ISG Provider Lens™

Cybersecurity – Solutions and Services

Managed Security Services - SOC (Midmarket)

Analyzing the cybersecurity market, comparing provider portfolio attractiveness and competitive strengths

Customized report courtesy of:

unisys

QUADRANT REPORT | JULY 2024 | U.S.

Table of Contents

Report Author: Gowtham Sampath and Dr. Maxime Martelli

Sophisticated threats and emerging technologies challenge enterprise growth and resilience objectives

In 2023, several high-profile data breaches and cyberattacks strengthened and drove the growth of the U.S. cybersecurity market. Data breaches in 2023 catapulted to 3,205 compared to 1,802 in 2022, affecting over 353 million individuals with compromises, including data breaches, leakage and exposure. The healthcare sector remained the primary target, witnessing more than double the number of data breach incidents compared to 2022, followed closely by the financial services industry, which experienced 744 incidents and marked a substantial increase.

Subsequently, the U.S. government heightened pressure on businesses to enhance their cybersecurity posture, resulting in several recent regulatory changes that are affecting the market:

SEC Cybersecurity Rule (July 2023): This mandate necessitates publicly traded companies to disclose cybersecurity incidents within four business days of identifying them as *material*" influencing shareholder investment decisions.

FTC Safeguards Rule update (2023): This update broadens the Safeguards Rule's scope, compelling non-bank financial institutions to report specific data breaches and addressing the security of health, financial and children's data. Compliance with these updates is critical for covered institutions.

State-level privacy laws: Regulations such as the California Consumer Privacy Act (CCPA) and similar laws in Virginia, Colorado, Utah and Connecticut establish a complex network of compliance requirements that businesses must adhere to depending on their location and the data they gather.

Potential federal data privacy legislation: Momentum is growing for federal data privacy legislation in the U.S. While the specifics remain uncertain, such legislation could profoundly affect how businesses gather, store and utilize consumer data.

CISOs are **prioritizing dynamic risk** management, **user awareness** and **cost-effectiveness.**

Executive Summary

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500); The NYDFS Cybersecurity Regulation establishes cybersecurity standards for financial services firms in New York. It mandates organizations to establish a strong cybersecurity program, appoint a Chief Information Security Officer (CISO), perform risk assessments, enforce access controls and report cybersecurity incidents to the NYDFS.

The U.S. cybersecurity market is dynamic, consistently pushing enterprises to grapple with evolving threats and adapt to novel technologies. These incidents have exposed vulnerabilities in critical infrastructure and software supply chains, necessitating CISOs to re-evaluate security strategies and prioritizing resilience planning.

ISG has identified the following challenges faced by enterprises in 2023 and early 2024:

Complying with a shifting regulatory landscape (2023-2024): The U.S. regulatory environment is becoming increasingly complex. Recent changes, such as the SEC Cybersecurity Rule, mandating breach disclosure; FTC Safeguards Rule updates (2023), expanding data security requirements; and the potential for a federal data privacy law create a compliance minefield. Keeping up with these changes and ensuring adherence significantly burden already stretched resources.

Mounting costs and ROI concerns: Boards and stakeholders often view cybersecurity budgets as a cost center. Implementing effective security measures requires significant investment in tools, technologies and personnel. Justifying these expenses with a clear ROI is a constant battle for enterprises. Metrics must go beyond basic security incidents prevented and demonstrate how strong security protects brand reputation, customer trust and, ultimately, business continuity.

Third-party risk management: Enterprises expose themselves to additional security risks by relying on third-party vendors and partners. Managing these risks requires robust vendor risk management programs, adding complexity to the overall security strategy.

Tool and technology consolidation: The proliferation of cybersecurity tools can lead to operational inefficiencies and information silos. Businesses are focusing on tool consolidation and adopting Security Information and Event Management (SIEM) platforms for centralized log management and threat detection.

Technology rationalization: Rationalizing existing security technology stacks to identify and eliminate redundant or outdated tools is becoming a priority. This helps streamline security operations and optimize resource allocation.

The talent gap and the cybersecurity skills shortage: Finding and retaining qualified cybersecurity professionals is a major hurdle for enterprises. The talent pool is not growing fast enough to keep pace with the evolving threat landscape and increasing demand for skilled personnel. This talent shortage creates a bottleneck, hindering the implementation of effective security strategies.

Evolving threat landscape (2023-2024): Cyberattackers are constantly innovating. Recent trends such as the rise of ransomware-as-a-service (RaaS) models, the potential misuse of generative AI (GenAI) for sophisticated phishing attacks and the growing focus on exploiting vulnerabilities in critical infrastructure and software supply chains necessitate continuous adaptation of security strategies. Enterprises need to stay ahead of the curve and anticipate future threats.

Communication and business acumen: Enterprises must translate complex cybersecurity risks and solutions into clear, actionable language for business leaders and boards. Strong communication and business acumen are crucial for gaining buy-in for security investments and ensuring that cybersecurity strategy aligns with overall business objectives.

Prioritization and resource allocation: With limited resources and a vast threat landscape, businesses need to prioritize vulnerabilities and allocate resources effectively. This requires a data-driven approach to risk management, focusing on areas with the highest potential impact in the event of a breach.

Although enterprises face complex and sophisticated threats, the market is responding to specific solutions and services that are growing in potential, including:

Passwordless IAM: Eliminating passwords through multifactor authentication (MFA) and other passwordless methods can significantly reduce the risk of compromised credentials.

Digital forensics and incident response (DFIR): The increasing frequency of cyberattacks drives the demand for robust DFIR capabilities. Investing in DFIR services ensures efficient response and investigation during security incidents.

Cybersecurity insurance: Rising cyberattacks prompt increased adoption of cybersecurity insurance. CISOs need to carefully evaluate insurance policies and ensure adequate coverage for potential breaches.

Quantum computing: While still in its nascent stages, the potential impact of quantum computing on cryptography necessitates a forward-thinking approach. CISOs should explore *quantum-safe* encryption solutions to prepare for potential future threats.

Risk management: Implementing robust risk management frameworks is crucial for identifying, assessing and mitigating cybersecurity risks. CISOs need to adopt a data-driven approach to risk management, prioritizing vulnerabilities based on potential impact and likelihood.

ISG's analysis also reveals that enterprises are investing in trending and emerging technologies, including:

GenAI: While GenAI offers exciting possibilities for automation and threat detection, its potential misuse for creating sophisticated phishing attacks or crafting social engineering tactics demands a proactive approach to defense strategies. CISOs need to consider implementing security awareness training programs specifically addressing AI-generated threats.

Zero trust: The growing adoption of zero trust architectures (ZTAs), emphasizing continuous verification, minimizes the attack surface and reduces the impact of breaches. However, managing zero trust implementations adds complexity and requires skilled personnel to configure and maintain effectively.

Automation: Automating routine security tasks and leveraging AI and ML for real-time threat detection and anomaly identification are crucial for improving overall security posture. However, concerns around bias in AI algorithms and the need for skilled personnel to interpret and manage these systems remain challenges.

The cybersecurity landscape presents distinct challenges and priorities for CISOs in large enterprises and SMBs. ISG analysis reveals the differences in the approach and challenges that would help service providers align their offerings and capabilities to grow in the U.S. market. The study also reveals that service providers in the quadrants have showcased exceptional portfolios and competitiveness across these areas.

Large enterprises:

ZTA implementation: Large enterprises will prioritize ZTA implementation to avoid traditional perimeter-based security and minimize the attack surface. This requires significant investment in access controls, identity management and continuous verification processes.

Cloud security expertise: As cloud adoption rises, securing cloud environments remains a top priority for large enterprises. This includes workload protection, data encryption and robust cloud infrastructure security controls.

Advanced threat detection and response (AT&DR): Large enterprises are increasingly vulnerable to sophisticated cyberattacks. Investing in advanced threat detection and response solutions with AI and ML capabilities will be crucial for identifying and neutralizing threats before they escalate.

Third-party risk management: Large enterprises with complex supply chains face significant third-party security risks. Strengthening vendor risk management programs and conducting thorough security assessments of third-party vendors will be a key CISO priority in 2024.

Compliance with evolving regulations: The ever-changing regulatory landscape, with updates to the SEC Cybersecurity Rule and potential federal data privacy legislation, necessitates ongoing compliance efforts. Large enterprises will need dedicated resources to stay abreast of regulatory changes and ensure adherence.

SMBs:

Cost-effective security solutions: Budget constraints are a major concern for SMBs. Finding cost-effective security solutions, such as managed security services (MSS) or cloud-based security offerings, will be a top priority for SMB CISOs. These solutions offer access to expertise and technologies that might be out of reach for in-house teams.

User education and security awareness training: The human element remains a critical vulnerability for SMBs. Prioritizing user education and security awareness training can significantly reduce the risk of phishing attacks and social engineering scams.

Incident response planning and readiness: While large-scale attacks might seem like a distant threat, having a well-defined incident response plan and conducting regular simulations will be crucial for SMBs to recover effectively from any security breach.

Patch management and vulnerability management: Keeping software and systems up to date with the latest security patches is essential for SMBs. Automating patch management processes and prioritizing critical vulnerabilities will help them mitigate common exploits.

Data security and privacy: Even with limited data collection compared to large enterprises, SMBs still handle sensitive customer information. Implementing strong data security practices and ensuring compliance with relevant data privacy regulations are essential for SMB CISOs.

Key differences in priorities:

Focus on advanced technologies: Large enterprises can invest in cutting-edge solutions, such as ZTA and advanced threat detection, while SMBs may prioritize more fundamental security measures.

Budgetary constraints: Cost-effectiveness is a major concern for SMBs, influencing their choice of security solutions.

In-house expertise: Large enterprises have the resources to build dedicated security teams, whereas SMBs often rely on outsourced solutions or limited in-house expertise.

Compliance complexity: Large enterprises face a more complex regulatory landscape with stricter compliance requirements.

Threat landscape focus: Large enterprises are more likely to be targeted by sophisticated attacks, while SMBs may be more vulnerable to common phishing attempts or malware infections.

Notes of quadrant positioning: This study assesses several security services and solution providers that offer similar portfolio attractiveness in most quadrantsquali. This reflects the relative maturity of the market, providers and offerings. It is understood that circumstances vary, and not all entities are equal. 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 may also observe similarities in portfolio axis (vertical axis) positioning with providers included in the ISG Provider Lens™ U.S. Public Sector Cybersecurity Solutions and Services study.

Enterprises in the U.S. market face multifaceted and complex cybersecurity challenges. CISOs are navigating a rapidly evolving regulatory landscape and must contend with increasingly sophisticated threats while managing constrained budgets. Enterprises are adopting a proactive and comprehensive approach, leveraging advanced technologies, implementing robust security measures and investing in workforce development.

As enterprises increasingly rely on cloud applications, remote workforces and interconnected systems, the complexity and sophistication of cyberthreats have escalated. This dynamic environment requires advanced security measures that go beyond traditional perimeter defenses. As cyberthreats continue to grow in sophistication, the adoption of such cutting-edge security measures will be essential for maintaining a strong cybersecurity posture.

The necessity for advanced cybersecurity solutions such as extended detection and response (XDR) and security service edge (SSE) is driven by the evolving threat landscape, increased cloud adoption and the need for comprehensive security frameworks. These innovative platforms address critical challenges faced by enterprises, ensuring resilient and efficient protection of digital assets and business operations.

Some of the existing challenges are listed below:

Complexity in security architectures: Managing disparate security tools and solutions can lead to inefficiencies and gaps in protection, making integrated platforms such as XDR and SSE critical for streamlined operations.

Reactive threat detection and response: Traditional security measures often fail to provide real-time visibility and response capabilities. XDR leverages advanced analytics and automation to detect, investigate and respond to threats across various endpoints.

Lax data privacy and governance: Ensuring data privacy and governance in a decentralized IT environment is challenging. SSE offers centralized security policies and governance frameworks to manage data protection effectively.

Lack of scalability and performance: As organizations grow, their security solutions must scale accordingly without compromising IT or business operational performance. XDR and SSE are designed to provide scalable, high-performance security across expansive and evolving IT landscapes.

Poor user experience: Balancing robust security with a seamless user experience is essential. Enterprises require innovative solutions designed to be minimally intrusive while maximizing protection and security posture.

Extended detection and response (XDR) trends

The XDR market is witnessing various innovative trends to improve threat detection, response and the overall security posture. XDR solutions are gaining traction due to their ability to collect and correlate data across multiple security layers, including emails, endpoints, servers, cloud workloads and networks, providing a multifaceted view of the organization's security posture.

The key trends in the XDR space are listed below:

Integration of AI and ML: One of the latest trends in XDR is the integration of AI and ML algorithms to enhance threat detection and response capabilities. These advanced technologies enable XDR platforms to identify complex threats, predict potential attacks and automate response actions, thereby reducing the burden on security teams.

Convergence with other security solutions: Another emerging trend is the convergence of XDR with other security solutions such as security information and event management (SIEM) and security orchestration, automation and response (SOAR). This convergence creates a unified security architecture, improving threat visibility, detection and response times while streamlining security operations.

Threat intelligence integration: XDR platforms increasingly integrate with threat intelligence feeds to enhance threat detection and response. Combining internal security data with external threat intelligence allows XDR solutions to provide contextual insights into potential threats. This helps security teams to make informed decisions and prioritize their response efforts.

XDR for cloud and SaaS environments: As organizations continue to adopt cloud and SaaS applications, XDR solutions are expanding their coverage to include these environments. Cloud-native XDR platforms can monitor and secure cloud workloads, containers and serverless applications while providing visibility on SaaS application usage and potential risks.

Threat and compromise detection capabilities: XDR solutions incorporate user and entity behavior analytics (UEBA) capabilities to detect insider threats and account compromises.

UEBA uses ML algorithms to analyze user behavior patterns and identify anomalies that could indicate malicious activity, helping organizations detect and respond to threats that might otherwise go unnoticed.

XDR enhancing security for ICS and OT environments: As the threat landscape for industrial control systems (ICS) and OT environments continues to evolve, security experts are tailoring XDR solutions to address these systems' unique security challenges. XDR for ICS and OT can monitor and analyze data from specialized industrial control systems, detecting threats early and enabling rapid response to minimize potential damage.

Compliance and regulatory support: With the increasing focus on data privacy and security regulations, organizations are enhancing XDR solutions to meet compliance requirements.

Enterprises are navigating a dynamic landscape characterized by increased adoption of cloud environments and evolving cyberthreats, necessitating security solutions that are scalable, flexible and robust. SSE solutions address these challenges by providing centralized visibility, advanced threat detection powered by AI and ML and seamless policy enforcement across all endpoints. By adopting SSE, organizations can ensure secure access to applications and data from any location, maintain compliance with regulatory standards and safeguard against data breaches and insider threats, thereby supporting business continuity and resilience in the face of a constantly changing threat landscape.

Challenges addressed by SSE Solutions are listed below:

Security of cloud applications: The proliferation of cloud services creates security complexities. SSE centralizes security policies and enforces consistent access control across all cloud applications.

Remote workforce security: With more employees working remotely, traditional perimeter-based security models become less effective. SSE provides secure access to cloud applications from any location, regardless of the device.

Data loss prevention (DLP): Data breaches and leaks are major concerns. SSE helps prevent sensitive data from being exfiltrated by enforcing DLP policies and data encryption across cloud services.

Shadow IT: Employees often use unsanctioned cloud applications. SSE provides visibility into shadow IT usage and allows for secure access control even for unapproved applications.

Complexity of security management: Managing multiple security point solutions can be complex and time consuming. SSE offers a unified platform for managing security policies across all cloud applications.

The SSE market is experiencing significant growth due to the increasing adoption of cloud applications, remote workforces and the need for a consolidated security approach.

Key trends shaping the market are listed below:

Cloud-native architectures: As businesses migrate to cloud environments, they adopt cloud-native security solutions that scale with workloads and support dynamic, distributed setups.

Convergence of security and networking: Thereis a growing trend to integrate networking and security functions into a single platform, streamlining operations and reducing the complexity of managing security and network performance.

Integration of SWGs and CASBs: Secure web gateways (SWGs) and cloud access security brokers (CASBs) are converging into comprehensive SSE solutions, providing unified threat protection, DLP and access control for cloud services.

Emphasis on zero trust security: SSE solutions are increasingly incorporating zero trust principles, granting access based on least privilege and continuous verification, enhancing security by minimizing the attack surface and lateral movement within the network.

SASE adoption: SSE is a foundational element of secure access service edge (SASE) architectures, which integrate network security and cloud access security into a unified cloud-delivered service.

AI and ML integration: SSE solutions leverage AI and ML to automate threat detection, improve anomaly identification and personalize security policies based on user behavior.

Focus on user experience: Balancing security with UX is crucial. SSE solutions are designed to be transparent to users, ensuring minimal disruption to their workflow while maintaining robust security.

Unified management consoles: There is a trend toward developing unified management interfaces that consolidate various security functions into a single dashboard, simplifying administration and providing a holistic view of the security landscape.

User and entity behavior analytics (UEBA): UEBA tools analyze the behavior of users and entities to identify potential security threats. By establishing baselines and detecting deviations, UEBA helps identify anomalous activities.

Identity-centric security: Emphasis on identity and access management (IAM) is becoming central to security strategies, ensuring that only authenticated and authorized users can access resources.

As businesses prioritize robust cybersecurity and navigate the complexities of the digital environment, the demand for innovative solutions such as XDR and SSE will be at the forefront of safeguarding their digital assets. As cyberthreats become more sophisticated and businesses rely increasingly on cloud services, XDR and SSE will be crucial in safeguarding enterprise security.

Provider Positioning

Page 1 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Accenture	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Leader
AT&T Cybersecurity	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger	Not In
Avatier	Product Challenger	Not In	Not In	Not In	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	Not In	Not In	Product Challenger	Not In
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BlackBerry	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BlueVoyant	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Product Challenger	Not In

Provider Positioning

Page 2 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Contender	Product Challenger	Contender	Product Challenger	Contender	Market Challenger	Not In
Capgemini	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Rising Star ★
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CDW	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger	Not In	Market Challenger	Not In	Not In
CGI	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger	Not In	Market Challenger	Not In	Product Challenger
Check Point Software	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 3 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Cognizant	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In
Computacenter	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Contender	Contender	Not In
Critical Start	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Leader	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	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	Not In	Not In	Not In
CyberArk	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
CyberSecOp	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Contender	Contender	Not In

Provider Positioning

Page 4 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Cyderes	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Product Challenger
Deloitte	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Leader
DXC Technology	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger
EmpowerID	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Eviden	Product Challenger	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Product Challenger
EY	Not In	Not In	Not In	Rising Star ★	Not In	Leader	Not In	Rising Star ★	Not In	Leader

Provider Positioning

Page 5 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Fischer Identity	Contender	Not In	Not In	Not In	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	Not In	Not In	Not In
Fortinet	Market Challenger	Leader	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Fortra	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In	Product Challenger	Not In	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Globant	Not In	Not In	Not In	Contender	Not In	Market Challenger	Not In	Contender	Not In	Not In
GTT	Not In	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger	Not In	Market Challenger	Not In
Happiest Minds	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Contender	Not In

Provider Positioning

Page 6 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
HCLTech	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Not In
HPE (Aruba)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Leader
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Not In
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Product Challenger	Not In	Leader	Not In	Product Challenger	Not In	Leader
Kroll	Not In	Not In	Not In	Product Challenger	Not In	Rising Star ★	Not In	Leader	Not In	Leader

Provider Positioning

Page 7 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Kudelski Security	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
Kyndryl	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Product Challenger
Lookout	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In	Contender
Lumen Technologies	Not In	Not In	Not In	Market Challenger	Not In	Product Challenger	Not In	Market Challenger	Not In	Not In
ManageEngine	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Microland	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Rising Star ★	Contender
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Mphasis	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In

Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In
Okta	Leader	Not In	Not In	Not In	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	Not In	Not In	Not In
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Optiv	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Product Challenger
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Perimeter 81	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Persistent Systems	Not In	Not In	Not In	Not In	Rising Star ★	Not In	Rising Star ★	Not In	Product Challenger	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Presidio	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Product Challenger	Not In
Proficio	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
PurpleSec	Not In	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Product Challenger	Not In
PwC	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Not In	Not In	Leader
Rackspace Technology	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Leader	Product Challenger	Leader	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 10 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
RSA	Market Challenger	Not In	Not In	Not In	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	Not In	Not In	Not In
Saviynt	Leader	Not In	Not In	Not In	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	Not In	Not In	Not In
Secureworks	Not In	Product Challenger	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
SecurityHQ	Not In	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Product Challenger	Not In
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 11 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
SLK Software	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Stefanini	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In	Not In	Not In
Syntax	Not In	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Not In	Not In
TCS	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Leader
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Thales	Market Challenger	Not In	Not In	Contender	Leader	Contender	Leader	Not In	Not In	Not In
Trellix	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

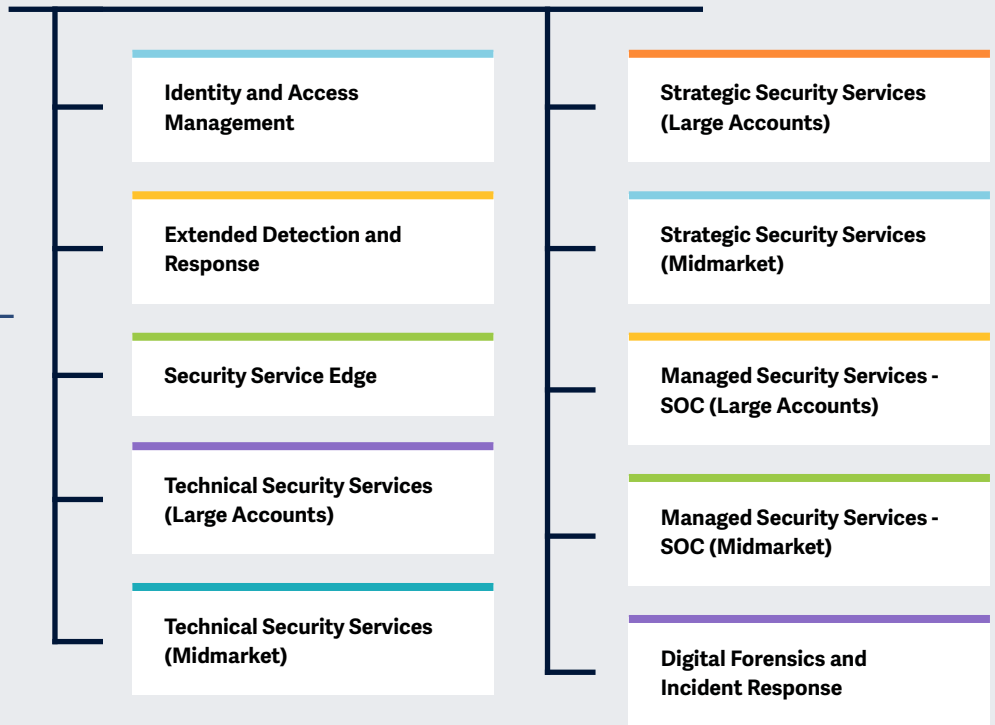
Provider Positioning

Page 12 of 12

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services (Large Accounts)	Technical Security Services (Midmarket)	Strategic Security Services (Large Accounts)	Strategic Security Services (Midmarket)	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Digital Forensics and Incident Response
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Product Challenger
Unisys	Not In	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Contender
Verizon Business	Not In	Not In	Not In	Leader	Not In	Product Challenger	Not In	Leader	Not In	Product Challenger
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Contender
Wipro	Not In	Not In	Not In	Leader	Not In	Leader	Not In	Leader	Not In	Product Challenger
Zensar Technologies	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Product Challenger	Not In
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Key focus areas for the **Cybersecurity – Solutions and Services**

Simplified Illustration Source: ISG 2024



Definition

The current cybersecurity landscape is dynamic, with changes occurring rapidly due to emerging threats, technological advancements and evolving regulatory environments.

The year 2023 could be termed as tumultuous from a cybersecurity perspective; the year saw increased sophistication and severity in the attacks. Enterprises responded by increasing their investments in cybersecurity and prioritizing relevant initiatives to prevent attacks and improve their security posture. Learnings from prior attacks in 2022 led to executives and businesses of all sizes and across industries investing in measures countering cyber threats. AI brings both challenges and opportunities to cybersecurity, offering automation for analysis and detection while posing risks of bias and misuse.

From an enterprise perspective, even small businesses realized their vulnerability to cyber threats, fueling demand for (managed) security and cyber resiliency services that would enable recovery and operation restoration post-cyber incidents.

Therefore, service providers and vendors are offering services and solutions that help enterprises ensure recovery and business continuity.

Security services providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats, understanding the transformative impact of technologies such as AI and ML, and staying attuned to evolving regulatory frameworks on data protection, such as NIS-2, in the European Union.

Cybercriminals exploited large-scale vulnerabilities, persistently using ransomware to disrupt business activities, specifically healthcare, supply chain and public sector services.

Consequently, businesses started to invest in solutions such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR), and cloud and endpoint security. 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 augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.

Scope of the Report

This ISG Provider Lens quadrant report covers the following Ten quadrants for services/ solutions: Identity and Access Management, Technical Security Services (Large Accounts), Technical Security Services (Midmarket), Strategic Security Services (Large Accounts), Strategic Security Services (Midmarket), Managed Security Services - SOC (Large Accounts), Managed Security Services - SOC (Midmarket), Digital Forensics and Incident Response, vendors offering Security Service Edge and Extended Detection and Response solutions are analyzed and positioned from a global perspective rather than individual regions.

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

- Transparency on the strengths and weaknesses of relevant providers/software vendors
- A differentiated positioning of providers by segments, including Large Accounts and Midmarket Technical Security Services (TSS), Strategic Security Services (SSS), Managed Security Services – SOC (MSS-SOC)
- Focus on the regional market specifically for Digital Forensics and Incident Response (DFIR)

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

Provider Classifications

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

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

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

- **Number of providers in each quadrant:** IISG 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 (exceptionsare 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.

Managed Security Services - SOC (Midmarket)

Who Should Read This Section

This report is essential for midmarket enterprises in the U.S. evaluating managed security service providers (MSSPs). It assesses providers offering IT and OT security monitoring and IT infrastructure management services. Midsize enterprises prioritize comprehensive security solutions for endpoints, networks and cloud environments, emphasizing cloud-native security, threat detection and data protection.

Proactive threat management is crucial, relying on advanced analytics and threat intelligence. Challenges include resource constraints and skill shortages, driving the need for cost-effective solutions and skilled cybersecurity professionals from service providers. Customized solutions tailored to industry-specific requirements and regulatory needs are expected.

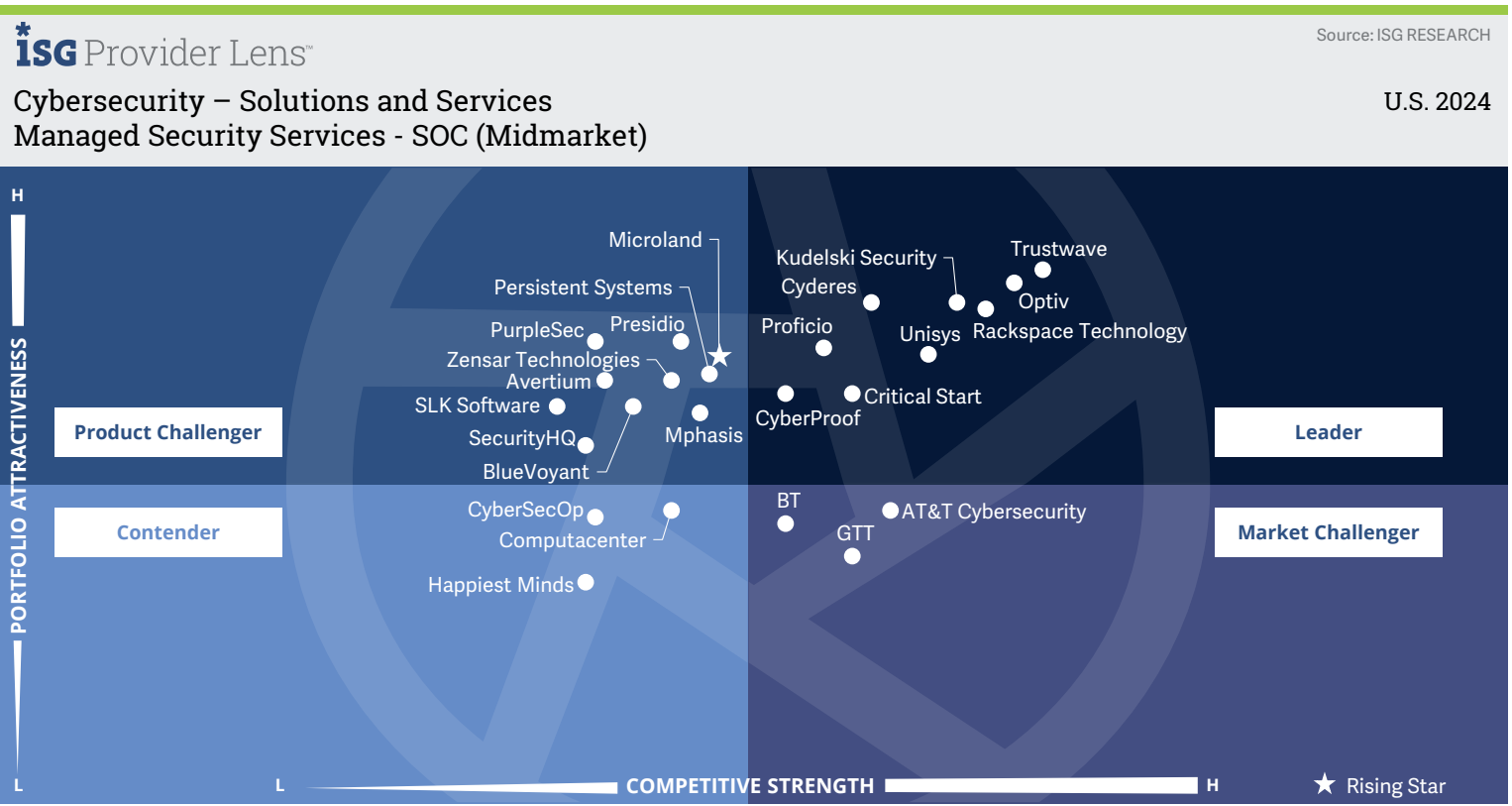
Midmarket enterprises increasingly adopt managed detection and response (MDR) services and Zero Trust security framework, expecting service providers to assist in implementing zero trust principles, including continuous authentication and least privilege access controls.

Strategy professionals responsible for information security strategies should read this report to ensure security alignment with business objectives.

Security professionals implementing and managing cybersecurity measures should read this report to safeguard their IT systems and data.

Technology professionals evaluating and selecting cybersecurity solutions should read this report to protect their technology infrastructure

Risk managers should read this report to identify, assess and mitigate cybersecurity risks that could impact their operations and objectives.



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

Gowtham Sampath

Definition

The providers assessed in the MSS-SOC quadrant offer services related to the continuous monitoring of IT and OT security infrastructures and management of IT infrastructure 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 response.

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional MSS with innovation to fortify 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 and infrastructure. They must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, 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** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, Security Information and Event Management (SIEM) services,** security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. **Manage own SOCs**
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models

Observations

The U.S. MSS market for midsize enterprises is witnessing significant growth, driven by several key trends observed by ISG:

Midsize enterprises recognize the limitations of in-house security resources and are turning to MSS and MDR for advanced protection from sophisticated threats.

The rise of cloud adoption is driving demand for scalable and cost-effective cloud-delivered MSS and MDR services.

Security providers are leveraging automation and AI to streamline services, making them more accessible and affordable.

MSS providers are increasingly offering bundled services that include security awareness training for employees, a crucial aspect of any security strategy.

Challenges for midsize enterprises:

Security budgets are often tight, making it crucial to find cost-effective solutions that deliver high value.

Midsize enterprises may lack the dedicated security personnel needed to manage and monitor security solutions effectively.

The vast array of MSS and MDR offerings can be overwhelming, making it difficult to find the right fit.

Entrusting sensitive data to a third-party provider requires careful evaluation of their security practices and data privacy policies.

When selecting MSS and MDR providers, midsize enterprises prioritize specific features:

Solutions tailored to the budget constraints of MSEs, offering flexible pricing models and transparent cost structures addressing industry-specific challenges

Continuous monitoring of threats and attacks, rapid response times to security incidents and continuous communication on security posture, threats identified and actions taken

Providers offering ongoing security awareness training for employees to improve overall cyber hygiene

From the 78 companies assessed for this study, 25 qualified for this quadrant, with nine being Leaders and a Rising Star.

Critical Start

Critical Start will acquire the security analytics firm Advanced Threat Analytics, which is already running its analytics platform in its security operations center and plans to provide resellers the combined CyberSOC/ATA team and technology for the MSS space.

CyberProof® A UST Company

CyberProof has extended its partnership with Google Cloud, focusing on leveraging Google Chronicle Security Operations and other Google Cloud Security solutions to extend the capabilities of CyberProof's AI-powered and adaptive managed XDR services.

Cyderes

Cyderes' Continued Security Operations offering brings experienced platform-certified professionals from its managed services team with expertise in multiple platforms, including Google Cloud Security's Chronicle, Microsoft Sentinel and Splunk.

Kudelski Security

Kudelski Security's MSS simplifies the management of security in contemporary work environments. Services from its Cyber Fusion Centers are tailored and informed by a comprehensive understanding of the client's context across endpoint, IT, cloud, and OT/ICS environments.

Optiv

Optiv announced the general availability of its technology-enabled third-party risk managed service, enabling companies to manage their third-party risk management lifecycle and improve compliance and risk management.

PROFICIO™

Proficio's ProSOC Identity Threat Detection and Response services are vendor-agnostic and use an Open XDR solution that works with existing security tools without proprietary agents or sensors. It also utilizes open-source threat feeds to enrich its threat intelligence.

Rackspace Technology harnesses advanced threat detection capabilities that use cloud-based security agents to monitor and analyze high volumes of traffic and events in real time, detecting known and unknown malware, ransomware, zero-day exploits and other threats.

Trustwave's recent acquisition by The Chertoff Group aligns with its mission to reduce cyber risk and fortify organizations against damaging and disruptive cybersecurity threats. This strategic move enables Trustwave to better meet the strenuous security needs of global enterprises.

Unisys' MSS portfolio covers 24/7 operational support, including SIEM, security device management, vulnerability management, Stealth™ services, GRC support, managed IAM services and cloud services. Its offerings include highly valuable, critical decision-making and operational analysis.

Microland (Rising Star) has partnered with industry-leading technology companies to accelerate innovation. It has a dynamic ecosystem of cyber partners and offers different variants of MDR solutions with a variety of options to address clients' cybersecurity needs.

Leader

"Unisys provides robust MSS with a strong emphasis on threat intelligence, advanced security analytics and a tailored approach to vulnerability management that combines cutting-edge technology with expert human intelligence."

Gowtham Sampath

Unisys

Overview

Unisys is headquartered in Pennsylvania, U.S. and operates in 27 countries. It has more than 16,200 employees across 57 global offices. In FY23 the company generated $2.0 billion in revenue, with Enterprise Computing Solutions as its largest segment. Unisys provides advanced cybersecurity services 24/7 through global SOCs. 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.

Strengths

Partnerships for advanced solutions: Unisys collaborates with partners such as Cylance for advanced endpoint protection using AI, ML and LogRhythm for cross-platform, enterprise-wide monitoring, detection and response. By partnering with industry experts, Unisys leverages cutting-edge technologies and expertise to deliver effective threat detection, incident response, and security monitoring services to clients.

Robust security intelligence: Unisys has robust security intelligence capabilities, distilling multiple security-related events into actionable insights. This capability enables Unisys to quickly identify and prioritize security incidents, helping organizations respond effectively to cyber threats and vulnerabilities.

Advanced endpoint protection: Unisys provides advanced endpoint protection services as part of its MDR offerings. This includes AI and ML-driven solutions to detect and respond to threats at the endpoint level, ensuring comprehensive protection against evolving cyber threats.

SIEM and security device management (SDM): Unisys offers SIEM and SDM services to monitor security events, analyze threats in real time and manage security devices effectively. This capability allows organizations to proactively identify and respond to security incidents, enhancing their overall cybersecurity posture.

Caution

Unisys should prioritize investment in marketing and awareness campaigns for its MDR service offering. This strategic move will enhance visibility and understanding of its MDR capabilities among potential clients, thereby expanding its market presence and driving growth.

Star of Excellence

A program, designed by ISG, to collect client feedback about providers' success in demonstrating the highest standards of client service excellence and customer centricity.

Source: ISG Star of Excellence™ research program, Insights till June 2024

In the ISG Star of Excellence™ research on enterprise customer experience (CX), clients have given feedback about their experience with service providers for their **Cybersecurity Solutions and Services**.

Based on the direct feedback of enterprise clients, below are the key highlights:

Client Business Role

▲ **Most satisfied**
Information Technology

▼ **Least satisfied**
Human Resources

Region

▲ **Most satisfied**
Africa

▼ **Least satisfied**
Eastern Europe

Industry

▲ **Most satisfied**
Chemicals

▼ **Least satisfied**
Public sector

Industry Average CX Score

▲ Highest CX: 91.0
▼ Lowest CX: 64.8

CX Score: 100 most satisfied, 0 least satisfied
Total responses (N) = 419

Most Important CX Pillar

Execution and Delivery

Service Delivery Models	Avg % of Work Done
Onsite	53.6%
Nearshore	21.6%
Offshore	24.8%

Appendix

Methodology & Team

The ISG Provider Lens 2024 – Cybersecurity – Solutions and Services research study analyzes the relevant software vendors/service providers in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Authors:
Gowtham Sampath and Dr. Maxime Martelli

Editor:
Ritu Sharma

Research Analyst:
Monica K

Data Analysts:
Rajesh Chillappagari and Laxmi Sahebrao

Quality & Consistency Advisor:
Doug Saylors

Project Manager:
Shreemadhu Rai B

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 May 2024, 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

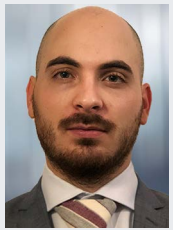
Author

Gowtham Sampath

Senior Manager, ISG Provider Lens™

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider LensTM 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.



Author

Dr. Maxime Martelli

Consulting Manager

Maxime Martelli is a Consulting Manager at ISG France. He takes part in ISG's "Digital & Strategy" solution for multinational firms and the public sector services, as well as applying his expertise around Information Security and Cloud Security projects. Author, teacher and lecturer in the field of IT, Maxime is passionate about technology and applies his knowledge of processes, digital strategy, and IT organization to satisfy his clients' requirements.

As a Security Analyst, he conducts transformation and strategy projects for all kind of Security tools and solutions, with a strong focus on SOC/SIEM and SASE next-generation security transformations.

Enterprise Context and Global Overview

Monica K

Assistant Manager, Lead Research Specialist

Monica K is an Assistant Manager and Lead Research Specialist and a digital expert at ISG. She has created content for the Provider Lens™ studies, as well as content from an enterprise perspective, and she is the author of the global summary report for Cybersecurity, ESG and sustainability market. Monica K brings over a decade year of experience and expertise in technology, business and market research for ISG clients. Her previous role was at a research firm where she specialized in emerging technologies such as IoT and product engineering, vendor profiling, and talent intelligence. Her portfolio included the management of comprehensive research projects and collaboration with internal stakeholders on diverse consulting initiatives.

Study Sponsor

Heiko Henkes

Director and Principal Analyst

Heiko Henkes serves as Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens™ (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as a strategic program manager and thought leader for IPL lead analysts.

Henkes heads Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice. His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation, IT competencies, sustainable business strategies and change management in a cloud-AI-driven business landscape. Henkes is known for his contributions as a keynote speaker on digital innovation, sharing insights on using technology for business growth and transformation.

IPL Product Owner

Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

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

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, 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 AI and 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 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™

JULY, 2024

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES