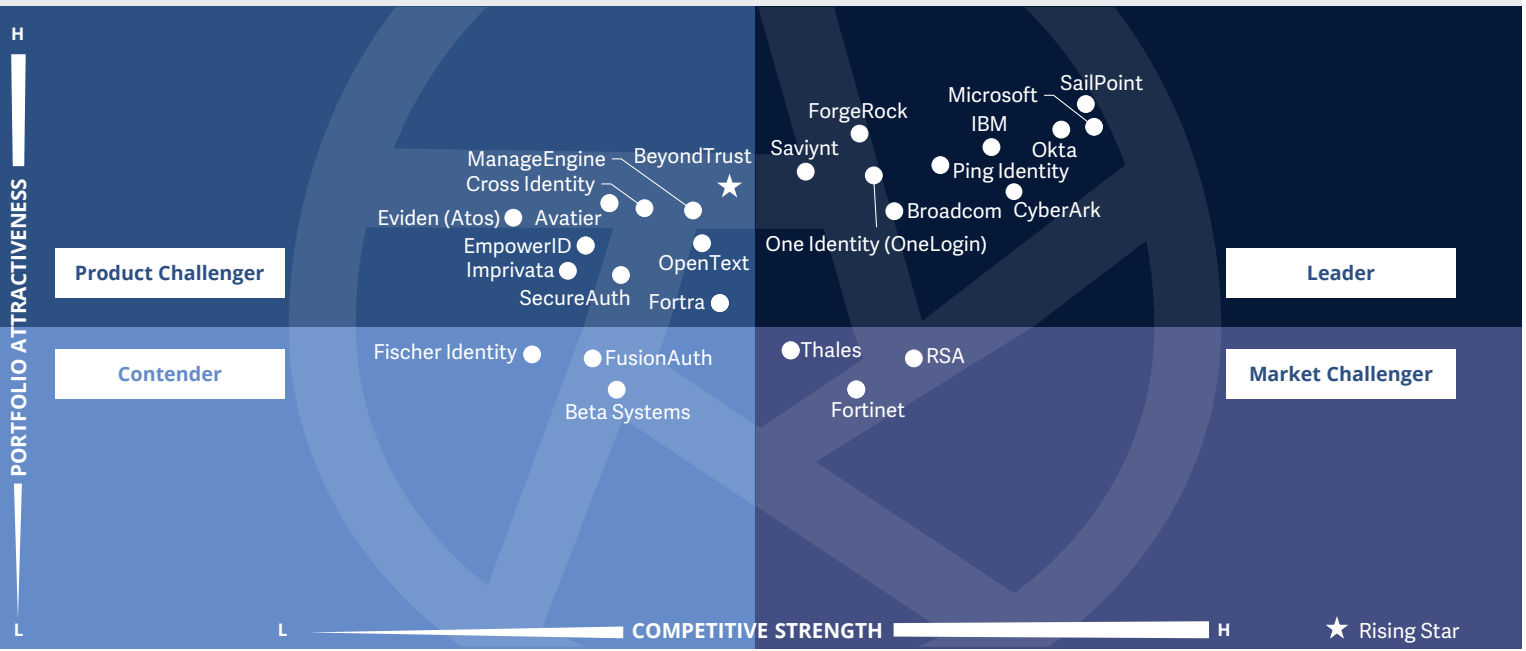
Strategy professionals should read this report to understand how IAM tools can enhance user experience while improving the security and efficiency of their systems and data.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Identity and Access Management (IAM)

U.S. 2023



This quadrant assesses IAM vendors with **proprietary solutions**, targeting **single sign-on (SSO), MFA and passwordless authentication**, with smart access control, **frictionless UX** and **zero-trust** security gaining traction.

Gowtham Kumar Sampath

Definition

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

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

Eligibility Criteria

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

Observations

Security and business leaders are under immense pressure to protect their businesses from data breaches as identity-related attacks are becoming increasingly common. Enterprises are adopting a zero-trust approach that prioritizes identity to manage the growing number of digital assets and identities. In 2023, we will see an increase in IAM vendors incorporating zero-trust principles into their products to provide a foundation for a zero-trust strategy.

Customer identity and access management (CIAM) continues to gain traction with rising data regulation mandates and data protection needs. The goal of IAM is transitioning from solely focusing on security through identity management to also delivering a smooth, seamless user experience. Few IAM solution providers are positioning themselves are CIAM-focused players. To meet the requirement of a consolidated platform that can manage multiple identity tools and simplify centralized identity management workflows IAM vendors such as Microsoft, One Identity (One Login) and CyberArk are prioritizing platform-based IAM solutions integrated with comprehensive functionalities to provide a unified experience.

IAM vendors are continuously enhancing their IAM suites by introducing new identity tools and features. These additions comprise various essential features such as identity threat detection and response, adaptive authentication, phishing resistance, blockchain-based decentralized identity and an array of biometric options for passwordless authentication.

From the 261 companies assessed for this study, 26 have qualified for this quadrant with 10 being Leaders and one a Rising Star.

Broadcom

Broadcom's IAM portfolio includes feature-rich products suitable for large enterprises, and its IAM Security Fabric strategy is making strides in the right direction, indicating a positive shift in its approach to identity and access management.

CyberArk

CyberArk primarily focuses on providing innovative solutions around privileged access security, encompassing emerging security requirements such as secure access to cloud-native applications and infrastructure and enhanced threat detection and response.

ForgeRock

ForgeRock has strong capabilities around access management and identity governance and administration (IGA) and continues to enhance its portfolio using emerging technologies such as AI and analytics to bolster its market position in the digital identity space.

IBM

IBM offers a diverse portfolio of offerings that encompass IAM, cloud access management and authentication, IGA, privileged access management (PAM), CIAM and hybrid access management system. IBM's cloud-native approach ensures automated risk protection and continuous user authentication across multicloud environments.

Microsoft

Microsoft is creating a true zero-trust mindset to ensure effective protection and organizational resilience. Microsoft Azure AD offers traditional features such as SSO, Lightweight Directory services, rights management, certificate services and federation services.

Okta

Okta provides an extensive set of identity tools, covering customer and workforce IAM for SaaS-based apps and multicloud environments. It also provides developer tools for easy implementation of SSO, MFA and passwordless authentication.

One Identity (OneLogin)

One Identity (OneLogin) is bringing new innovations to the security space after the acquisition of OneLogin. The company has invested significantly in product rollouts, enhancements and integrations to provide momentum to enterprises' journeys toward an identity-centric approach.

Ping Identity

Ping Identity continues to focus on identity-centric solutions with advanced capabilities such as risk-adaptive authentication, which allows customization using a low-code/no-code interface, and identity orchestration.

SailPoint

SailPoint's AI-driven approach to delivering identity security at scale addresses the pain points of modern enterprises. With the recent acquisition of SecZetta, it has broadened its portfolio through the addition of new capabilities around non-employee identity.

Saviynt

Saviynt's cloud-native identity platform unifies multiple identity tools. It offers considerable user visibility, allowing enterprises to significantly reduce security incidents and compliance violations.

BeyondTrust

BeyondTrust (Rising Star) offers a privileged remote access option, ideal for large enterprises with robust functionalities. It can be easily deployed because of its intuitive interface and enhances user experience consistently.

Extended Detection and Response (XDR)

Who Should Read This Section

This quadrant is relevant to enterprises in the U.S. for evaluating extended detection and response (XDR) solution providers. It further assesses how each provider helps enterprises increase visibility across all telemetry sources and obtain a unified view of threat detection and response.

ISG defines the current positioning of XDR players in the U.S. with a comprehensive overview of the market's competitive landscape.

The need for a holistic view of cyber threats across several endpoints is driving the adoption of XDR solutions among enterprises in the U.S., for their ability to incorporate best practices from cyber incidents constantly. XDR enables an enterprise to integrate disparate internal and external data sources to not only identify and investigate threats in a simplified way but also support threat defense proactively. An XDR platform includes automated threat detection, threat hunting capabilities and incident response playbooks that can streamline enterprise responses enterprises through highly detailed alerts and guided remediation. An XDR solution provides contextualized threat analysis, which helps security teams better understand the nature of a threat and its potential impact. The analysis ideally has information about the attacker's tactics, techniques and procedures (TTPs) and the vulnerabilities and assets targeted. Implementing an XDR solution can become challenging for enterprises if the vendor chosen has limited integration capabilities, because the tool must be wholly embedded in the enterprise's existing IT infrastructure.

Cybersecurity professionals should read this report as it provides valuable insights into XDR solutions that improve endpoint visibility for unified threat detection and response in enterprises. response.

Technology professionals should read this report because it highlights the integration capabilities of XDR vendors that can help with improved detection and faster responses to threats.

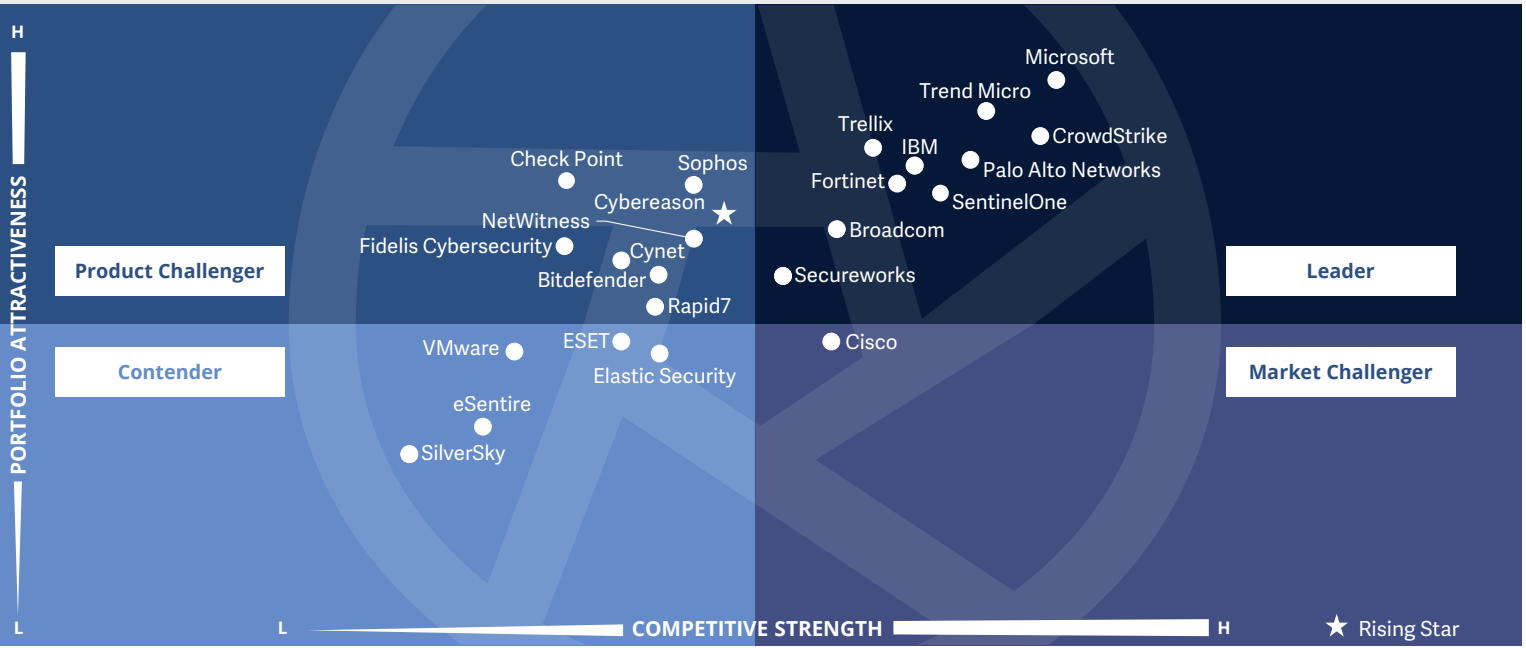
Strategy professionals should read this report to understand the capabilities of the XDR vendors helping enterprises manage security risks effectively and make informed decisions about their security strategies.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Extended Detection and Response (XDR)

U.S. 2023



This quadrant assesses vendors that offer XDR solutions comprising **multiple products and solutions integrated** into a **single pane of glass** to view, **detect and respond** with sophisticated capabilities.

Gowtham Kumar Sampath

Definition

The XDR solution providers assessed for this quadrant are characterized by their ability to offer a platform that integrates, correlates and contextualizes data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-delivered technology, comprising multiple-point solutions. It uses advanced analytics to correlate alerts from multiple sources, including from weak individual signals to enable accurate detections. XDR solutions consolidate and integrate multiple products and are designed to provide comprehensive workspace security, network security or workload security. Typically, XDR solutions are aimed at vastly improving visibility and improving context to the identified threat across the enterprise. Therefore, these solutions include specific characteristics, including telemetry and contextual data analysis, detection and response. XDR solutions comprise multiple products and solutions integrated into a single pane of glass to view, detect and respond with sophisticated capabilities. High automation maturity and contextual analysis offer unique response capabilities tailored to the affected system, and prioritize alerts based on severity against known reference frameworks. Pure service providers that do not offer an XDR solution based on proprietary software are not included here. XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expense, and are particularly suitable for security operations teams that have difficulty in managing a best-of-breed solutions portfolio or getting value from a security information and event management (SIEM) or security, orchestration, automation and response (SOAR) solution.

Eligibility Criteria

1. The XDR offering should be based on **proprietary software** and not on third-party software.
2. An XDR solution needs to have two primary components: **XDR front end and XDR back end**.
3. The front end should have **three or more solutions or sensors**, including, but not limited to, **endpoint detection and response, endpoint protection platforms**, network protection (firewalls, IDPS), **network detection and response**, identity management, email security, mobile threat detection, cloud workload protection and identification of deception.
4. The solution provides **comprehensive and total coverage and visibility of all endpoints** in a network.
5. The solution demonstrates **effectiveness in blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware.
6. The solution leverages **threat intelligence**, and analyzes and offers **real-time insights on threats** emanating across endpoints.
7. The solution should include **automated response features.**

Observations

Extended detection and response solutions have started gaining mindshare and traction in the market in the last two years. Enterprises are seeking to better understand and correlate intelligence gathered from the broad range of security tools deployed within their IT infrastructure. Although the market is divided between open XDR and native XDR tools, for this quadrant, ISG has considered native XDR vendors that enterprises prefer for their ability to readily offer an integrated product suite.

Some of the key trends in the XDR market include:

- Vendors have built their capabilities based on their existing leadership and presence in the endpoint detection and response (EDR) market, with some capitalizing on existing products for network, cloud and applications.
- Native XDR offers better telemetry with out-of-the-box integrations possible with existing native or proprietary products, creating a strong product suite. Enterprises have started preferring such single vendor platforms as they allow integration, reduced costs and a single console for unified management.
- XDR solutions are highly automated and correlate logs, alerts and notifications from a number of internal and external sources, delivering enhanced threat intelligence.
- Leading products also incorporate behavior- and context-led analytics engines to better understand attack vectors and the kill chain, and have gained priority over the last year.
- Most leading vendors also offer open integration with other EDR and network detection and response (NDR) products to ease integration.
- Strong XDR products are characterized by single pane of glass dashboards and a unified console that offers enhanced visibility with the context to threat management.

From the 261 companies assessed for this study, 24 have qualified for this quadrant with 10 being Leaders and one a Rising Star

Broadcom

Broadcom provides real-time threat visibility and management across on-premises, cloud or hybrid infrastructures, using a single agent for attack surface reduction, attack and breach prevention and EDR within a single console.

CrowdStrike

CrowdStrike's cloud-native, AI-powered platform notes patterns in behavior to analyze security threats and prevent them in real time. Third-party integrations help clients verify users' device posture before granting access to internal or external applications.

Fortinet

Fortinet's Security Fabric and FortiGuard Labs provide a robust foundation for XDR, with a common data structure, correlated telemetry, unified visibility, automated analytics, incident investigation, native integration and seamless interoperation.

IBM

IBM's ReaQta acquisition has helped its XDR portfolio and presence in the market. IBM capitalizes on its broad security solutions and QRadar suite to offer a strong solution with notable intelligence, correlation and threat investigation capabilities.

Microsoft

Microsoft has gained significant ground and mindshare in the market due to the ease of use and advanced capabilities of its endpoint suite of offerings. Its vast presence in the market has also enabled it to offer support to legacy products.

Palo Alto Networks

Palo Alto Networks' Cortex XDR agent is a comprehensive prevention stack that leverages AI-based analytics using a local ML model with data sets from global sources and access to the forensic investigation tool from its Unit 42 security consulting group.

Secureworks

Secureworks' flagship Taegis XDR platform draws on its decades of experience in securing large enterprises. The company is shifting to a product approach and relies on the success of this platform, which has seen double growth over the past year.

SentinelOne

SentinelOne acquired Attivo Networks, allowing it to leverage the Singularity XDR platform's capabilities to mitigate threats across endpoints, cloud workloads, IoT devices, mobile devices and data. SentinelOne has scored the highest in analytic detections with the MITRE evaluations for three consecutive years.

Trellix

Trellix (McAfee) monitors threats and behaviors to prevent sophisticated attacks by using a broad set of capabilities such as advanced detection, response, proactive and adaptive investigation and real-time threat intelligence. Trellix XDR uses AI-guided threat investigation to rapidly prioritize threats and minimize potential disruption.

Trend Micro

Trend Micro's Apex One™ is a critical component of its endpoint security offering, allowing users to add security and investigation capabilities. It offers threat detection, response and investigation with a unified console for management.

Cybereason (Rising Star) integrates endpoint telemetry with behavior analytics to detect and end cyberattacks anywhere in an enterprise's IT environment.

Security Service Edge (SSE)

Who Should Read This Section

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

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

With increasing cloud adoption, businesses need a robust security solution to protect digital assets and grant secured access to a remote workforce. These solutions focus on user-centricity and deliver security to end users through the cloud rather than allowing users to centrally access enterprise applications and databases over dedicated networks. As enterprises consolidate security and remote access services under a single framework, SSE offerings provide a unified management console for real-time visibility of security events across the entire security infrastructure. This unification helps businesses maintain compliance with various security regulations and standards by providing a single control point for security policies and configurations.

SSE solutions improve the efficiency of enterprises' security operations and are gaining popularity as a trial run before implementing secure access service edge (SASE) solutions. SSE providers must offer adequate technical support and robust integration between multiple security components. Enterprises increasingly embrace security features specific to web apps and APIs and automated advanced analytics features such as user entity behavior analytics (UEBA).

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

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

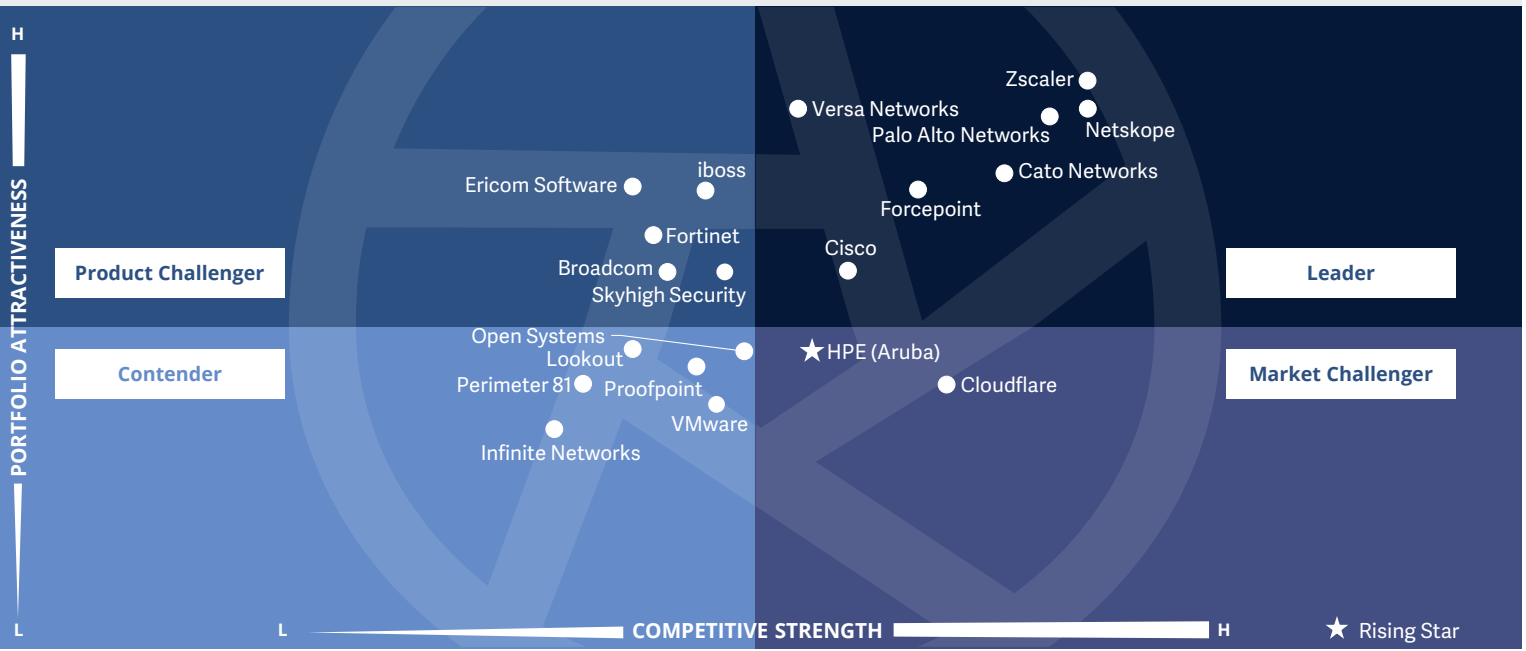
Technology professionals can benefit from this report because it outlines how SSE providers assist enterprises in adopting an enterprise-wide, zero trust framework to improve their security posture.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Security Service Edge (SSE)

Global 2023



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

Gowtham Kumar Sampath

Security Service Edge (SSE)

Definition

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

Vendors showcase experience in satisfying local, regional and domestic laws (such as for data sovereignty) for global clients.

The network components of secure access secure edge (SASE), such as SD-WAN or micro-segmentation, are not included in this quadrant but are covered in the Network - Software Defined Solutions and Services study.

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

Eligibility Criteria

1. The SSE should be offered as an **integrated solution** and must have these essential components: **zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**.
2. The above components must be **predominantly based on proprietary** software, they may **partially rely on partner solutions** but **cannot completely rely on third-party** software.
3. Vendors should have **globally located POPs** to deliver these solutions.
4. The solution should be capable of **delivering SSE to both cloud and on-premises** environments (including hybrid environments).
5. The solution should exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/ UEBA)** to detect and prevent malicious or suspicious intent.
6. The solution should be offered with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities.
7. The solution should be **fully and globally available**.

Observations

Security Service Edge is a new quadrant being analyzed at a global level as the area is in the early stages of maturity and adoption among enterprises. SSE includes solutions that enable enterprises with secure access to the cloud, ease remote work, secure edge computing and enable digital transformation.

Some of the trends being observed in the SSE space include:

- The growth in the volume of remote and hybrid workers and the transition to the cloud for apps and data have created the right environment for SSE deployments.
- Enterprises are no longer experiencing high UX with the use of virtual private networks (VPN) for secure access. Apart from the latency and reliability issues, the use of VPN also increases the probability of security breaches due to a lack of patching. Due to these drawbacks, SSE is emerging as a viable option for secure access to enterprise data.
- Enterprises are facing budget constraints and are cautious about RoI when utilizing premium options such as AWS Direct Connect or Microsoft ExpressRoute.
- Vendors are enabling a single pane of glass, unified view by combining operational and device data to deliver enhanced visibility across an enterprise with automated alerts, remote monitoring and management, as well as security monitoring.
- While the market has products offered as open and native SSE, enterprises are preferring native or converged SSE solutions to gain the benefits of an integrated suite of products and for enhanced interoperability with existing security tools, with vendors investing in continual innovation to mitigate evolving threats.
- Apart from the advantages of secure access to the cloud, enterprises leverage SSE to gain extensive visibility on shadow IT, which includes non-approved apps, devices and Internet usage.

From the 261 companies assessed for this study, 20 have qualified for this quadrant with seven being Leaders and one a Rising Star

Cato Networks

Cato Networks offers a native, converged solution that has inherent strength in its SASE capabilities. Given the market shift and interest in phasing SSE deployments to achieve SASE, the company has positioned its SSE 360 at the core of its portfolio.

Cisco

Cisco delivers its Cisco Umbrella as a converged solution, powered by an in-house AI engine and playbooks with elements of data loss prevention (DLP), extended detection and response (XDR) and threat hunting to improve visibility, threat investigation and remediation.

Forcepoint

Forcepoint has been building its SSE architecture and roadmap with strategic acquisitions such as those of BitGlass and Cyberinc, thus consolidating its data-first SSE platform. The solution is delivered on the tenets of one platform, one console and one agent.

Netskope

Netskope has gained significant growth momentum over the past year, building on its SASE capabilities and enhancing its offering with real-time controls and focus on enhancing UX and continuously improving performance.

Palo Alto Networks

Palo Alto Networks has undergone substantial growth and its SSE strategy is aimed at ZTNA 2.0, which directly addresses the requirement for securing hybrid enterprises and remote workforces with out-of-the-box configurations built on best practices.

Versa Networks

Versa Networks offers multiple products aimed at addressing the specific needs of enterprises that are struggling to deploy zero trust and have remote workers. The solution uses AI to monitor user and device security posture, thus improving threat identification accuracy.

Zscaler continues to lead the market with its leadership in the SASE space, with Zero Trust Exchange that is aimed at addressing business risks while enabling enterprises to realize the promise of digital transformation.

HPE (Aruba) (Rising Star), with its recent acquisition of Axis Security, has made inroads and found momentum in its entry into the SSE market. Combined with its existing partnership with Lookout's SSE capabilities is helping the company improve visibility into shadow IT/unsanctioned apps.

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.

Business professionals should read this report to balance data security, customer experience and privacy amidst digital transformation at the forefront of businesses today.

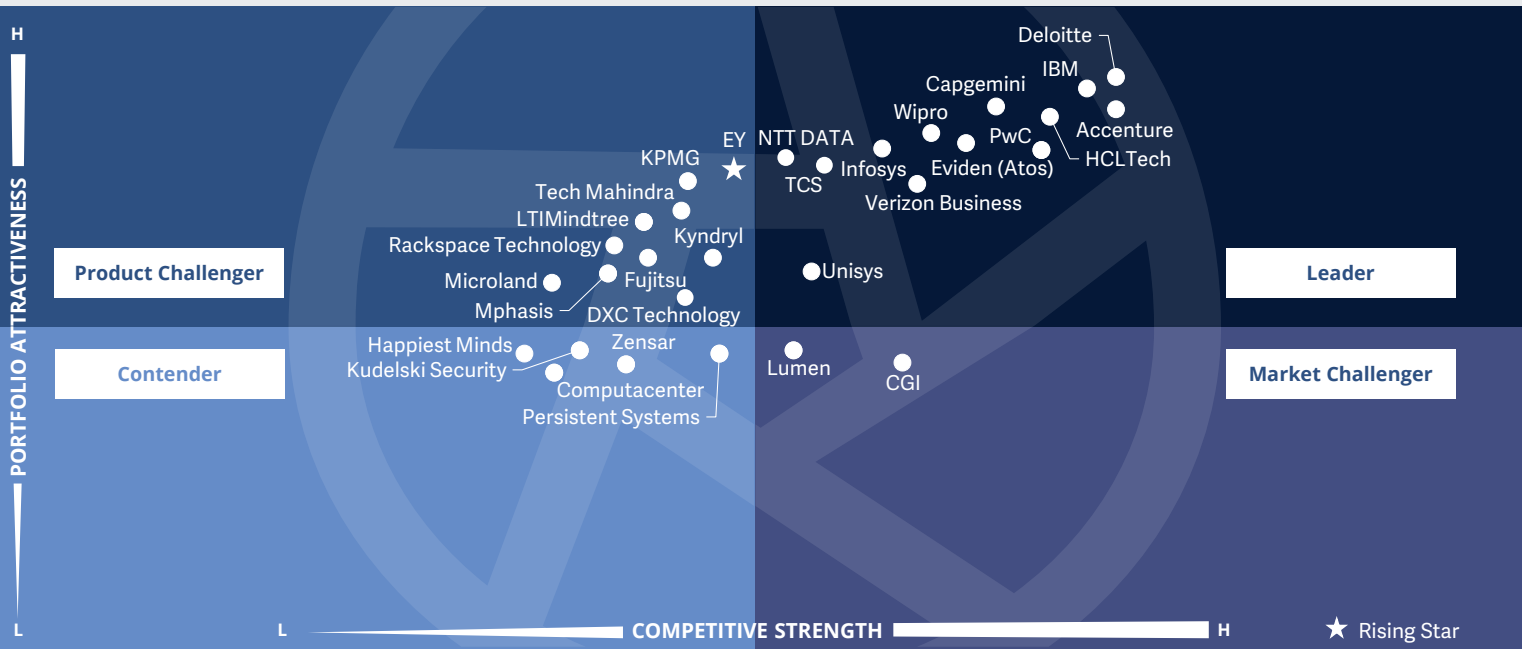
Security and data professionals should read this report to gain insights into how providers comply with security and data protection laws to stay abreast with market trends.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Technical Security Services

U.S. 2023



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

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.

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

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

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

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

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

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

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

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.

Leader

"Infosys delivers a comprehensive and constantly evolving portfolio of TSS, powered by a large pool of talented security operations teams, an extensive partner network of technology vendors and reusable artifacts and IP to deliver agility and scale."

Gowtham Kumar Sampath

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 transforms and enables clients to embrace zero trust security architecture strategy by guiding them from the current state to the target state of security technology adoption. Infosys has strategic partnerships with over 25 leading players to co-build solutions and global GTM strategies aligned to local market needs.

Strengths

Building strong competencies: The Infosys Cyber Security Center of Excellence (CoE) has strategic partnerships with over 25 technology partners, which helps to co-develop solutions and determine joint GTM strategies. Infosys has built over 100 reusable use cases, spanning areas such as IAM, infrastructure security, data security, more than 200 reusable bots and automation platforms for identity operations, SOX governance, patch management and vulnerability management.

Structured portfolio: Infosys delivers TSS aligned with its standard 4D principles of Diagnose (consulting), Design (high-level design and low-level design), Deliver (deployment and migration) and Defend (operation and optimization).

Enterprises gain comprehensive services with a large talent pool and ready to deliver, reusable assets in priority topics such as security maturity assessment, IAM, identity governance and administration (IGA), SASE, cloud security, endpoint detection and response (EDR), micro-segmentation and zero trust.

Building talent with partnerships with academia: Infosys has partnered with national (NIIT) and international (Purdue University) academic institutions to develop and nurture talent at scale. This helps in upskilling, reskilling and cross-skilling talent in advanced technologies by leveraging customized learning material, training by leading faculty, periodic assessments and hands-on experience.

Caution

Infosys should build awareness and thought leadership on its capabilities around cost optimization and rationalization of security solutions.

Infosys should seek to invest in a platform-led approach as enterprises are shifting from point-based solutions to taking a platform approach.

Strategic Security Services

Who Should Read This Section

In this quadrant, ISG evaluates service providers specializing in strategic security services (SSS) for companies across industries in the U.S. that can assess the security maturity and risk posture of these enterprises to define tailored cybersecurity strategies.

ISG defines the current positioning of SSS players in the U.S. with a comprehensive overview of the market's competitive landscape.

The increased focus of enterprises on cyber resiliency is driving the strategic security services market in U.S. Enterprises are seeking consulting services to formulate business continuity roadmaps and prioritize business-critical applications for data recovery. Cyber risk profiling and quantification services are gaining momentum as they allow businesses to prioritize their risk management efforts, based on the severity and likelihood of different cyber threats. Enterprises are also actively engaging stakeholders in cybersecurity programs since there is a strong need for creating an error-proof security architecture. With increased focus on security risks at the executive level, enterprises prioritize security awareness and training services to help board members, key business executives and employees develop cyber literacy and establish best practices to better respond to cyberattacks. In the meanwhile, there is also a significant demand from the midmarket for broad cybersecurity services that extend beyond threat detection and response.

Providers can capitalize on this demand by offering the right advisory capabilities and resources, ensuring constant technical environment maturity and developing advanced threat defense solutions tailored to their specific needs.

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

Strategy professionals should read this report to determine the vision and strategy for enterprise security. It supports decision-making on partnerships and helps in taking cost-reduction initiatives.

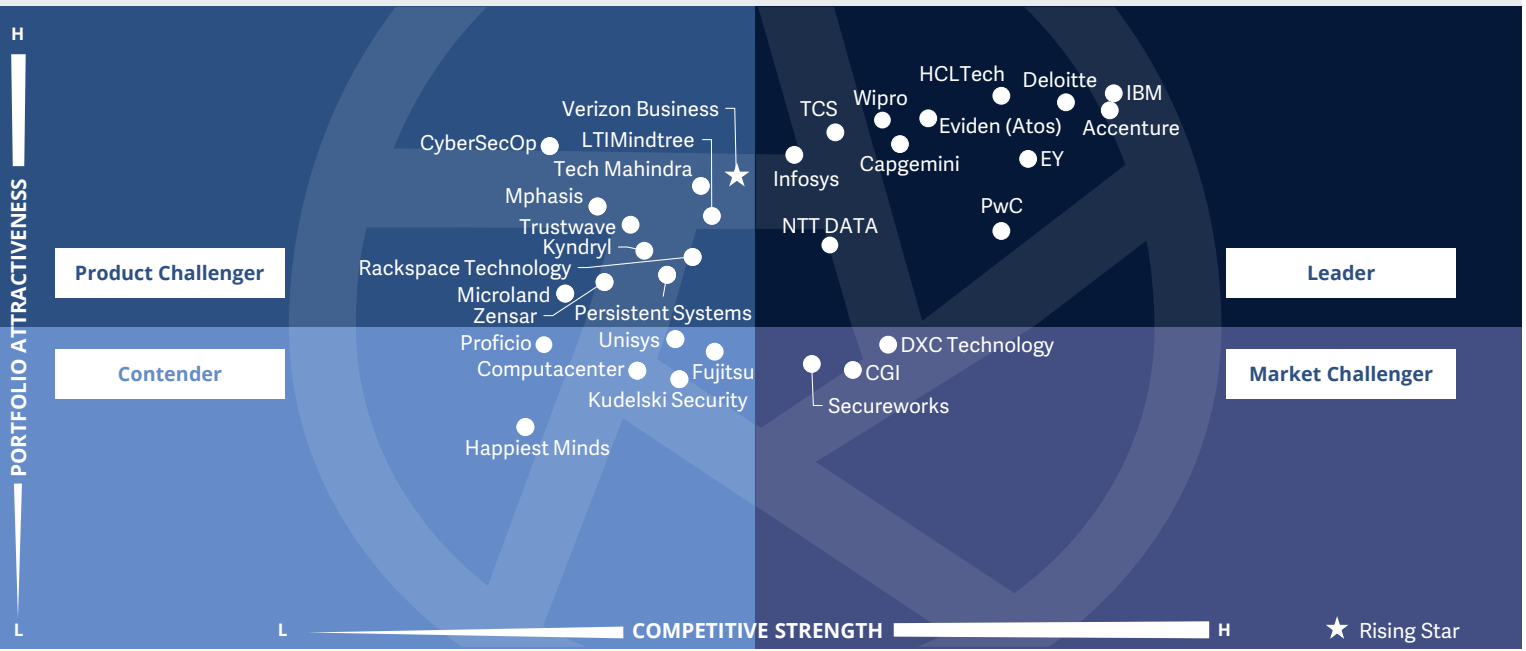
Technology professionals should read this report because it highlights the emerging trends in the security landscape. It also gives insights into providers' abilities to develop tailored security platforms.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Strategic Security Services

U.S. 2023



This quadrant assesses service providers that employ **security consultants** with extensive experience in **planning, developing and managing** end-to-end **security programs** for enterprises with **business continuity** roadmaps for **recovery**.

Gowtham Kumar Sampath

Definition

The Strategic Security Services (SSS) providers assessed for this quadrant offer consulting for IT and OT security. The services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategies for enterprises (tailored to specific requirements).

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

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

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

Eligibility Criteria

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

Observations

Advisory and consulting continue to remain the entry and foundational phase of most engagements in the cybersecurity market. Strategic security services have seen significant demand in the backdrop of enterprise digital transformation initiatives. Many enterprises are struggling with their existing security infrastructure due to the vast number of tools, solutions and systems they've adopted to address ad-hoc, independent challenges.

Some of the other developments in this space are:

- The increased focus on business resilience has created a demand for offerings that align cybersecurity with business priorities. In this environment, enterprises prefer providers that have a notable understanding of the business context with considerable vertical experience.
- Service providers are witnessing increased demand for services and solutions with next-generation technologies that address areas such as cloud security, identity and access management (IAM), secure access service edge (SASE), zero trust and IT/OT security.
- There is strong demand for integrated training and awareness offerings that foster a culture dedicated to cybersecurity among employees and board members. Providers are developing standardized trainings such as tabletop and cyber crisis exercises with red/blue/purple teaming, plus threat management, incident response and other services.
- Cybersecurity solutions and services that include in-depth intelligence with industry-aligned assessments, including supply chain risks, are gaining traction.
- Chief Information Security Officers (CISOs) are preferring solutions that quantify risks, in terms of their monetary implications. This enables them to prioritize as well as educate board members to take appropriate security measures.

From the 261 companies assessed for this study, 32 have qualified for this quadrant with 12 being Leaders and one a Rising Star

accenture

Accenture's competitive advantage stems from its significant technical expertise and expansive network of partners from the technology industry, academia and external security researchers, combined with dedicated internal cybersecurity resources.

Capgemini

Capgemini's Applied Innovation Exchange (AIE) network helps drive innovation and collaboration with clients, allowing them to contextualize their requirements within their specific industry. The approach allows enterprises to gain industry- and business-aligned advisory to mitigate risks.

Deloitte

Deloitte relies on undertaking a data discovery process before assessing the findings from both value and cost perspectives to offer advisory services, assisting enterprises with the technical and strategic aspects of data management.

EVIDEN an atos business

Eviden (Atos) has made multiple consulting-based acquisitions, including of Fidem and SEC Consult Group, particularly to enhance its advisory portfolio. It can offer vertical-specific capabilities and enable enterprises to achieve cyber resilience.

EY

EY's consulting portfolio is complemented by its next-generation security operations and response services that help enterprises build a transformation strategy and roadmap through advanced security operations.

HCLTech

HCLTech uses a 360-degree security framework and consulting approach, backed by a competent services delivery model, to provide superior levels of security to its clients, focusing on people, processes, technology and culture to maintain leadership in the market.

IBM's security intelligence operations and consulting services are aimed at helping clients develop maturity in intelligence-driven operations across their IT environments. The IBM X-Force Command Center offers first-hand knowledge-enhancing advisory capabilities.

Infosys leverages technologies that are enhanced with proprietary content, gained from vast research and rich experience obtained through use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture.

NTT DATA

NTT DATA relies on powerful risk management capability, combining security information and event management (SIEM) and IT system data directly into a proprietary application to quantify risk exposure. The company supports more than 200 different vendor technologies.

PwC

PwC's offerings are designed to support the transformation journey and allay associated risks in adopting emerging technologies for its clients. It offers a simulation platform capable of mimicking real-world threat scenarios to help CISOs address the concerns of C-level executives.

TCS' cybersecurity team has deep domain and industry experience to contextualize cybersecurity programs to specific client business needs and risk appetite. The company's focus areas include OT/IoT, cloud, forensics, incident response professional services, development, integrations and cyber risk and resiliency.

Wipro offers its clients a combination of innovative platform-based security solutions, a unique risk-based approach and the experience of more than 6,000 security experts to improve their security posture.

Verizon Business (Rising Star) offers strong advisory capabilities addressing risk, network and quality of experience for clients. It takes a unique asset-based risk quantification approach, customizing actions specific to the existing solutions and risk postures of enterprises.

Leader

"Infosys has built competency in delivering highly successful SSS projects that prioritize enterprise needs for a stable security posture. It leverages a combination of technology, talent and innovation to address risk management."

Gowtham Kumar Sampath

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. It has a strategic alliance with over 25 leading security vendors and OEMs to co-develop solutions. With approximately 6,000 dedicated cybersecurity professionals worldwide, Infosys has service capabilities around cyber advisory for IAM, GRC, data privacy and protection, vulnerability management, cloud security, infrastructure security, threat detection and response and emerging technologies.

Strengths

Bouquet of security services: Infosys offers a broad spectrum of SSS with an extensive ecosystem of partners. Infosys' security consulting capabilities span zero trust, data security, IAM, OT security and compliance, cloud security, and quantitative and cyber risk management in an effort to protect organizations from the evolving nature of cybercrimes.

Investments in talent and upskilling: Infosys leverages its global security talent pool to help enterprise clients in improving visibility, prioritizing cyber spend, aligning cybersecurity strategy with overall security strategy and driving a culture of risk-based decision-making. It focuses on upskilling through collaborations with academia to address the widening talent gap.

Investing in innovation: Infosys has a strong focus on innovations in cybersecurity, which is led by its Infosys Center for Emerging Technology Solutions (iCETS) program. The company invests a significant amount of its revenue in developing new security solutions and is continually updating its services to meet the evolving needs of its clients. Infosys recently updated its GRC and cyber advisory services to help enterprises mitigate cybersecurity risks.

Caution

Infosys should create awareness around risk quantification, supply chain risk management, technology rationalization and geopolitical risks.

Infosys should promote its capabilities in technology consolidation, rationalization and cost optimization.

Managed Security Services - SOC (Large Accounts)

Who Should Read This Section

In this quadrant, ISG evaluates providers specializing in managed security services (MSS) for large enterprises across industries in the U.S., helping them combat security threats. It also provides insights on how each provider addresses critical challenges in the market.

ISG defines the current positioning of MSS players in the U.S. with a comprehensive overview of the market's competitive landscape.

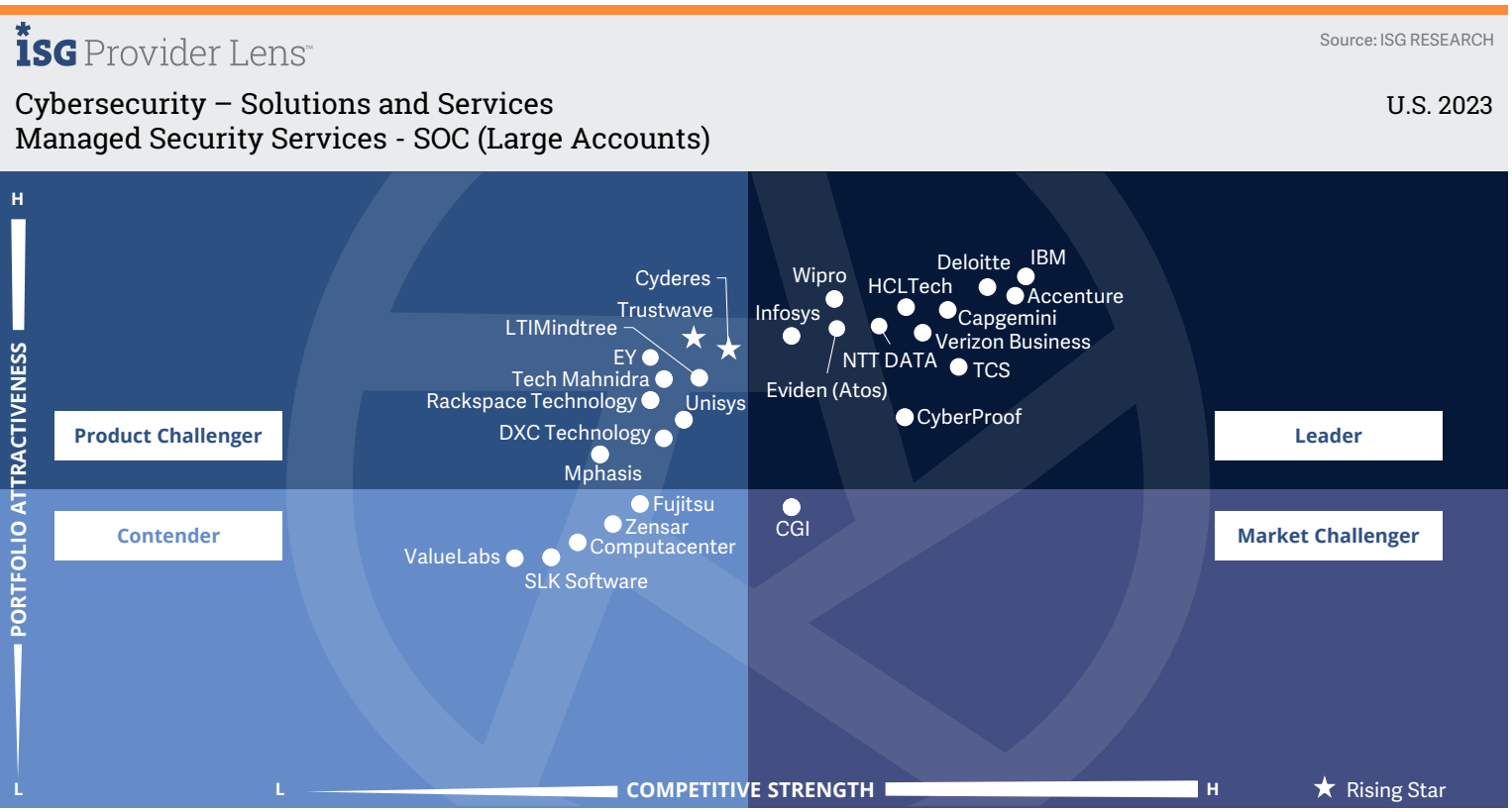
With the increased frequency and sophistication of cyber threats, there is a growing demand for security operations center (SOC) services for monitoring and the use of analytics. Enterprise clients expect their MSS providers to use advanced platforms and technologies such as AI and ML and provide expert-level services that can help detect and respond to security incidents quickly and efficiently. By incorporating threat intelligence feeds and other advanced analytics capabilities into SOC services, clients can have enhanced visibility into potential threats and ensure more proactive threat detection and response.

To minimize the impact of security incidents, reduce downtime, and prevent the loss of data and other critical assets, it is becoming essential for enterprises to implement active incident response plans and disaster recovery procedures. Enterprises are now seeking help with early-stage response and incident management and leveraging automated incident response playbooks designed to take remediated actions in response to the detected security incidents. This follows a risk-based approach, where analyst intervention is required for high-risk and complex incidents to provide critical context and expertise.

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.

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.

Business professionals should read this report because it gives valuable insights into simplifying security operations. It offers practical solutions for reducing complexity and enhancing efficiency.



This quadrant assesses providers that can combine traditional MSS with the **latest technologies**, infrastructure and **experts skilled in threat hunting** and **incident management** to fortify their clients with an **integrated cyber defense** mechanism.

Gowtham Kumar Sampath

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).

Observations

Managed security services (MSS) continue to grow in demand and have matured as a security delivery model, but there is room for the adoption of technology and service capabilities.

For this quadrant, ISG has excluded providers that have less than 40 percent of revenue from large enterprises ($5 billion or more in revenue).

Some of the other developments in this space are:

- Most providers have integrated their offerings with managed detection and response (MDR) and extended detection and response (XDR) services and are partnering with MDR platform providers. Their offerings include advanced technologies such as AI, ML and behavior analytics for enabling proactive security monitoring, alarm validation, security orchestration and automation.
- As remote working has become the new normal, MSS focus on helping clients with innovative and advanced offerings in the areas of governance, risk and compliance (GRC), identity and access controls, remote access, threat management and endpoint protection.
- One of the key factors impacting the MSS market is the lack of talented specialists that are capable of managing the current challenging requirements. Enterprises and providers realize that technology alone might not solve the problem; they require human-led expertise to address sophisticated threats.
- Providers are investing in innovations for their cyber centers or defense centers, fortifying them with superior and next-generation capabilities in threat intelligence, adversary simulations, incident response services and behavior analytics.

From the 261 companies assessed for this study, 27 have qualified for this quadrant with 12 being Leaders and two as Rising Stars.

accenture

Accenture has a 7,000-member strong cybersecurity team that applies strategy and transformational processes in client engagements. It is complemented by a network of global cyber fusion centers and SOCs, specializing in more than a dozen industry verticals.

Capgemini

Capgemini's global network of cyber defense centers (CDCs) provides advanced, analytics-driven SIEM services that combine incident detection and response and monitoring. Capgemini has developed a highly automated and scalable global cyber insurance.

CyberProof

CyberProof approaches its clients by way of use cases that aim to identify and map business risks against the most likely attack scenarios. These gaps improve detection and response capabilities against the MITRE ATT&CK matrix.

Deloitte

Deloitte is focused on MDR over other aspects of traditional managed security. It offers a proactive threat-hunting service to identify and investigate advanced threats by using telemetry from EDR tools and logging data from a cyber data lake.

EVIDEN an atos business

Eviden (Atos) MDR uses advanced security analytics on endpoints, user behavior, applications and network for deeper multi-vector detection. Atos AIsaac® leverages more than 75 AI models that enable automated hunting and data mining.

HCLTech

HCLTech takes a structured approach to its key offerings that includes managed protection services, cybersecurity monitoring and incident response, security assurance services, IAM operations, GRC operations, security of things operations and cloud-security-as-a-service operation.

IBM's managed security services can serve clients seeking dedicated teams to deliver custom solutions for specific compliance, privacy or clearance requirements and support unique service requirements, data access restrictions or bespoke client infrastructure.

Infosys relies on its strategically located cyber defense centers to deliver managed detection and response services. Its Cyber Next platform is designed to constantly monitor for threats and deliver intelligence through comprehensive protection.

NTT DATA

NTT DATA has integrated a zero-trust framework into its consulting services, extending it to integration and managed services. Its threat intelligence, ML, advanced analytics and threat behavior modeling detect both known and unknown threats that typically evade standard detection techniques.

TCS delivers services through its more than 12 threat management centers and over 200 security operations centers, most of which are client specific. It has invested in developing platforms for most of the managed security services that can integrate with existing technology stacks.

Verizon Business's advanced SOC solutions are fully customizable offerings designed for enterprises to maximize their SIEM and related security investments. It enables its clients to monitor and manage all IT assets via a single interface and dashboard.

Wipro leverages its SOCs with a 24/7/365 service delivery model to analyze system-prioritized alerts in near real time. Its Managed Security Services business caters to client needs spanning intelligence, protection, detection, remediation, response and recovery.

Cyderes

Cyderes (Rising Star) derives its strength from combining aspects of technology such as AI and automation, with intelligence to build its managed security offering and enhance IT security monitoring, incident detection and incident response times.

Trustwave

Trustwave's (Rising Star) experts and SOCs provide a combination of automated analysis by a cloud engine with human analysis for advanced threat triage, threat hunting, reverse engineering and other activities. Its investment in SpiderLabs helps in gathering and utilizing global threat intelligence.

Leader

"Infosys' MSS offerings are designed to address the burgeoning need for business resiliency. They are powered by its global cyber defense centers offering high levels of automation for threat intelligence, detection and response and vulnerability management."

Gowtham Kumar Sampath

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 provides enhanced security monitoring and managed services with hybrid tools and the Cyber Next platform, delivered from a global network of cyber defense centers. Infosys helps clients undergo security transformation by way of its wide array of proprietary tools, solution accelerators and playbooks for MSS for accelerated value realization.

Strengths

Comprehensive portfolio: Infosys delivers its Managed Protection Detection and Response (MPDR) services, addressing the need for risk resiliency among enterprises and are designed to manage the cyber risk landscape effectively. The MSS model is designed for flexibility and empowers organizations with people, processes and technologies to secure their critical assets and data.

Innovative and secure services: Infosys' MSS offerings are powered by its Cyber Next platform that provides visibility into security events and has the capability for automated responses to contain and remediate in case of security anomalies, provide intelligence about the latest threats that could damage business, ensure proactive vulnerability management and has the ability to manage security and architecture compliance. Infosys has also created multiple platforms such as Cyber Gaze, Cyber Hunt, Cyber Compass and Cyber Central and upgrades them constantly.

Investment in talent and IP: The MSS offerings are delivered through Infosys' global network of cyber defense centers strategically spread across the globe, enabling enterprises to constantly improve their cybersecurity posture. Infosys has partnerships with vendors in developing areas such as SASE, IT/OT security, IAM and cloud to upskill talent and stay ahead of technology evolution in the cybersecurity domain.

Caution

Infosys should enhance awareness and thought leadership around its incident response and recovery capabilities that address enterprise need for business resilience.

Infosys should showcase case studies to build awareness for its co-managed service capabilities as large enterprises prefer these offerings.

Managed Security Services - SOC (Midmarket)

Who Should Read This Section

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

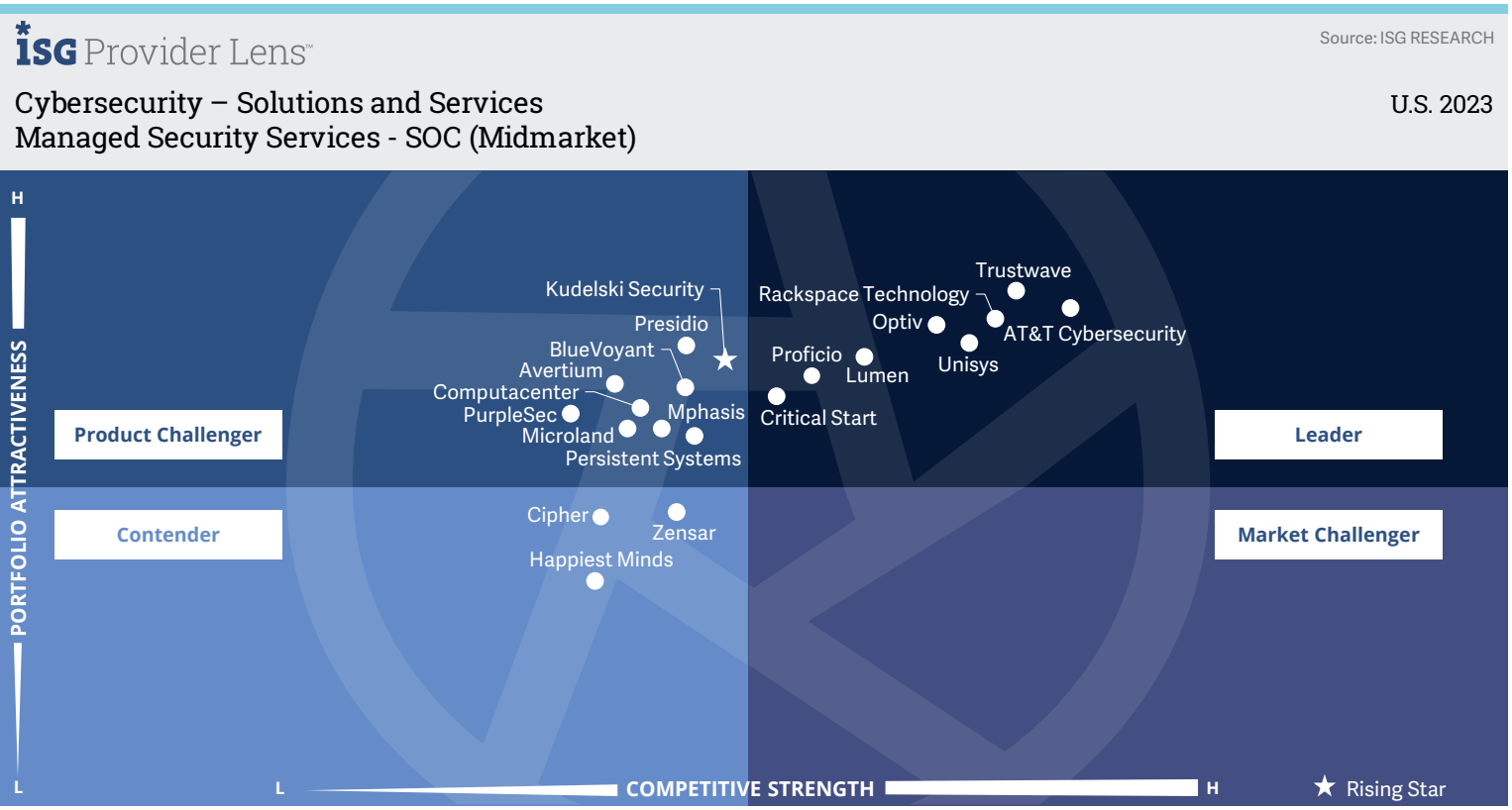
ISG defines the current positioning of MSS players in the U.S. with a comprehensive overview of the market's competitive landscape.

Midsize enterprises are currently at a high risk of cyberattacks such as ransomware and phishing due to the increased use of web- and mobile-based applications for business operations after the pandemic. Consequently, these enterprises have recognized the importance of incident detection and response capabilities to mitigate these risks and ensure business continuity after an attack. To achieve this, they need to clearly understand their existing security coverage in comparison with the latest cyberattack techniques. Therefore, they are increasingly focusing on improving their threat detection capabilities through managed detection and response (MDR) services. These services enable them to detect, analyze, investigate and quickly respond to cyber threats using various threat mitigation and containment approaches. Enterprises expect MDR providers to include security awareness and training as a part of their offering since they lack the competence to defend themselves against sophisticated cyberattacks and implement innovative security plans.

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 gives valuable insights into simplifying security operations. It offers practical solutions for reducing complexity and enhancing efficiency.

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



This quadrant assesses providers that can combine traditional MSS with the **latest technologies**, infrastructure and **experts skilled in threat hunting** and **incident management** to fortify their clients with an **integrated cyber defense** mechanism.

Gowtham Kumar Sampath

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).

Observations

Demand for managed security services (MSS) continues to grow and the services have matured as a security delivery model, but there is room for the adoption of technology and service capabilities.

For this quadrant, ISG has excluded providers that have less than 40 percent of revenue from midmarket enterprises (revenue less than $5 billion).

Some of the other developments in this space are:

- Most providers have integrated their offerings with managed detection and response (MDR) and extended detection and response (XDR) services and are partnering with MDR platform providers. Their offerings include advanced technologies such as AI, ML and behavior analytics for enabling proactive security monitoring, alarm validation, security orchestration and automation.
- As remote working has become the new normal, MSS providers focus on helping clients with innovative and advanced offerings in the areas of governance, risk and compliance (GRC), identity and access controls, remote access, threat management and endpoint protection.
- One of the key factors impacting the MSS market is the lack of talented specialists that are capable of managing the current challenging requirements. Enterprises and providers realize that technology alone might not solve the problem; they require human-led expertise to address sophisticated threats.
- Providers are investing in innovations for their cyber centers or defense centers, fortifying them with superior and next-generation capabilities in threat intelligence, adversary simulations, incident response services and behavior analytics.

From the 261 companies assessed for this study, 20 have qualified for this quadrant with eight being Leaders and one a Rising Star.

AT&T Cybersecurity

AT&T Cybersecurity leverages its rich ecosystem of cybersecurity technologies and strategic alliances to offer global insights and Alien Labs™- powered eight SOCs to deliver tactical threat intelligence, enabling resilient threat detection and response.

Critical Start

Critical Start's proprietary platform and third-party intelligence help define and develop new detection methods. This also helps in implementing new techniques and on improving its threat research and intelligence platform.

LUMEN

Lumen Technologies' investment in its labs and a strong partner ecosystem enhance the intelligence that feeds its AI-powered adaptive platform, resulting in advanced threat detection and response capabilities to quickly neutralize threats before an attack.

Optiv

Optiv takes a consulting and advisory approach to its managed services, delivering strong capabilities with a comprehensive portfolio that identifies vulnerabilities and ensures a suitable threat response. Its advanced Fusion Center Operations leverage smart automation and data fusion to upgrade SOC maturity.

PROFICIO

Proficio offers MSS that cater to client needs, spanning intelligence, protection, detection, remediation, response and recovery. Its integrated, automated and comprehensive capabilities help improve visibility into a client's entire data center and cloud environment.

Rackspace Technology

Rackspace Technology leverages its in-house R&D and proprietary security architecture with decades of experience in handling data center infrastructure to create a robust and integrated offering. Security platforms are integrated into management tools to give customers one view of their organization's vulnerability and threats.

Trustwave

Trustwave's experts and SOCs provide a combination of automated analysis by a cloud engine with human analysis for advanced threat triage, threat hunting, reverse engineering and other activities. Its investment in SpiderLabs helps in gathering and utilizing global threat intelligence.

Unisys

Unisys leverages its network of global delivery centers to provide flexible support based on client needs. It also delivers a methodology based on the IT Infrastructure Library (ITIL), with annual ISO and SSAE audits, helping clients meet compliance requirements.

Kudelski Security

Kudelski Security's (Rising Star) offerings are designed to specifically address the requirements of midmarket enterprises, and are powered by the FusionDetect™ Platform. The services are highly customized and delivered from SOCs that use proprietary and industry-leading technologies.

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

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

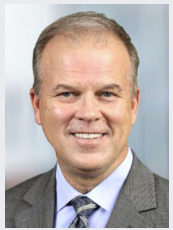
Bhuvaneshwari Mohan

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™

JUNE, 2023

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES