

Cybersecurity – Solutions and Services

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

Customized report courtesy of:

Infosys®



Executive Summary	04
Provider Positioning	11
Introduction	
Definition	23
Scope of Report	25
Provider Classifications	26
Appendix	
Methodology & Team	93
Author & Editor Biographies	94
About Our Company & Research	97
Star of Excellence	90
Customer Experience (CX) Insights	91

Identity and Access Management	27 – 32
Who Should Read This Section	28
Quadrant	29
Definition & Eligibility Criteria	30
Observations	31

Extended Detection and Response	33 – 38
Who Should Read This Section	34
Quadrant	35
Definition & Eligibility Criteria	36
Observations	37

Security Service Edge	39 – 44
Who Should Read This Section	40
Quadrant	41
Definition & Eligibility Criteria	42
Observations	43

Technical Security Services (Large Accounts)	45 – 51
Who Should Read This Section	46
Quadrant	47
Definition & Eligibility Criteria	48
Observations	49
Provider Profile	51

Technical Security Services (Midmarket)	52 – 57
Who Should Read This Section	53
Quadrant	54
Definition & Eligibility Criteria	55
Observations	56

Strategic Security Services (Large Accounts)	58 – 64
Who Should Read This Section	59
Quadrant	60
Definition & Eligibility Criteria	61
Observations	62
Provider Profile	64

Strategic Security Services (Midmarket) 65 – 70

Who Should Read This Section	66
Quadrant	67
Definition & Eligibility Criteria	68
Observations	69

Managed Security Services - SOC (Large Accounts) 71 – 77

Who Should Read This Section	72
Quadrant	73
Definition & Eligibility Criteria	74
Observations	75
Provider Profile	77

Managed Security Services - SOC (Midmarket) 78 – 83

Who Should Read This Section	79
Quadrant	80
Definition & Eligibility Criteria	81
Observations	82

Digital Forensics and Incident Response 84 – 89

Who Should Read This Section	85
Quadrant	86
Definition & Eligibility Criteria	87
Observations	88

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.



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 quadrants. 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:

There is 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


	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


	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


	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
Cyberes	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


	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


	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


	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


	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

	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



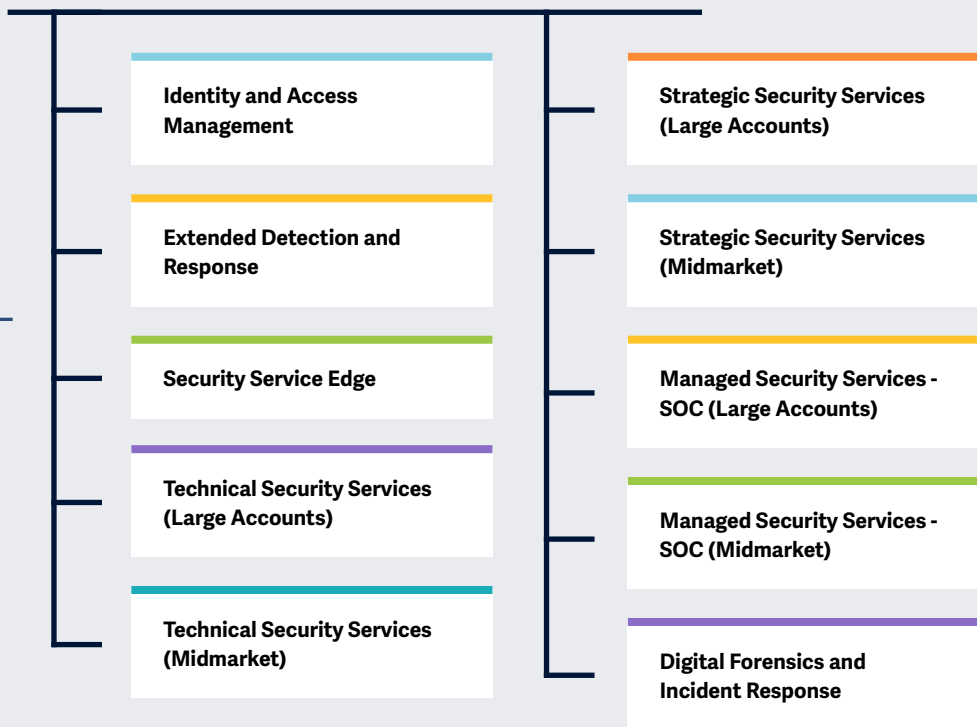
 Provider Positioning

	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 (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.

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.

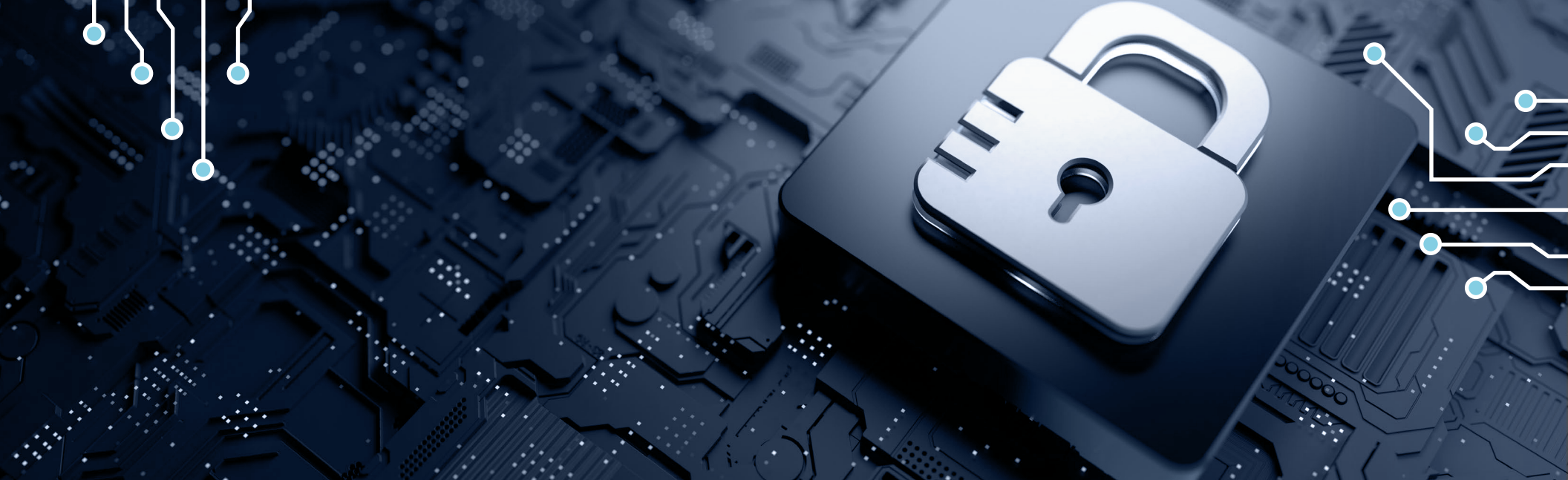
Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength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

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

Who Should Read This Section

This report is relevant for enterprises across industries in the U.S. to evaluate IAM solutions providers. Specifically, it targets key decision-makers responsible for assessing providers' capabilities in offering proprietary software and associated services for managing enterprise user identities and devices.

IAM solutions play a crucial role in safeguarding digital assets by controlling user access to systems, applications and data. Organizations within the U.S. require robust IAM strategies to safeguard sensitive information, prevent unauthorized access and comply with regulations.

Enterprises in the U.S. demand IAM solutions that can seamlessly adapt to various technological advancements such as cloud environments, hybrid infrastructures, Zero Trust frameworks, privacy regulations, AI and behavioral analytics. With the growing adoption of cloud and software-as-a-service (SaaS) applications, ensuring secure access across hybrid environments poses a complex challenge.

Additionally, there is a noticeable trend among U.S. organizations toward embracing passwordless authentication methods while simultaneously recognizing the critical importance of effective access policy management. Therefore, this report serves as a valuable resource for U.S. enterprises navigating the evolving landscape of IAM solutions and their implications on cybersecurity strategies and remote work environments.



IT professionals responsible for safeguarding digital assets, managing user access and ensuring compliance with regulations should read this report to understand the current security landscape.



Strategy professionals should read this report to understand how IAM solutions secure digital assets, adapt to evolving landscapes and ensure regulatory compliance to furbish a robust cybersecurity strategy.

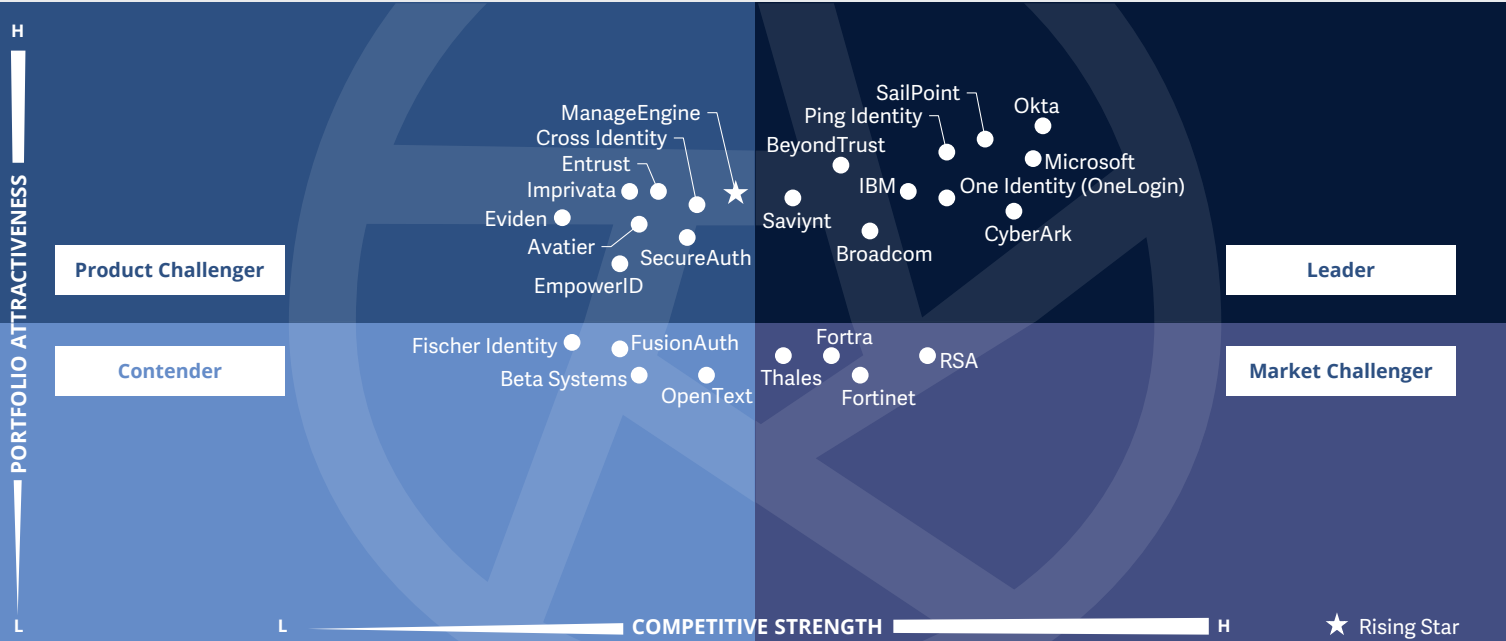


Cybersecurity professionals should read this report to improve their cybersecurity posture with evolving technologies such as cloud, Zero Trust, privacy regulations, AI and behavioral analytics.



Technology professionals will benefit from the latest IAM trend insights, such as passwordless authentication and access policy management, enabling informed decision-making for improved security posture.





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

Gowtham Sampath



Identity and Access Management

Definition

IAM 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 excludes 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, customer-managed clouds or as-a-service models or a combination thereof.

IAM solutions aim to manage (collect, record and administer) user identities and related access rights and 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 offer additional functionalities for social media and mobile use to address specific security needs beyond traditional web and contextual rights management. This quadrant also includes machine identity management.

Eligibility Criteria

1. Offer solutions that can be **deployed** as an **on-premises, cloud, identity-as-a-service** (IDaaS) or a managed third-party model
2. Offer solutions that can **support authentication** as a combination of **single-sign-on (SSO), multifactor authentication (MFA)**, and risk-based and context-based models
3. Offer solutions that can **support role-based access** and PAM
4. Provide **access management** for one or more enterprise needs such as **cloud, endpoint, mobile devices, APIs and web applications**
5. Offer solutions that can **support one or more legacy and new IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM
6. Offer a portfolio with one or more of the following – **directory solutions, dashboard or self-service management** and lifecycle management (migration, sync and replication) solutions – to support secure access



Identity and Access Management

Observations

The U.S. IAM market is driven by the need for secure access control and compliance in today's digital landscape. Enterprises seek solutions that are scalable and flexible and integrate seamlessly with existing infrastructure.

The growing adoption of zero trust models relies heavily on IAM for granular access control and user verification.

As cloud adoption skyrockets, organizations require cloud-specific IAM solutions for managing access across diverse platforms.

MFA is becoming the norm, bolstering access security with additional layers of verification.

Increased awareness of the risks associated with privileged users leads to greater PAM adoption for secure access control.

Integration of AI and ML allows for anomaly detection, risk assessment and automated user provisioning, streamlining IAM processes.

However, enterprises face the following challenges in implementing effective IAM solutions.

Managing access across diverse on-premises, cloud and hybrid environments presents a significant hurdle.

Navigating complex data privacy regulations such as HIPAA and GDPR adds another layer of complexity to IAM implementation.

To overcome these challenges, enterprises seek IAM solutions with the below specific characteristics:

Support for advanced authentication methods like MFA and passwordless authentication is crucial for robust security.

Integration with threat intelligence feeds allows for risk assessment and anomaly detection, further strengthening the security posture.

Additional trends, such as vendor consolidation and a focus on UX, are also shaping the market. Biometric authentication methods such as facial recognition and fingerprint scanners are gaining traction as well.

From the 78 companies assessed for this study, 26 qualified for this quadrant, with ten being Leaders and a Rising Star.



BeyondTrust acquired Entitle, a pioneering privilege management solution that discovers, manages and automates just-in-time (JIT) access and modern identity governance and administration (IGA) across the entire cloud estate, consolidating its Privilege Identity Security.

Broadcom

Broadcom's integration of Symantec PIM with its security portfolio provides a unified platform for managing privileged access across hybrid and multicloud environments, enhancing control and visibility with AI to identify suspicious activities and potential breaches.

CyberArk

CyberArk's PAM platform has passwordless authentication capabilities, increasing security and user convenience and providing comprehensive identity lifecycle management, access governance and risk mitigation tools for holistic identity security.



IBM's X-Force Threat Intelligence Index highlights that streamlining identity management through a unified IAM provider and strengthening legacy applications with modern security protocols are crucial to mitigating risks.

Microsoft

Microsoft's recent launch of Copilot for Security recommends ways to automate prevention and resolution for future identity attacks, such as Microsoft Entra Conditional Access policy, to improve security posture and reduce help desk calls.

Okta

Okta announced its support for passkeys as passwordless authentication for Okta Customer Identity Cloud and the creation of its own Okta AI, providing phishing-resistant, passwordless authentication to enhance experiences and protect against cyberattacks.



Identity and Access Management

One Identity (OneLogin)

One Identity (OneLogin) announced the availability of One Identity Cloud PAM Essentials, a SaaS-based solution for simplified PAM that specifically focuses on cloud applications and infrastructure, providing complete visibility into user activities.



Ping Identity's (OneLogin) acquisition of ForgeRock is helping create a broader portfolio, including new capabilities in identity management, governance, verification, decentralized identity in authorization and risk and fraud signals.

SailPoint

SailPoint launched Atlas, an updated multitenant SaaS identity security platform that uses an identity data lake using Snowflake. The solution is designed to scale to meet the needs of the most complex scenarios for the largest and most complex enterprise environments.

Saviynt

Saviynt announced that its Enterprise Identity Cloud (EIC) platform manages over 50 million identities, showcasing the demand for a cloud-based converged identity platform that cost-effectively manages both human and machine identities.

ManageEngine

ManageEngine (Rising Star) announced the addition of access certification and identity risk assessment functionalities to ADManager Plus, its on-premises identity governance and administration (IGA) solution, enhancing the compliance posture of enterprises.





Extended Detection and Response

Extended Detection and Response

Who Should Read This Section

This quadrant is relevant to enterprises globally for evaluating extended detection and response (XDR) solution providers. It assesses how each provider helps enterprises increase visibility across all telemetry sources and obtain a unified view of threat detection and response. ISG offers an analysis of the current positioning of global XDR players with a comprehensive overview of the market's competitive landscape.

Enterprises recognize the need for a proactive approach to threat detection and response, driven by data science techniques and dynamically updated threat intelligence. XDR empowers enterprises of all sizes and security maturity levels to achieve robust threat detection and response capabilities, regardless of limited security personnel, expertise or budget for a dedicated security operations center (SOC). A well-built XDR solution is an SOC enabler that presents a descriptive view of threats and automates initial triage tasks.

Using MITRE ATT&CK framework and open-source intelligence, XDR models detect anomalies and classify attacks based on specific tactics and techniques, providing actionable insights for SOC analysts. It enriches alerts with context, correlating events to determine true threat severity and attack chain participation. This reduces false positives and saves valuable investigative time. Advanced XDR solutions prioritize alerts based on risk scoring and business impact, guiding incident response planning. Additionally, XDR solutions should have a robust set of APIs that allow the extension of workflow functionalities to other external systems to streamline containment actions to events.



Cybersecurity professionals can gain valuable insights into XDR solutions that aid enterprises in enhancing visibility across endpoints to enable unified threat detection and response.



Technology professionals should read this report to understand XDR providers' integration capabilities and how they help with improved detection and faster response times to threats.

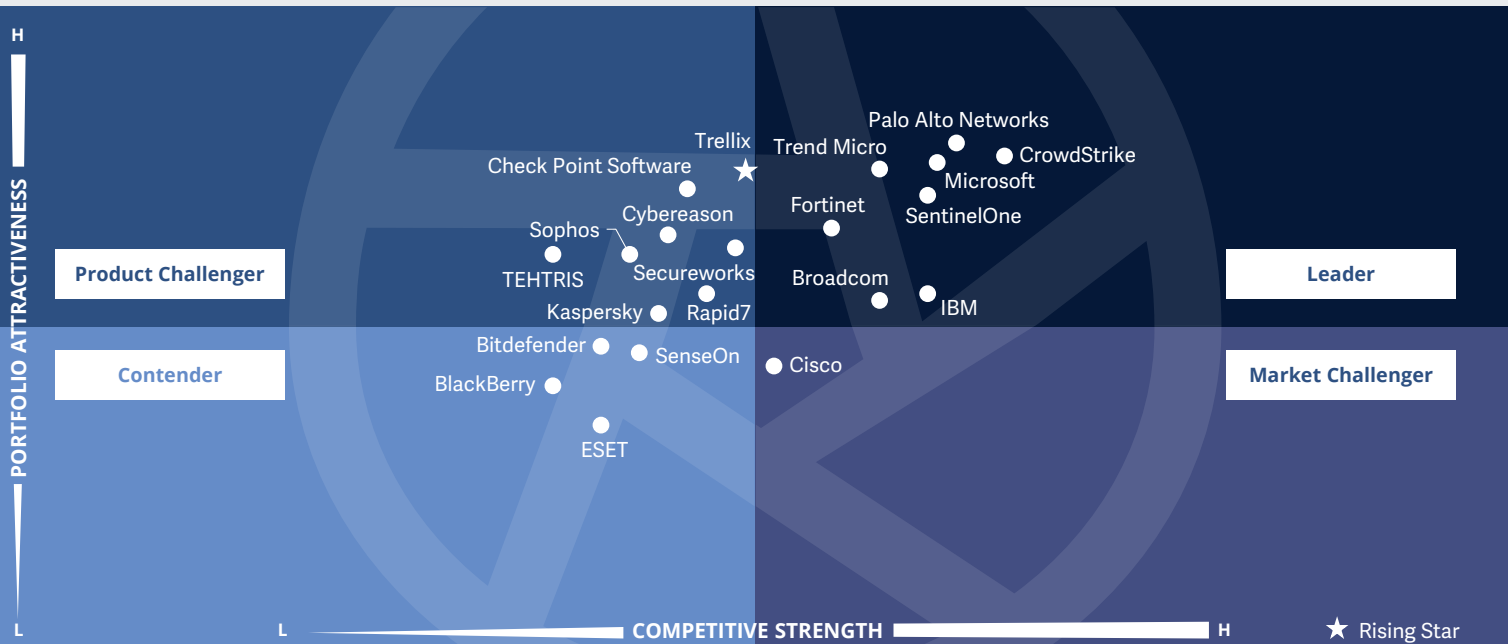


Strategy professionals should read this report to understand XDR providers' capabilities in helping enterprises manage security risks effectively and make informed security decisions.



Cybersecurity – Solutions and Services
Extended Detection and Response

Global 2024



The Extended Detection and Response quadrant assesses security vendors’ ability to provide **integrated threat detection, investigation and response capabilities across multiple endpoints, networks and cloud environments.**

Dr. Maxime Martelli



Extended Detection and Response

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 weak individual signals, to enable accurate detections. XDR solutions consolidate and integrate multiple products, providing comprehensive security for workspaces, networks and workloads. Typically, XDR solutions are aimed at vastly improving visibility and context understanding of identified threats across the enterprise. Characteristics of these solutions include telemetry and contextual data analysis for detection and response. XDR solutions comprise multiple products integrated into a single pane of glass for sophisticated viewing, detection and response capabilities.

Their high automation maturity and contextual analysis offer tailored responses to affected systems, prioritizing alerts based on severity against known reference frameworks. This quadrant excludes **pure service providers that do not offer an XDR solution based on proprietary software**. XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expenses. They are particularly suitable for security operations teams struggling to manage diverse solution portfolios or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

Eligibility Criteria

1. Offer XDR solutions based on **proprietary software** and not on third-party software
2. Ensure an XDR solution has two primary components: **XDR front end and XDR back end**
3. Offer front end with **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. Provide solution with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solution capable of **blocking sophisticated threats such as advanced persistent threats, ransomware and malware**
6. Provide solution using **threat intelligence and real-time insights on threats** emanating across endpoints
7. Offer solution including **automated response features**



Extended Detection and Response

Observations

In 2024, the XDR market is evolving with several new trends and advancements. XDR solutions are integrating advanced AI and ML capabilities, thus enhancing behavioral analytics and automating response actions based on learned patterns.

Vendors have also increased their focus on cloud security and are providing comprehensive visibility and protection across hybrid and multicloud environments. XDR platforms are closely aligning with the MITRE ATT&CK framework, enabling more informed threat-hunting and response strategies.

XDR vendors are expanding their offerings to include robust managed detection and response (MDR) services, catering to organizations facing skill shortages. Moreover, XDR solutions are leveraging advanced UEBA for proactive threat detection and response. Automation and orchestration capabilities within XDR platforms are maturing, thus streamlining incident response processes and reducing manual tasks. XDR also aligns with

zero trust principles, emphasizing continuous verification and strict access controls while incorporating features to support regulatory compliance requirements.

Such advancements underscore XDR's role in delivering sophisticated threat detection, response and compliance capabilities amid evolving cyber threats.

From the 35 companies assessed for this study, 21 qualified for this quadrant, with eight being Leaders and a Rising Star.

Broadcom

Broadcom's XDR includes comprehensive visibility, advanced analytics, automated response and a simplified management console, enabling organizations to effectively protect their digital assets against evolving threats.

CrowdStrike

CrowdStrike's Falcon® Insight XDR flexibility meets the increasing market demand for a simplified and single-pane-of-glass control panel with its Falcon tool. It aims to increase industry robustness by supporting standards and frameworks like CrowdXDR Alliance.

Fortinet

Fortinet's FortiXDR can be seamlessly integrated with Fortinet Security Fabric and Fortinet's other security products to streamline incident response with automated workflows and playbooks. This integration allows fast containment and threat remediation.

IBM

IBM's Security QRadar XDR undertakes a proactive and coordinated approach to threat detection and response, with multiple modules and integration across networks, clouds, endpoints and other workloads.

Microsoft

Microsoft's extensive customer base and strong brand recognition have helped the company establish a prominent position in the XDR market. Its XDR integrates its Defender Advanced Threat Protection (ATP) to provide threat detection and response.

Palo Alto Networks

Palo Alto Networks' strong market presence, commitment to innovation and focus on secure access service edge/security service edge (SASE/SSE) solutions for organizations make Cortex XDR a robust product and Palo Alto Networks a Leader in the XDR quadrant.

SentinelOne

SentinelOne maintains its momentum as one of the leading XDR vendors by using patented behavioral AI algorithms to detect and classify malicious activities. All security functions are bundled in a single agent, thus eliminating the need for multiple security products.



Extended Detection and Response

Trend Micro

Trend Micro expanded its endpoint detection and response (EDR) capabilities into a next-generation XDR product, which aligns with the MITRE ATT&CK framework and offers dynamic risk assessments. Its automation capabilities deliver advanced XDR.

Trellix

Trellix (Rising Star) XDR boasts an adaptable and interoperable framework that seamlessly connects with a vast array of external security solutions, fostering a unified cybersecurity strategy combined with a sophisticated threat detection mechanism.





Security Service Edge

Who Should Read This Section

This report is relevant to enterprises globally 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). It evaluates how each provider helps enterprises ensure security across hybrid and multicloud ecosystems.

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

Due to the rapid shift to hybrid work models, enterprises seek solutions that accommodate employees, partners, suppliers, and customers accessing internal apps, the internet and SaaS applications. Enterprises want SSE solutions that simplify the adoption and deployment of security policies. A streamlined approach reduces complexity and accelerates implementation. Enterprises expect SSE platforms to monitor and track user activity across a network. Furthermore, SSE providers must protect all users from ransomware and other advanced malware threats.

Enterprises adopt SSE to address modern security challenges, simplify access and enhance digital experiences. They seek providers that offer streamlined solutions, robust protection and agility in a rapidly evolving landscape.

The need for unified, secure access in a hybrid workforce drives SSE adoption. Enterprises expect SSE providers to offer simplified deployment, VPN bypass and robust malware protection. Providers should innovate, customize, prioritize UX and expand their global reach to succeed.



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.

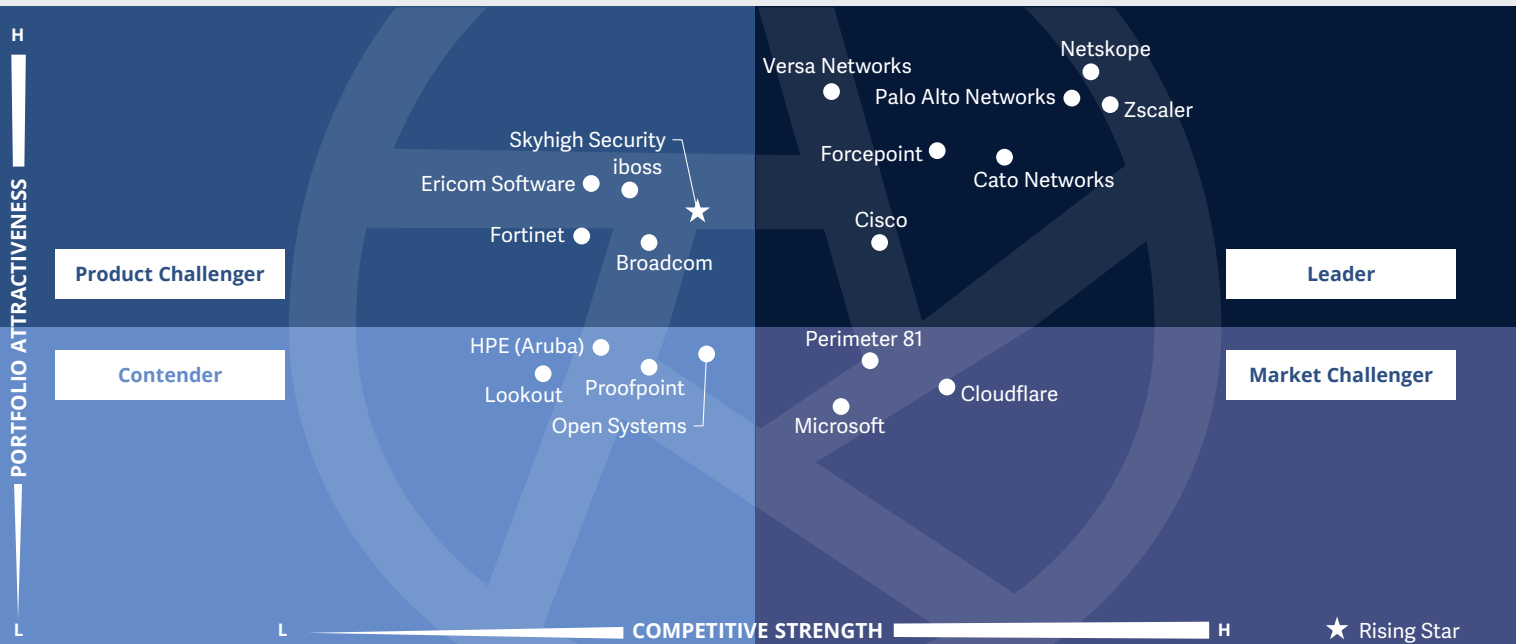


Strategy professionals can gain insights into SSE providers' critical capabilities and focus on user-centricity, delivering security to end users at the edge or devices through cloud.



Technology professionals will be able to understand how SSE providers assist enterprises in adopting an enterprise-wide zero-trust framework to improve their security posture.





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 Sampath



Security Service Edge

Definition

The SSE solution providers assessed for this quadrant offer cloud-centric solutions combining proprietary software or hardware and associated services, enabling secure access to the cloud, SaaS, 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 leakage/loss prevention (DLP), browser isolation and next-generation firewall (NGFW) to secure access to both cloud and on-premises applications.

Vendors showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients.

This quadrant excludes the network components of secure access service edge (SASE), such as SD-WAN, which are covered in the ISG Provider Lens™ Network – Software Defined Solutions and Services 2024 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 access enterprise applications and databases – over dedicated networks centrally. ZTNA creates exclusive connectivity between users and applications, using context-based behavioral analysis to manage access. CASB offers visibility, enforces security policies and compliance, and controls 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, with advanced automation to assess UX.

Eligibility Criteria

1. Provide SSE as an **integrated solution with zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**
2. Offer solutions **predominantly based on proprietary software, they may partially rely on partner solutions while avoiding complete dependency on third-party software**
3. Maintain **globally located POPs** to deliver these solutions
4. **Deliver SSE to both cloud and on-premises environments (including hybrid environments)**
5. Exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/UEBA)** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **globally availability of the solution**



Observations

The Security Service Edge market is currently witnessing rapid growth driven by the increasing adoption of cloud applications, expanding remote workforce and evolving cyber threat landscape. ISG's analysis reveals several enterprise challenges necessitating SSE deployments:

Organizations are increasingly using a mix of cloud platforms (public, private and hybrid), as traditional security solutions failed to ensure consistent security across these diverse environments.

With the rise of remote work, securing access to cloud applications from various locations and devices becomes crucial.

Managing a complex security ecosystem with multiple-point solutions can be challenging.

Strict regulations like the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA) and GDPR require robust data security measures.

Vendor selection: Differentiation and characteristics in the SSE market

Enterprises prioritize SSE vendors that cater to their industry-specific compliance and regulations and data security concerns.

They seek vendors offering open standards and pre-built integrations with existing security tools and cloud platforms to avoid vendor lock-in and simplify deployment.

SSE solutions need to scale effectively to accommodate growth in cloud application usage and user base, with low latency and reliable performance, which are essential for ensuring a positive UX for geographically dispersed workforces.

Enterprises prefer vendors with robust threat intelligence capabilities and a proven track record of security expertise.

Transparency in pricing and a clear understanding of the TCO, including integration costs, is critical for companies when selecting an SSE vendor.

From the 35 companies assessed for this study, 19 qualified for this quadrant, with seven being Leaders and a Rising Star.

Cato Networks

Cato Networks focuses on improving the integration and performance of its SSE solutions by upgrading its ZTNA capabilities within the Secure Connect platform and expanding its partnerships with cloud providers.

Cisco

Cisco prioritizes integrating its SSE solution, Secure Access, with other Cisco security products to achieve a unified approach. The company also strengthens partnerships with cloud providers like Microsoft to enhance Secure Access' functionalities.

Forcepoint

Forcepoint focuses on expanding the reach of its Forcepoint Cloud Security Gateway, an SSE platform, by launching integrations with additional cloud platforms. This strategic move aligns with the growing adoption of multicloud environments.

Netskope

Netskope is expanding its global data center network, aiming to offer lower latency, improved performance and user reach. The company is also focusing on partnerships with SIEM vendors to enhance threat detection and investigation capabilities within its SSE platform.

Palo Alto Networks

Palo Alto Networks has introduced improvements to UX and streamlined policy management tools within its Prisma SASE platform. The company also strengthened partnerships with cloud providers such as AWS to offer preconfigured security policies.

Versa Networks

Versa Networks has introduced enhanced cloud workload protection functionalities within its Versa SASE platform and established partnerships with threat intelligence providers to improve threat detection capabilities, ensuring comprehensive protection for customers.



Security Service Edge



Zscaler has expanded its global data center network to improve performance for its Zscaler ZSSP platform. It also increased focus on partnerships with SASE framework providers for industry-standard secure access, fostering a unified and secure cloud security ecosystem.

Skyhigh Security

Skyhigh Security (Rising Star) has launched Cloud Workload Protection Platform (CWPP) integration to offer comprehensive cloud security alongside its core SSE platform. This offering surpasses basic SSE functionalities, extending additional protection for cloud workloads.





Technical Security Services (Large Accounts)

Technical Security Services (Large Accounts)

Who Should Read This Section

This report is relevant to U.S. enterprises evaluating technical security service (TSS) providers, particularly focusing on threat response activities and evidence preservation against attackers.

These enterprises are seeking all-encompassing solutions integrating endpoint, network, identity and threat intelligence for robust cybersecurity. They prioritize providers delivering tailored solutions for diverse cloud environments, ensuring robust protection of cloud-hosted data and applications.

Furthermore, enterprises prioritize providers aligning with the zero trust model, emphasizing continuous verification and stringent access controls. They concentrate on providers offering sophisticated identity and access management (IAM) solutions to secure user access across organization. Additionally, enterprises opt for providers equipped with proactive threat hunting capabilities to identify and mitigate potential threats before escalation.

In their pursuit of robust security, enterprises adopt risk-based security strategies. They actively seek providers offering risk assessment services to identify and address critical security risks effectively. Embracing secure access service edge (SASE) solutions becomes paramount, especially in light of the increasing prevalence of remote work, given their integrated security and networking capabilities.

To enhance their incident response capabilities, enterprises prioritize providers offering incident response planning and training services, ensuring prompt and effective responses to security incidents. Lastly, they seek providers offering solutions that comply with industry-specific regulations and standards, crucial for organizations operating in regulated industries.



Technology professionals responsible for cybersecurity strategies should read the report to stay informed about the latest trends and best practices.



Risk management professionals should read the report to understand risk-based security strategies and risk assessment services.



Cloud architects and administrators should read this report to stay abreast of trends and considerations for securing cloud-hosted data and applications.

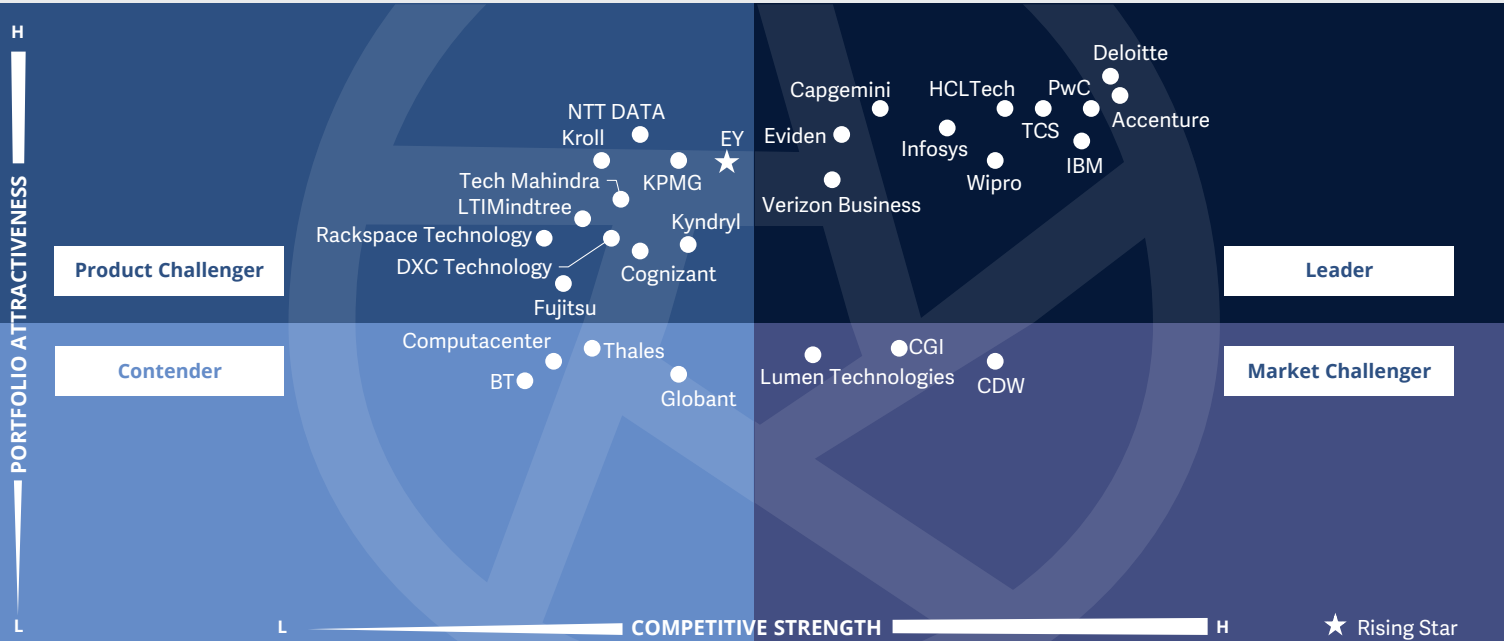


Security professionals should read the report to gain insights into trends and considerations for evaluating TSS providers.



Cybersecurity – Solutions and Services
 Technical Security Services (Large Accounts)

U.S. 2024



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 Sampath



Technical Security Services (Large Accounts)

Definition

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

TSS providers offer standardized playbooks and road maps 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 complete or individual transformations of existing security architectures 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.

TSS providers invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio scope. This quadrant also encompasses classic MSS provided without a security operations center (SOC).

This quadrant examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other vendors.

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Have gained **authorization by security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies



Technical Security Services (Large Accounts)

Observations

The U.S. TSS market for large enterprises is a rapidly growing sector driven by the sophisticated threat landscape and the growing complexity of security solutions.

This growth is further fueled by the following:

Increased cloud adoption necessitates cloud-specific security implementations, driving demand for services such as Cloud Security Posture Management (CSPM) and Zero Trust Network Access (ZTNA).

Automating repetitive tasks such as log analysis and incident response frees up security teams for strategic initiatives.

Integration and interoperability of diverse security tools and platforms for holistic security posture management is crucial.

The market is witnessing specialization in OT security and industrial control systems (ICS) security as cyberthreats target critical infrastructure.

Market challenges:

Implementing and maintaining robust cybersecurity solutions is expensive, even for large enterprises with limited budgets.

Managing and securing complex IT infrastructure with diverse technologies and legacy systems adds another layer of complexity.

Large enterprises must comply with various data privacy regulations, requiring ongoing adaptation and adjustments to their security posture.

Enterprises seek providers with the following characteristics:

Ability to integrate and manage solutions from various vendors and diverse technology stacks

Understanding and ability to navigate complex data privacy regulations

24/7 support, proactive monitoring and immediate response capabilities

Ability to scale solutions and adapt to evolving security needs supporting the growth and changing landscape of large enterprises

From the 78 companies assessed for this study, 29 qualified for this quadrant, with eleven being Leaders and a Rising Star.

accenture

Accenture showcases deep expertise with a focus on automation, cloud security solutions and industry-specific integrations, positioning it as a valuable partner for organizations seeking robust technical security solutions.

Capgemini

Capgemini's cybersecurity services leverage the latest technologies and best practices, including DevSecOps, cloud-native security analytics and the MITRE ATT&CK framework, to provide advanced security monitoring and response capabilities.

Deloitte.

Deloitte has announced multiple collaborations with cloud providers and enterprise software vendors focused on delivering secure cloud migration and management services. These collaborations demonstrate the company's commitment to cloud security solutions for U.S. enterprises.

EVIDEN

an atos business

Eviden (an Atos Business) has over 6,000 cybersecurity specialists, providing a global scale and depth of expertise in implementing and integrating security products and solutions. The company has a large ecosystem of technology partners, providing a function-leading toolset and proprietary solutions.



Technical Security Services (Large Accounts)

HCLTech

HCLTech's TSS solutions are delivered by over 1,250 trained and dedicated professionals with extensive experience in TSS across diverse domains and technologies, including networks, cloud, OT, IoT, IAM, data privacy and SASE.



IBM's expansion of its X-Force offering reflects an ongoing investment in threat intelligence. This investment allows IBM to provide U.S. companies with the latest threat data to inform their security implementations and decision-making.



Infosys has strategic partnerships with more than 25 leading partners that help build collaborative solutions and GTM plans. Its partnerships with academic institutions, both national and international, allow it to develop and nurture talent at scale.



PwC invests heavily in service enhancement, including the development of proprietary accelerators that help maximize the ROI for cybersecurity and privacy technologies tailored to clients' specific needs.



TCS provides implementation services for adopting Zero Trust security models, helping organizations minimize attack surfaces and improve access control. TCS offers specialized cloud services for cloud security posture management, workload security and compliance.

Verizon Business

Verizon Business actively invests in expanding its technical cybersecurity implementation and deployment services. The company leverages its network expertise, partnerships and focus on advanced technologies to provide comprehensive solutions for businesses of all sizes.



Wipro offers industrial IoT cybersecurity services to effectively manage operational technology cyber risk and implement efficient technology service operating models for clients in oil and gas, water and power utilities, mining and manufacturing industries.

EY

EY (Rising Star) assists enterprises in strategizing and implementing a holistic cybersecurity strategy. EY also helps design and operate cyber programs with due considerations to the evolving threat landscape, ensuring long-term resilience, flexibility and evolving business needs.



Infosys



“Infosys’ focus on an integrated approach, infrastructure security services, robust partner ecosystem, underlying automation and continuous innovation sets it apart as a leading provider of comprehensive cybersecurity services.”

Gowtham Sampath

Overview

Infosys is headquartered in Bengaluru, India . It has more than 322,600 employees across 274 offices in 56 countries. In FY23 the company generated \$18.2 billion in revenue, with Financial Services as its largest segment. Infosys transforms and enables clients to embrace a zero trust security architecture strategy by navigating them from the current state to the target state of security technology adoption. The company has strategic partnerships with over 25 leading partners for building joint solutions and global GTM to align with local market needs.

Strengths

Infrastructure security services: Infosys offers infrastructure security services to help enterprises secure their infrastructure while transforming digitally. These services include designing, deploying, configuring, integrating and managing network security with next-generation firewalls and micro-segmentation, delivering zero trust network access and email protection controls, including ATP and sandboxing solutions.

Continuous innovation: Infosys Cyber Security, in collaboration with Infosys Centre for Emerging Technology Solutions (ICETS), constantly innovates, validates and launches new solutions to enhance customers’ risk resiliency. The ICETS develops capabilities and capacities to support business growth through competency development via

training, academic collaborations, partner-led certifications, solution labs and automation for delivery excellence. Infosys leverages more than 25 strategic partnerships that build collaborative solutions and GTM plans.

Underlying automation: Infosys’ dedicated automation team helps clients build use cases, bots and accelerators. The company has developed more than 100 reusable use cases spanning IAM, infrastructure security, data security and over 200 reusable bots. It also provides automation platforms (Infosys IPs) for identity operations and infrastructure operations, supporting SOX governance, patch management and vulnerability management.

Caution

While Infosys may rely heavily on pre-built scripts and third-party automation tools during deployments to streamline processes, this approach raises concerns about potential limitations in flexibility and customization compared to providers that develop their own deployment tools.





Technical Security Services (Midmarket)

Technical Security Services (Midmarket)

Who Should Read This Section

The report is relevant to U.S. midsize enterprises, offering crucial insights into the evolving landscape of technical security service providers. It highlights key trends, including the adoption of proactive threat response measures such as incident detection and containment strategies.

These enterprises face escalating cyber threats and require robust solutions for threat response and evidence preservation. They prioritize providers offering advanced threat intelligence and response capabilities to mitigate risks effectively.

U.S. midsize enterprises are increasingly adopting integrated security solutions encompassing threat detection, incident response and evidence preservation. They seek providers that offer comprehensive services tailored to their specific needs, including real-time threat monitoring, forensic analysis and evidence collection, enabling rapid incident response and minimizing disruption to business operations.

Looking ahead, U.S. midsize enterprises are keen to adopt emerging technologies such as AI and ML for proactive threat detection and response, seeking providers leveraging these technologies to enhance security posture and stay ahead of evolving cyber threats.

Service providers are responding to these demands by offering innovative solutions that integrate advanced analytics, automation and threat intelligence. They focus on delivering holistic security services that address the entire threat lifecycle, from detection to containment and remediation. Additionally, these providers emphasize the importance of evidence preservation techniques, such as digital forensics and chain of custody procedures, to support legal proceedings and regulatory compliance.



Strategy professionals should read this report to evaluate TSS providers, focusing on threat response activities and evidence preservation against attackers.



Risk managers should review this report to understand MSSPs' capabilities in addressing potential threats and vulnerabilities, enhancing organizational resilience.



Security professionals should read this report to assess TSS providers offering threat detection, vulnerability management and security awareness training.

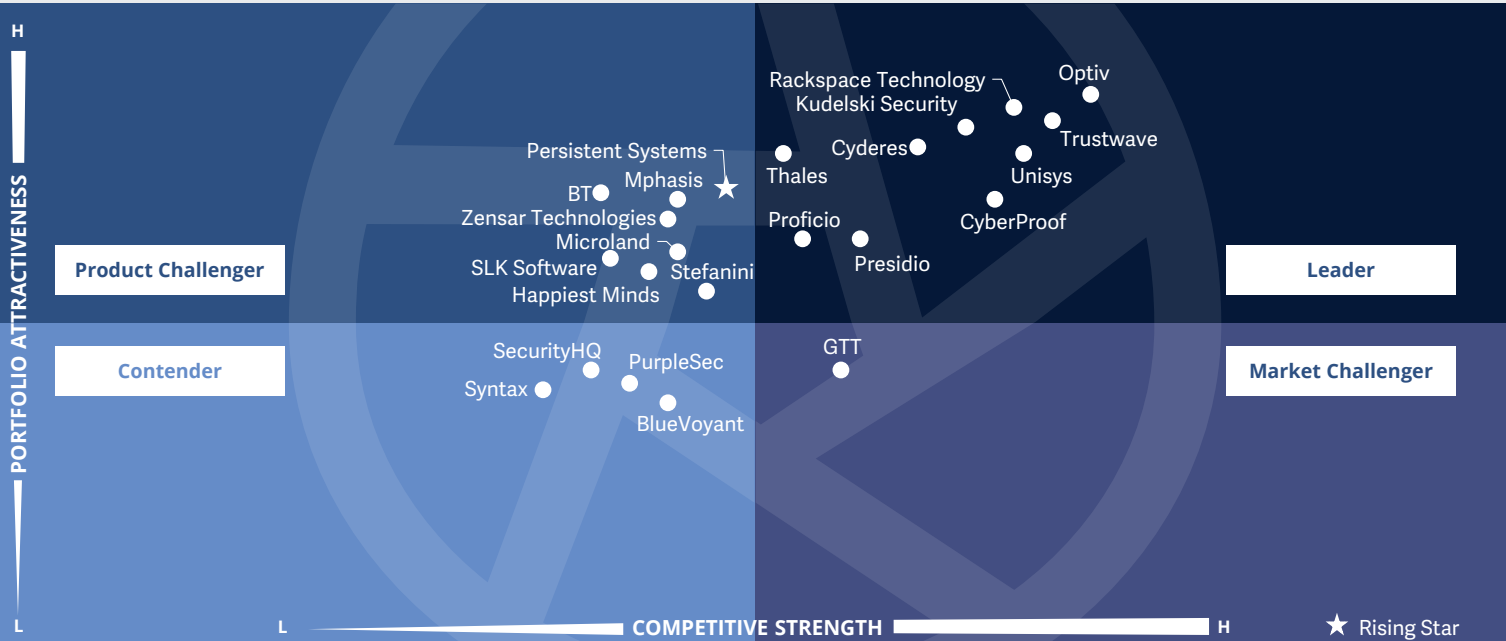


Business leaders should consider this report to understand MSSPs' roles in evidence preservation against attackers, aiding in effective incident response and asset protection.



Cybersecurity – Solutions and Services
Technical Security Services (Midmarket)

U.S. 2024



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 Sampath



Technical Security Services (Midmarket)

Definition

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

TSS providers offer standardized playbooks and road maps 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 complete or individual transformations of existing security architectures 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.

TSS providers invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio scope. This quadrant also encompasses classic MSS provided without a security operations center (SOC).

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Have gained **authorization by security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies



Technical Security Services (Midmarket)

Observations

As cyber threats continue to evolve, the TSS midmarket will see further advancements in cost-effective, user-friendly and scalable solutions specifically designed to empower SMBs in their cybersecurity journey.

Key trends:

Automating routine security tasks such as patching and log analysis streamlines operations for resource-constrained teams.

Compliance-as-a-service offerings help SMEs navigate complex data privacy regulations without dedicated compliance teams.

SaaS-based security solutions offer subscription models, eliminating upfront hardware and software costs for SMEs.

Security solutions are designed with user-friendly interfaces and minimal technical expertise requirements for easier implementation and management.

Midmarket challenges:

Smaller IT teams and tighter budgets make it difficult to implement and manage complex security solutions in-house and retain qualified cybersecurity professionals.

Insufficient cybersecurity awareness among employees can increase the risk of human error-induced security incidents.

Protecting sensitive customer and business data is crucial, but SMEs often lack the necessary security infrastructure.

Navigating and adhering to data privacy regulations can be overwhelming for resource-constrained teams.

Midmarket enterprises look for service providers with the following characteristics:

Affordable solutions that deliver high value without exceeding their budget limitations

Solutions that are easy to deploy and manage, requiring minimal technical expertise from internal teams

Reliable and responsive support services that are crucial for addressing security issues and concerns promptly

Expertise in relevant data privacy regulations that help SMEs achieve compliance efficiently

From the 78 companies assessed for this study, 23 qualified for this quadrant, with ten being Leaders and a Rising Star.



CyberProof has been investing in improving cloud and network partnerships. This collaboration focuses on tighter integration between CyberProof's security orchestration, automation and response (SOAR) platform, aiming to streamline cloud workload protection for businesses.

Cyderes

Cyderes has collaborated with Google and Microsoft to deliver an innovative cloud workload security solution to clients. Employing a risk-based methodology, Cyderes evaluates clients' current cloud security architecture and designs future-state architectures accordingly.

Kudelski Security

Kudelski Security offers product installation services and migration to tech-on-tap services, firewall optimization and service tune-ups with certified field engineers, ensuring the organization's security technologies function correctly and integrate seamlessly.

Optiv

Optiv offers independent security software vendor solutions via the Google Cloud Marketplace. This enables clients to conveniently access and implement the most suitable Optiv solutions tailored to their specific business requirements and regulatory mandates.

Presidio

Presidio is being acquired by private equity firm Clayton Dubilier and Rice (CD&R) as part of a bid to expand the \$6-billion solution provider's managed cloud services and digital offerings that will provide advanced services to accelerate sales growth.



Proficio's Active Defense Response-as-a-Service solution establishes a unified security environment by integrating with major security tools and technologies throughout the client's IT landscape, strengthening defenses from network perimeters to endpoints.



Technical Security Services (Midmarket)



Rackspace Technology extends its partnership with Palo Alto Networks, combining expertise in multicloud computing and security operations to help organizations protect their data and applications, simplify their security operations and accelerate their multicloud adoption.



Thales acquired Imperva from private equity firm Thoma Bravo, enabling growth in data security and Thales' entry into the application security market, benefitting from its strong complementarity and cultural fit in terms of clients and addressable markets.



Trustwave SpiderLabs has released comprehensive research that explores the specific threats and risks the financial services industry faces, along with exposing its tactics, techniques and procedures, and practical insights and mitigations to strengthen defenses.



Unisys' cybersecurity solutions foster a secure environment and a scalable ZTA, allowing remote user access solely to necessary resources rather than the entire network to address vulnerabilities and reinforce defenses, effectively thwarting attacks.



Persistent Systems (Rising Star) leverages strategic OEM partnerships with a 360-degree relationship with Zscaler, IBM, Color Tokens, Exabeam and others, where Persistent provides engineering support, pro-serve and managed services support, as well as go-to-market with its sales teams.





Strategic Security Services (Large Accounts)

Strategic Security Services (Large Accounts)

Who Should Read This Section

This report targets enterprises across various industries in the U.S. involved in assessing strategic security services (SSS) providers. Specifically, it is aimed at decision-makers responsible for evaluating service providers offering security audits, compliance and risk advisory services, security assessments, security solution consulting and awareness and training.

The increasing reliance on cybersecurity consulting services is propelled by several factors, including the escalating frequency and sophistication of cyberattacks, the demand for advanced security solutions and the growing adoption of cloud-based services. Consequently, organizations are investing in security consulting services to bolster their cybersecurity defenses and counter cyber threats effectively.

In the U.S., the cybersecurity consulting sector is witnessing significant growth and transformation. Organizations are increasingly realizing the importance of robust cybersecurity strategies in safeguarding their sensitive data and digital assets.

The ever-evolving complexity of modern cyber threats and the rapid advancements in technology pose substantial challenges for enterprises striving to fortify their digital infrastructure. Strategic security consulting plays a pivotal role in guiding organizations through this dynamic landscape, equipping them with the necessary expertise and guidance to implement effective security measures and mitigate risks efficiently. Therefore, this report is essential for U.S. enterprises navigating the complexities of cybersecurity and seeking to enhance their security posture effectively.



Strategy professionals within enterprises across industries in the U.S. should read this report to understand security service trends, aiding in provider selection and cybersecurity enhancement.



IT leaders and security professionals should read this report to understand the evolving landscape of IT security consulting services.

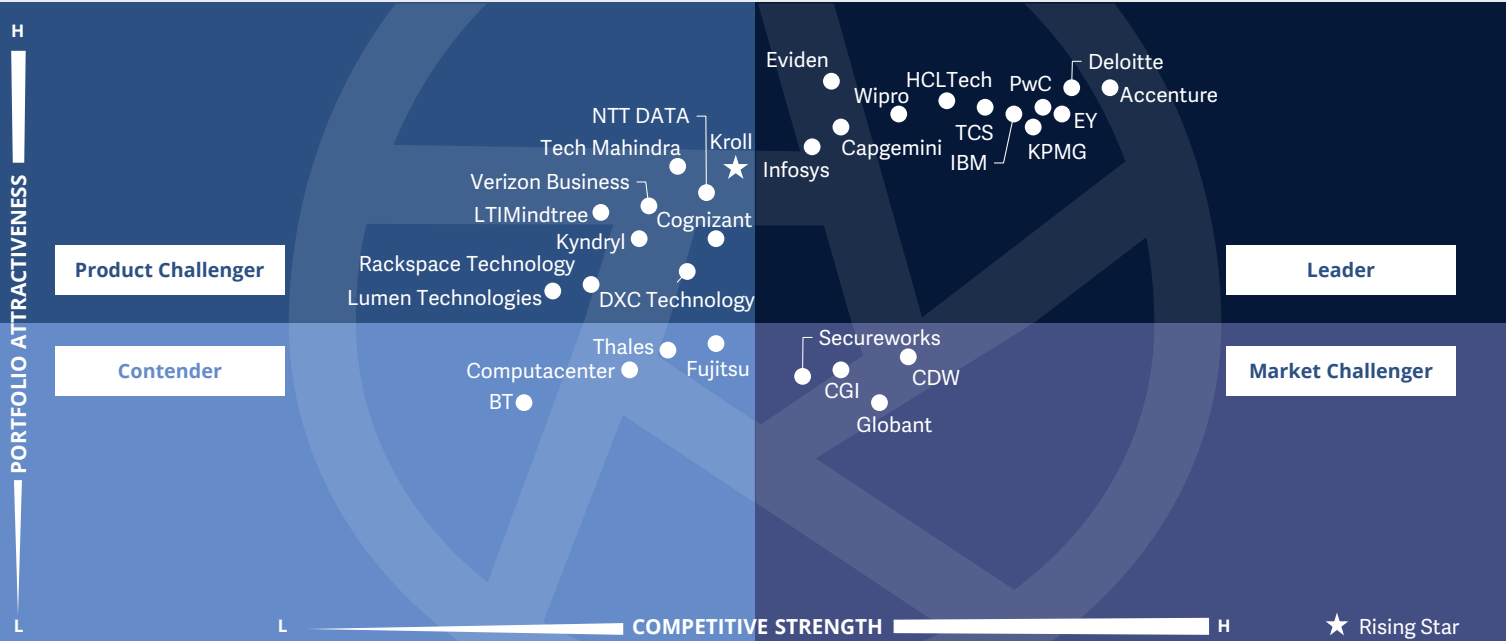


Business analysts and consultants specializing in cybersecurity or enterprise strategy will benefit from the insights into the current cybersecurity landscape provided in this report.



Cybersecurity – Solutions and Services
Strategic Security Services (Large Accounts)

U.S. 2024



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 road maps for recovery.**

Gowtham Sampath



Strategic Security Services (Large Accounts)

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting, and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with 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 vCISO (virtual Chief Information Security Officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity road maps 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, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Offer at least one of the above strategic security services in the respective country
3. Provide security consulting services using frameworks
4. No exclusive focus on proprietary products or solutions



Strategic Security Services (Large Accounts)

Observations

The U.S. cybersecurity advisory and consulting market is poised for continued growth driven by the need for increased risk assessments, complex cybersecurity technology and digital transformation initiatives.

Current trends:

Enterprises are shifting from reactive incident response to proactive security measures. This includes risk assessments, vulnerability management, penetration testing and security awareness training.

Security providers are moving toward integrated solutions that combine advisory, consulting, risk assessment and resilience services into a single offering.

As cloud adoption accelerates, demand for cloud-specific security expertise is soaring.

Security services leverage automation and ML to streamline processes, improve threat detection accuracy and reduce human error.

Large enterprise challenges:

The cybersecurity skills gap makes it difficult for enterprises to build and maintain in-house security teams.

The ever-changing regulatory landscape with frameworks such as HIPAA, PCI DSS and GDPR necessitates ongoing compliance assessments and adjustments to security posture.

The expanding attack surface due to third-party vendors necessitates robust vendor risk management (VRM) processes.

Integrating various security solutions from different vendors can be complex.

Enterprises value providers with the following characteristics:

Deep understanding of their specific industry's security threats and compliance requirements

Access to real-time threat intelligence feeds allows enterprises to stay ahead of evolving cyber threats and prioritize security investments

Ability to demonstrate a clear ROI from their security services

From the 78 companies assessed for this study, 30 qualified for this quadrant, with twelve being Leaders and a Rising Star.

accenture

Accenture acquired CyberTech, a cybersecurity consultancy specializing in OT security. This bolsters its expertise in securing critical infrastructure, which is increasingly crucial for U.S. organizations across various industries.

Capgemini

Capgemini actively participates in industry conferences and workshops focused on cyber resilience. The company's involvement in these events demonstrates its commitment to helping U.S. companies build robust incident response and recovery capabilities.

Deloitte.

Deloitte's *Cyber Threat Hunting Report 2024*, released in February 2024, highlights new and concerning tactics cybercriminals use. This ongoing threat research showcases the provider's commitment to keeping clients informed about the latest cyber threats.

EVIDEN an atos business

Eviden (an Atos Business) showcases strong technical competency and has customized its portfolio to build innovative cybersecurity services around zero trust and emerging technologies, such as cloud, 5G, IIoT and IoT, focusing more on the strategic and assessment areas of technology consulting.

EY

EY's Cognitive Cyber Centre offers a cohesive, integrated cybersecurity platform designed to empower businesses to identify, respond to and prevent emerging threats utilizing AI, ML, advanced behavioral analytics and threat-hunting capabilities.

HCLTech

HCLTech prioritizes business objectives over specific technologies and ensures that solution aligns with clients' overall security strategy with dedicated labs and CoEs, continuously researching and analyzing relevant technologies such as GenAI, ML and blockchain.



Strategic Security Services (Large Accounts)



IBM's unified security approach is vendor-agnostic, providing enterprises with predictive and proactive cyber risk management across an enterprise's security program with a focus on proprietary techniques and technologies to guide clients through transformation.



Infosys partners with QuintessenceLabs for quantum cryptography to help enterprises build secure connections. With quantum cryptography, Infosys can help protect data stores with high entropy symmetric keys and quantum-safe encryption.



KPMG helps businesses develop and implement strategic cyber programs. These programs involve in-depth risk assessments, financial analysis of cyber threats and the creation of a well-structured decision-making framework.



PwC's Global Centre for Crisis & Resilience consists of a dedicated team of professionals that support clients with crisis readiness, response and recovery. Its industry-specific knowledge and regulatory insights enable clients to navigate complex cybersecurity challenges.



TCS' Machine First approach helps enterprises realize resiliency with data and applications secured in the cloud from current and emerging threats. TCS' advisory is powered by nine CoEs that focus on designing research-backed, cutting-edge cybersecurity solutions.



Wipro's acquisitions of strategy consulting firms Ampion, Capco and Edgile have led to the development of Wipro CyberTransform, an integrated suite to help enterprises accelerate their digital transformation in a highly secure manner, against modern threats and risks.

Kroll

Kroll's (Rising Star) seven-step process is enhanced through its experience conducting cyber tabletop exercises (TTX) for organizations of diverse sizes, complexity and industry sectors, helping enterprise teams practice their roles to perform effectively during incidents.



Infosys



“Infosys’ cybersecurity advisory and consulting, risk assessment, robust infrastructure and resilience capabilities in the U.S. are built on a comprehensive strategy and framework, with an integrated approach and strong focus on zero trust security.”

Gowtham Sampath

Overview

Infosys is headquartered in Bengaluru, India. It has more than 322,600 employees across 274 offices in 56 countries. In FY23 the company generated \$18.2 billion in revenue, with Financial Services as its largest segment. It has a strategic alliance with over 25 leading security vendors and OEMs to develop joint solutions. With approximately 6,000 dedicated cybersecurity professionals worldwide, Infosys offers service capabilities around cyber advisory and GRC. Infosys’ security consulting capabilities span zero trust, data security, IAM, OT security and compliance, cloud security, and quantitative and cyber risk management.

Strengths

Integrated approach: Infosys’ cybersecurity program is an amalgamation of a comprehensive cybersecurity strategy and framework, proficiently driven through a strong governance program endorsed by the Management — Information Security Council and the Board. The Information Security Group plays a vital role in delivering assurance and trust to all Infosys customers and stakeholders by securing their information and information systems.

Comprehensive offerings: Infosys’ SSS are divided into two categories: Cyber Consulting & Advisory and GRC Services. These categories help fortify cyber resiliency by advising and supporting customers to proactively navigate their cybersecurity risks, including strategic, operational, reputational,

technical and compliance aspects.

This approach helps build robust and scalable strategies, frameworks, policies and architecture, thereby assuring digital trust.

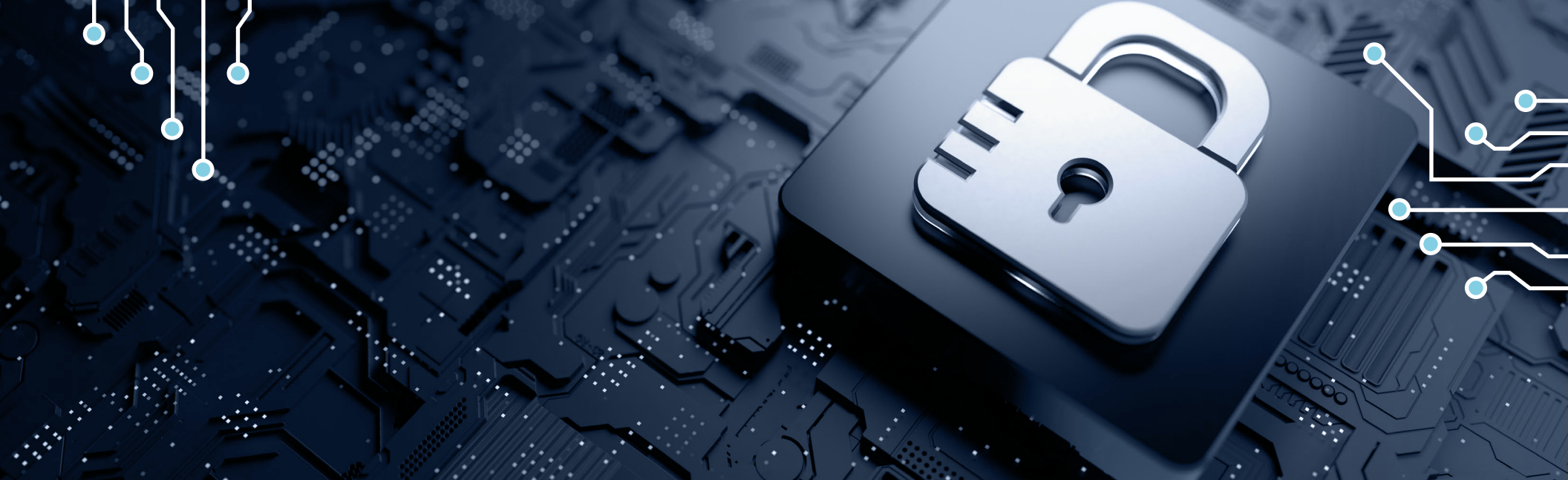
Aligning with business strategy:

Infosys empowers enterprises to make informed decisions while aligning their enterprise/security strategy with the dynamic ecosystem of tools, technologies, regulations, suppliers and workforce in an integrated, agile, scalable and cost-effective manner. This helps them improve visibility, prioritize cyber spend, align cybersecurity strategy with enterprise strategy and drive a culture of risk-based decision-making.

Caution

While Infosys offers security assessments, its primary focus might be on general security posture evaluations, potentially limiting its capabilities for U.S. enterprises seeking advanced threat intelligence or red teaming services, which are offered by established providers with dedicated practices in these areas.





Strategic Security Services (Midmarket)

Strategic Security Services (Midmarket)

Who Should Read This Section

This report is pertinent to midsize enterprises in the U.S. seeking strategic security services (SSS). It is essential for decision-makers responsible for selecting security service providers. The report evaluates firms offering a spectrum of services, including security audits, compliance and risk advisory, assessments, consulting on security solutions and training programs.

Enterprises tasked with safeguarding their enterprises' digital assets, privacy and compliance standards should closely examine this report. It provides valuable insights into the capabilities of various service providers, aiding in informed decision-making aligned with organizations' security needs and budget constraints.

Key trends in enterprise adoption highlighted in this report include an increasing recognition of the importance of robust cybersecurity measures, driven by rising cyber threats and regulatory requirements. Midmarket enterprises are increasingly investing in comprehensive security solutions to protect their sensitive data and maintain regulatory compliance. Additionally, there is a growing emphasis on proactive security measures, such as regular security audits and employee training, to mitigate risks effectively.

This report serves as a valuable resource for midmarket enterprises navigating the complex landscape of SSS. It enables them to make informed decisions to enhance their cybersecurity posture and safeguard their business operations.



Strategy professionals should read this report to stay informed about SSS and ensure alignment with overall IT goals and objectives.



IT directors responsible for the implementation and management of IT infrastructure should read this report to ensure organizations' systems and networks are adequately protected.



Security professionals should read the report to gain insights into SSS to develop and implement robust cybersecurity strategies.

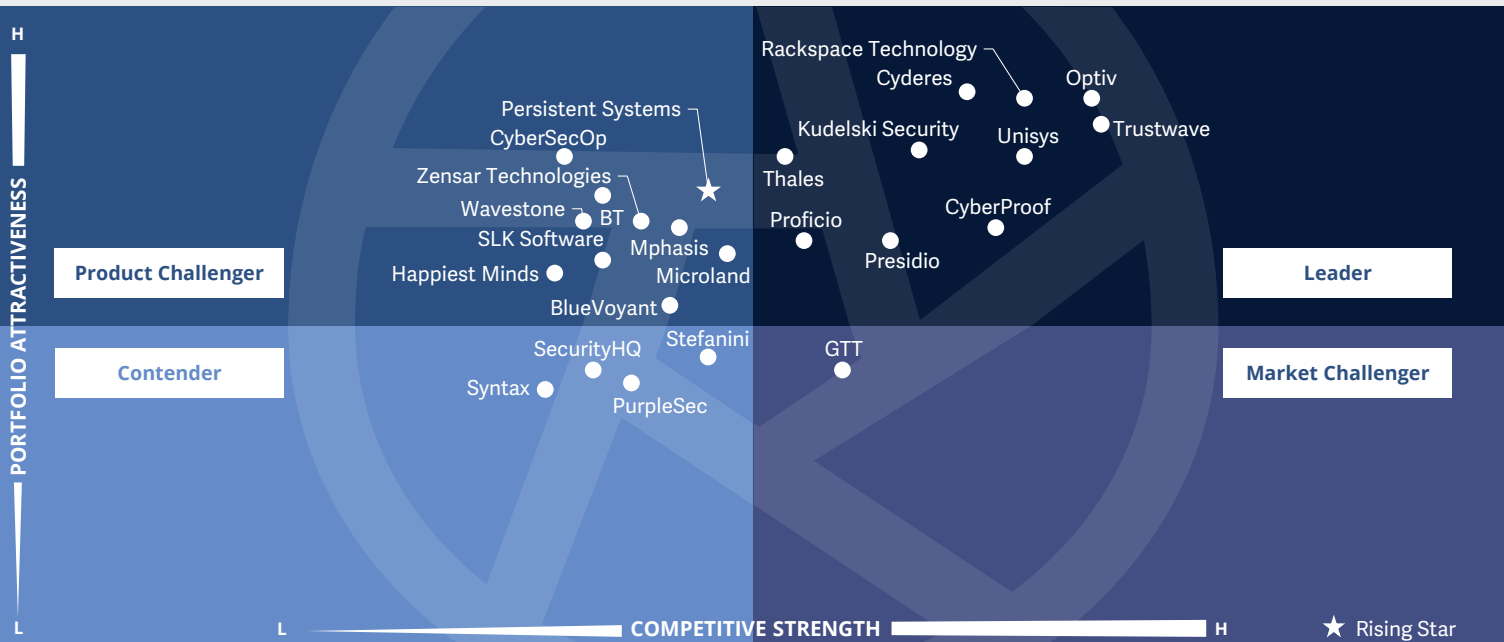


Technology professionals should read this report to be aware of the latest trends and solutions in cybersecurity to guide technology-related decisions.



**Cybersecurity – Solutions and Services
Strategic Security Services (Midmarket)**

U.S. 2024



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 road maps for recovery.**

Gowtham Sampath



Strategic Security Services (Midmarket)

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting, and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with 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 vCISO (virtual Chief Information Security Officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity road maps 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, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Offer at least one of the above strategic security services in the respective country
3. Provide security consulting services using frameworks
4. No exclusive focus on proprietary products or solutions



Strategic Security Services (Midmarket)

Observations

The U.S. SSS midmarket is expected to continue its strong growth trajectory. As cyber threats evolve, midsize enterprises must adopt proactive cybersecurity approaches. Finding the right security provider with experience, expertise and cost-effective solutions will be pivotal to success in this dynamic digital landscape.

Key trends:

The ever-changing threat landscape, marked by sophisticated attacks, underscores the need for proactive security measures across all business sizes.

Stricter data privacy regulations such as GDPR and CCPA compel midsize enterprises to invest in robust security practices.

The migration of MSEs to cloud environments drives the demand for cloud security expertise.

Key challenges:

Security budgets often lag behind evolving threats and finding skilled cybersecurity professionals can be difficult.

Implementing robust security controls may sometimes impede business agility, requiring a careful balancing act.

Understanding and integrating various security tools can be overwhelming for in-house IT teams.

Midsize enterprises may lack the dedicated cybersecurity expertise necessary to manage and maintain a comprehensive security posture.

Differentiation in cybersecurity providers:

Offering security solutions tailored to the specific needs and budget of midsized businesses

Demonstrating a track record of implementing industry-standard security controls for midsize enterprises in their respective sectors

Prioritizing clear communication and providing ongoing security awareness training for employees

Recognizing the growing reliance of midsize enterprises on third-party vendors and offering robust vendor risk management practices

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



CyberProof's consulting and professional services offer proactive addressing and overseeing cyber risks, ensuring the confidentiality, integrity and availability of data, systems and operations. This fosters trust and delivers long-term value to clients.

Cyderes

Cyderes has strategically acquired Ipseity Security, a top IAM firm. This acquisition enhances Cyderes' proficiency in cloud identity, access governance and PAM, while facilitating broader service expansion within the entire IAM ecosystem.

Kudelski Security

Kudelski Security is expanding its U.S. presence to meet the growing market demand for cybersecurity offerings and managed services. The Phoenix location will serve as the U.S. headquarters for the security business, featuring an executive briefing center and Cyber Fusion Center.

Optiv

Optiv is undertaking expansion initiatives driven by intensifying cyber threats and evolving customer needs. These initiatives include services for managing and remediating vulnerabilities by offering consulting services to build an effective vulnerability management program.

Presidio

Presidio, recognized as one of Cisco's top partners, has aggressively expanded its cloud and security services offerings in the last five years. The company has strong partnerships with AWS, Google, Microsoft, Palo Alto Networks and Dell Technologies.



Proficio Breach and Attack Simulation (ProBAS) offers robust and responsive cybersecurity, combining advanced technology with expert analysis. This proactive approach helps identify vulnerabilities, thoroughly assess infrastructure and empower teams against various cyber threats.



Strategic Security Services (Midmarket)



Rackspace Technology's skilled consultative services, combined with cybersecurity strategy planning and assessments, safeguard enterprise digital investments. This ensures security resilience and compliance, leading to predictable business outcomes.



Thales Cybersecurity Solutions & Consulting offering analyzes cybersecurity risk for mission-critical systems and organizations. Thales also provides Cybersecurity Enterprise HealthCheck, a modular assessment tool that measures businesses' cyber maturity.



Trustwave's in-depth analysis reveals the cybersecurity threats faced by educational institutions. This insight equips cybersecurity leaders in the education sector with actionable strategies to mitigate sector-specific risks.

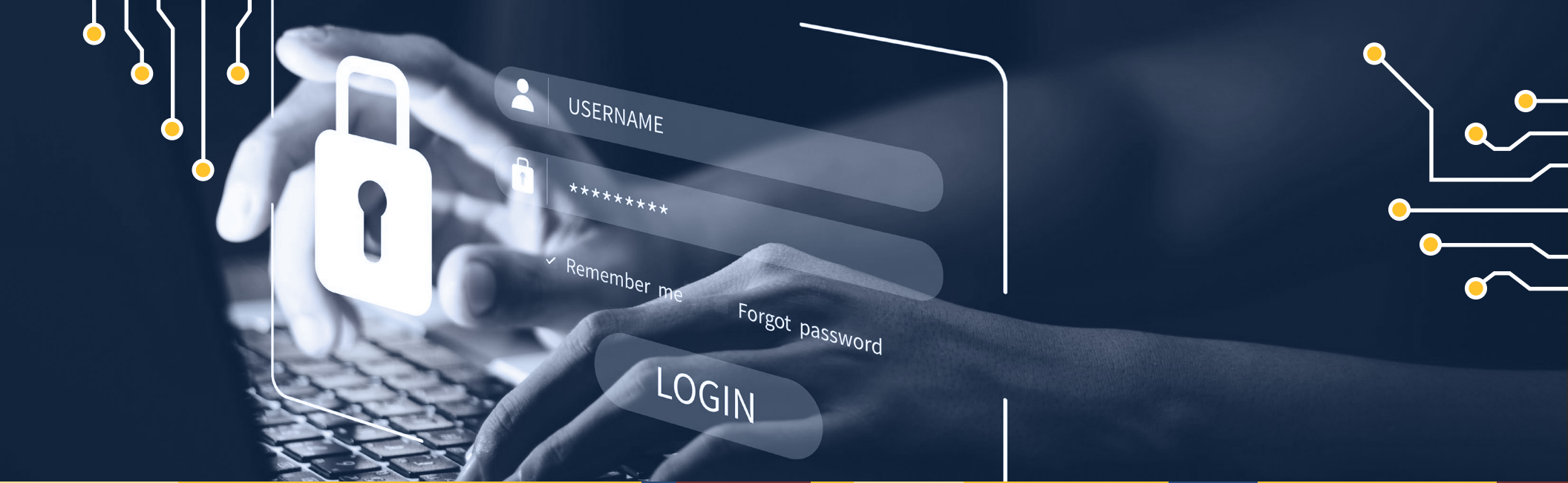


Unisys' consulting services guide clients in identifying critical operational objectives and aligning strategic technology goals. These services assist in developing a robust security strategy that minimizes cyber risk and delivers maximum business value.



Persistent Systems (Rising Star) helps clients in their journey toward a secure digital future, providing expertise, agility and unwavering support using established industry frameworks such as NIST and ISO and vertical industry-centric best practices.





Managed Security Services - SOC (Large Accounts)

Managed Security Services - SOC (Large Accounts)

Who Should Read This Section

This report is crucial for U.S. enterprises evaluating managed security service providers (MSSPs). It assesses providers offering services related to continuously monitoring IT and OT security infrastructures and IT infrastructure management.

With the rise in cyber threats, businesses are increasingly turning to specialized providers for comprehensive security solutions. MSS are evolving to meet the demands of cloud-focused operations, providing tailored solutions for cloud-native security, threat detection and data protection.

Enterprises seek providers utilizing threat intelligence and advanced analytics to proactively identify and mitigate security threats, with a focus on ML- and AI-powered threat detection. Managed detection and response (MDR) services, combining threat detection, incident investigation and response orchestration, are gaining popularity for enhanced incident response capabilities.

Addressing regulatory pressures, MSSPs offer compliance-focused solutions to help enterprises meet industry regulations and data protection laws, avoiding penalties and data breaches. The adoption of zero trust security architecture is on the rise, with providers assisting in implementing principles such as continuous authentication and micro-segmentation.

As remote and mobile devices access corporate networks, the demand for managed endpoint security services is growing. Providers offer solutions such as endpoint protection platforms (EPP), endpoint detection and response (EDR) and mobile device management (MDM) to secure diverse endpoints.



Security professionals should read this report to gain insights into the latest trends and best practices for selecting MSS.



Technical professionals deciding on cybersecurity strategies, services and providers will find valuable information to make informed choices for enhancing their organization's security posture.

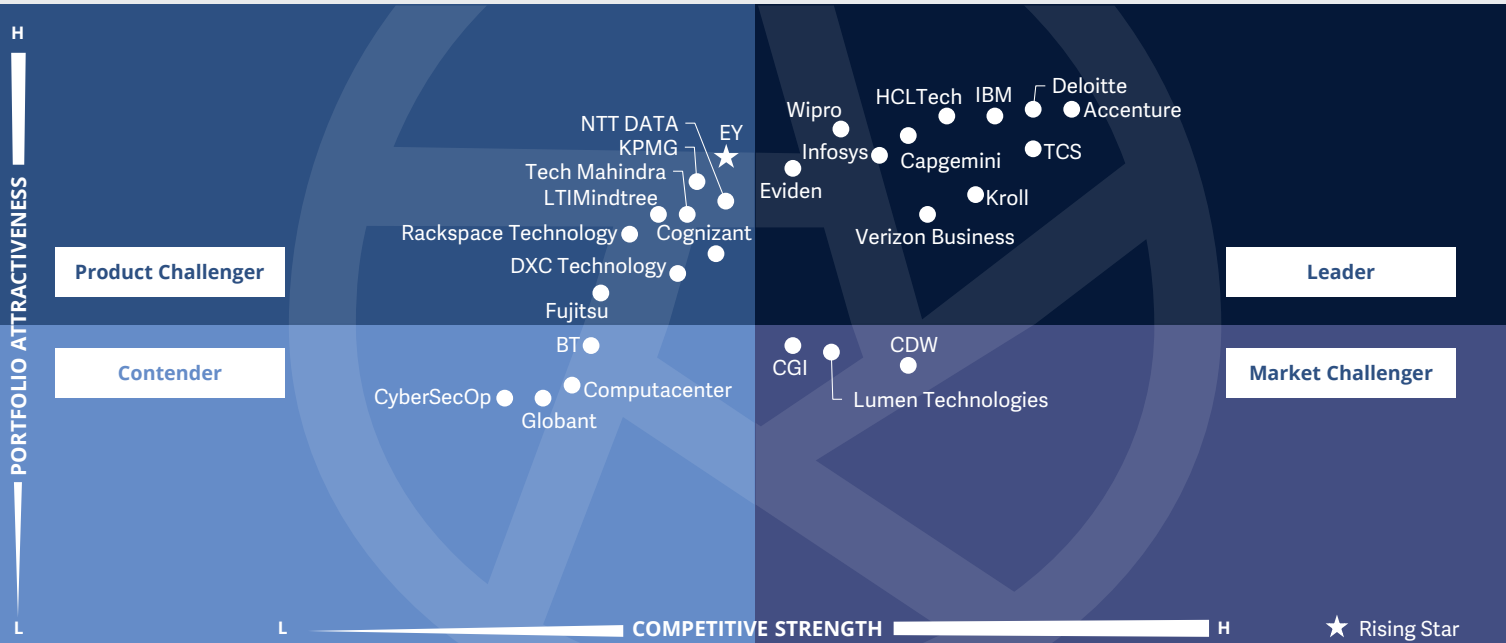


Risk management professionals involved in GRC can gain insights into how MSS align with regulatory requirements and contribute to overall risk mitigation.



Cybersecurity – Solutions and Services
Managed Security Services - SOC (Large Accounts)

U.S. 2024



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

Gowtham Sampath



Managed Security Services - SOC (Large Accounts)

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). 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 SOC's support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools.

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 SOC's**
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



Managed Security Services - SOC (Large Accounts)

Observations

The U.S. MSS market is experiencing significant growth fueled by several key factors:

The increasing sophistication of cyberattacks compels businesses to seek advanced security monitoring and threat detection capabilities.

The cybersecurity skills gap makes it difficult for large enterprises to build and maintain in-house security teams, driving them toward MSS providers for support.

Stricter data privacy regulations such as GDPR and CCPA necessitate ongoing security monitoring and compliance management, increasing the demand for MSS and MDR services.

Enterprises' migration to cloud environments necessitates cloud-based security monitoring and management solutions to protect their digital assets.

Large enterprises face unique challenges in the MSS and MDR market:

Managing security across diverse on-premises, cloud and hybrid environments requires specialized expertise and integration capabilities.

Entrusting sensitive data to a third-party security provider requires careful evaluation of data security practices and contractual agreements.

Large enterprises require customized security solutions tailored to their specific threat landscape and industry regulations.

Enterprises seek specific strengths when selecting MSS and MDR providers:

A comprehensive suite of services, including threat detection, incident response, vulnerability management and security information and event management (SIEM).

Leverage automation, AI, ML and threat intelligence to identify and respond to sophisticated cyberattacks in real time.

Ability to scale services up or down to meet evolving security needs, especially in cloud environments.

Clear communication regarding security incidents, service performance and security best practices.

From the 78 companies assessed for this study, 27 qualified for this quadrant, with eleven being Leaders and a Rising Star.

accenture

Accenture's MDR services include early detection and response capabilities, security monitoring for on-premises and cloud infrastructure, SaaS security monitoring and security analytics and automation. It provides curated playbooks and use case libraries to enhance threat detection and response.

cognizant

Capgemini's MSS and MDR capabilities leverage the MITRE ATT&CK framework, enabling the use of tactics and techniques for developing use cases to enhance threat detection and response capabilities.

Deloitte.

Deloitte is a recognized security leader in Google Cloud's alliance ecosystem, with nine Google Cloud specializations and thousands of certified practitioners, demonstrating its industry-leading expertise in managed cloud security services.

EVIDEN an atos business

Eviden (an Atos Business) MDR solution uses advanced security analytics on endpoints, user behavior, applications and networks for deeper multivector detection. Atos Alsaac® leverages over 75 AI models to enable automated hunting and data mining.

HCLTech

HCLTech's Universal MDR service empowers organizations to proactively detect and respond to cyber threats across infrastructure, cloud, applications, identities, networks, users and endpoints. It offers real-time alerting, detection and response capabilities for holistic protection.

IBM.

IBM offers a comprehensive security ecosystem, integrating its best-in-class security products alongside third-party solutions within its MSS and MDR services. This offering provides a unified security environment and access to a wider range of security capabilities.



Managed Security Services - SOC (Large Accounts)



Infosys relies on strategically located cyber defense centers to deliver MDR services. Its Cyber Next platform constantly monitors threats and delivers intelligence for comprehensive protection.

Kroll

Kroll's Responder MDR employs an outcome-based approach by identifying and stopping threat actors before significant harm occurs. It enhances Microsoft's technology by integrating frontline threat intelligence, enabling thorough and efficient threat hunting.



TCS delivers services through 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 MSS that can integrate with existing technology stacks.

Verizon Business

Verizon Business offers advanced SOC solutions that are customizable for enterprises to maximize their SIEM and related security investments. These solutions enable clients to monitor and manage all IT assets via a single interface and dashboard.



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

EY

EY's (Rising Star) next-generation TDR solutions integrate specialized talent, streamlined processes and cutting-edge technology. It offers comprehensive visibility into the attack lifecycle, bolstering the capability to detect, hunt and respond to threats.





“Infosys focuses on building trust and transparency in its advanced MSS and MDR capabilities and helps organizations effectively manage incidents and threats, contain and remediate security anomalies, and improve their overall cybersecurity posture.”

Gowtham Sampath

Infosys

Overview

Infosys is headquartered in Bengaluru, India. It has more than 322,600 employees across 274 offices in 56 countries. In FY23 the company generated \$18.2 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 (CDCs). With a focus on security transformation, Infosys supports clients with a wide array of proprietary tools, solution accelerators and playbooks for MSS for accelerated value realization.

Strengths

Advanced security platform: Infosys’ MSS are powered by an advanced security platform that provides 24/7 security monitoring and threat intelligence via a global network of CDCs. This platform helps organizations effectively manage incidents and threat management by leveraging advanced security platforms and a global pool of security analysts.

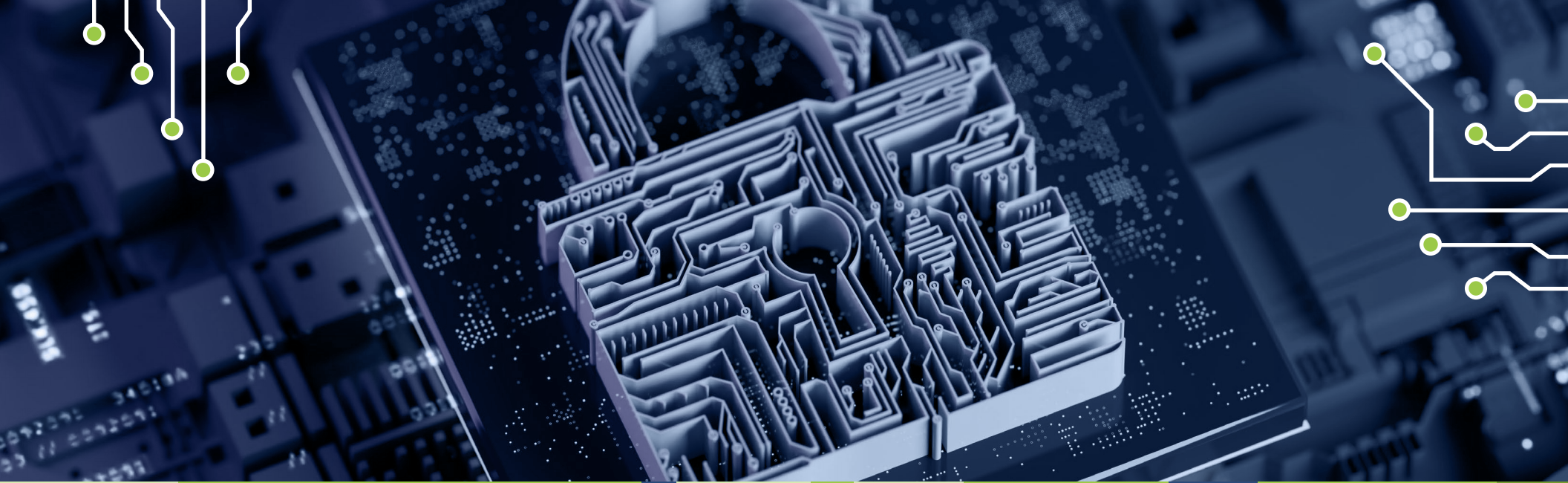
Integrated threat intelligence: Infosys’ MSS offer integrated threat intelligence, which helps organizations stay informed about the latest threats and vulnerabilities. This integrated threat intelligence is delivered through a global network of cyber defense centers, providing organizations with a comprehensive view of the threat landscape.

Comprehensive solution: Infosys’ MSS offer a comprehensive solution for round-the-clock security, including security monitoring and platform support for SOC tools such as SIEM, SOAR, threat intelligence platform (TIP), user and entity behavior analytics (UEBA), decoy services, forensics, malware reverse engineering and threat hunting. These comprehensive solutions help identify, investigate and respond to threats effectively and efficiently. Infosys’ MSS provide threat containment by leveraging highly skilled global SWAT teams.

Caution

Infosys should develop its own proprietary security tools and solutions to reduce reliance on partners and ensure greater control over the quality and performance of its offerings. Its emphasis on cost-effectiveness might lead to standardized service packages with limited customization options.





Managed Security Services - SOC (Midmarket)

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

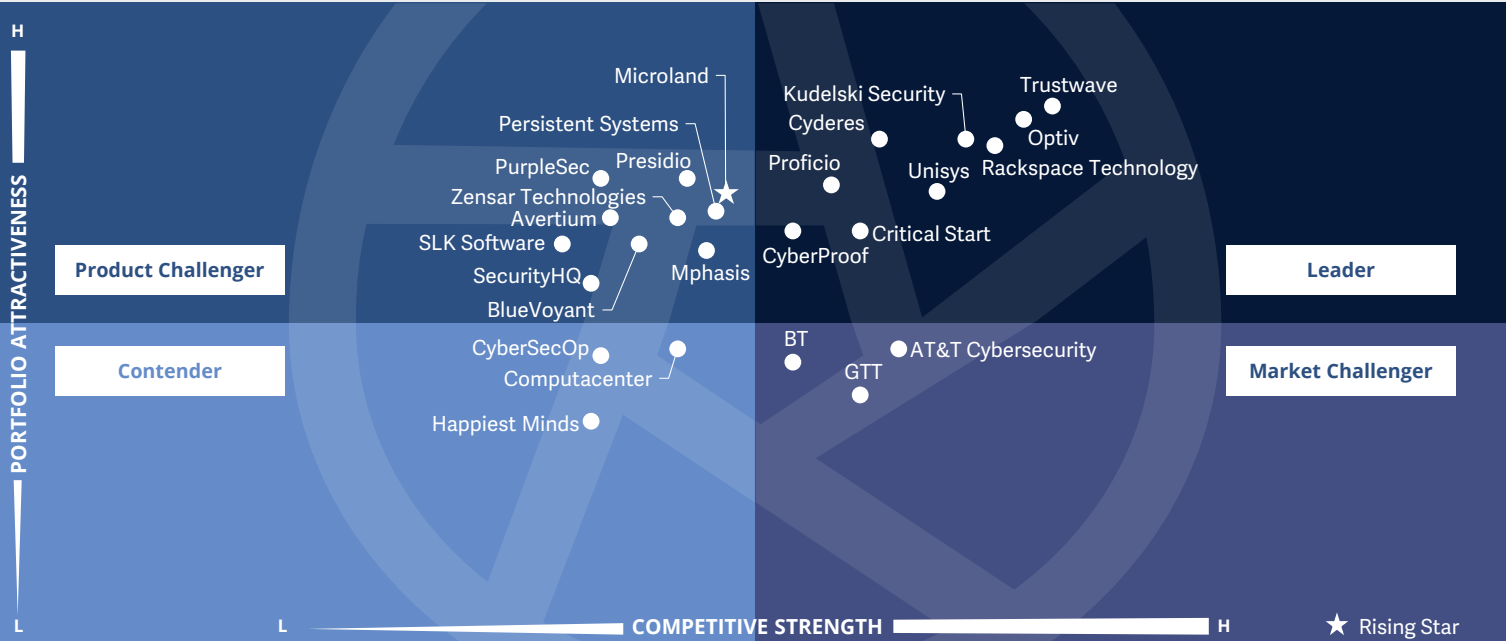


Risk managers should read this report to identify, assess and mitigate cybersecurity risks that could impact their operations and objectives.



Cybersecurity – Solutions and Services
Managed Security Services - SOC (Midmarket)

U.S. 2024



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



Managed Security Services - SOC (Midmarket)

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



Managed Security Services - SOC (Midmarket)

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.

Cyber**Proof**
AUST 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.

Cyberes

Cyberes' 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.



Managed Security Services - SOC (Midmarket)



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.





Digital Forensics and Incident Response

Who Should Read This Section

This report addresses U.S. enterprises assessing digital forensics and incident response (DFIR) service providers, seeking prompt incident response, advanced threat detection, using technologies such as ML and thorough forensic analysis for root cause understanding and legal compliance.

Challenges faced by enterprises encompass skill shortages, incident complexity, integration issues and resource constraints. Skill gaps in DFIR expertise may impede internal incident response, emphasizing the critical role of external providers. Modern cyber threats' intricate nature necessitates specialized expertise for effective navigation.

Enterprises expect transparency, customized solutions, knowledge sharing and post-incident recommendations from DFIR providers. Clear and ongoing communication, tailored services, collaborative knowledge transfer and proactive guidance are considered pivotal for successful partnerships.

Several adoption trends have emerged amid these expectations. Managed DFIR services are gaining popularity as enterprises outsource incident response processes. Automation and orchestration streamline DFIR workflows, improving response times. Integration with threat intelligence services is widespread, enhancing incident detection and response capabilities. Cloud-based DFIR solutions are also gaining traction in line with the growing reliance on cloud services.



Security professionals managing incident response and cybersecurity operations should read this report to understand the trends and challenges in the DFIR landscape.



Strategy professionals overseeing security posture of enterprises can benefit from insights this report gives into the challenges, expectations and adoption trends in DFIR services.



Technology professionals procuring technology services, including DFIR services, can use the report to assess criteria and considerations when selecting DFIR service providers.

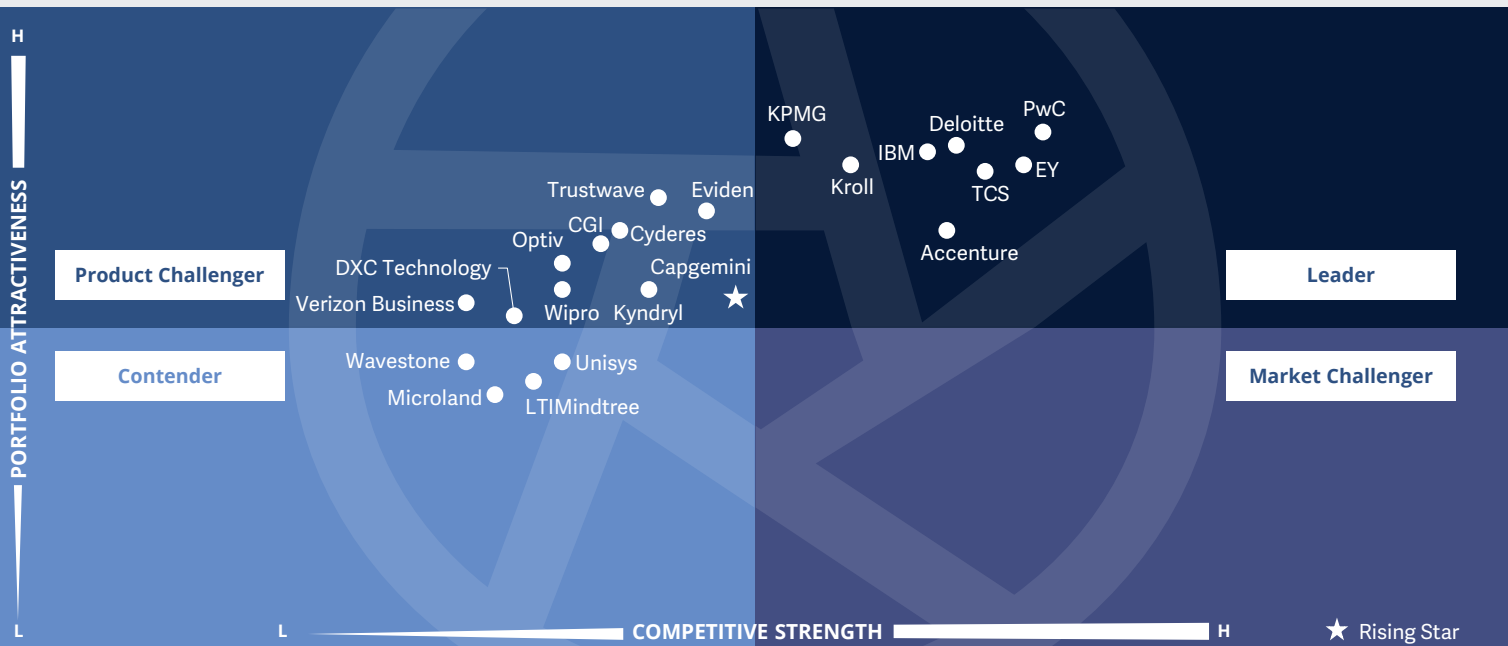


Compliance professionals overseeing compliance requirements should read this report to understand DFIR services' contribution to legal compliance.



Cybersecurity – Solutions and Services
Digital Forensics and Incident Response

U.S. 2024



This quadrant assesses providers that offer digital forensics and incident response services that establish **effective threat response, utilizing sophisticated incident response playbooks and forensics to understand threat actor behavior and root causes.**

Gowtham Sampath



Digital Forensics and Incident Response

Definition

Providers assessed in the DFIR quadrant offer services related to threat response activities while preserving evidence against attackers.

DFIR involves the identification, investigation, containment, and remediation of cybersecurity incidents. The escalation in frequency and severity of cybersecurity incidents has added to the adoption of DFIR services. Service providers should showcase in-depth and hands-on capabilities in addressing digital forensics, electronic discovery, predefined criteria-based triage, timeline analysis, log analysis, malware analysis and artifact examination. Following a breach, DFIR plays a vital role in uncovering data loss and damage specifics.

DFIR services help establish effective threat response, utilizing sophisticated incident response playbooks and forensics to understand threat actor behavior and root causes. DFIR providers should possess experience in assisting enterprises with

litigation support for insurance claims and post-breach regulatory audits. They are adept in using in-house and third-party tools such as security information and event management (SIEM), security orchestration, automation and response (SOAR), endpoint detection and response (EDR), and extended detection and response (XDR).

This quadrant examines service providers that provide proven DFIR techniques, methodologies and are able to work with best-of-breed tools to respond to cybersecurity incidents.

Eligibility Criteria

1. Must have a **dedicated incident response team** (CERT or CSIRT) of experts with relevant certifications such as GCFA, GCFE and CISSP, showcasing their expertise and commitment to maintaining industry standards.
2. Possess experience and expertise in **handling a variety** of SIEM, SOAR, EDR and XDR solutions
3. The DFIR services will **not only identify the breach** but also create the timeline, root cause and impact of the breach.
4. **Possess capabilities** in malware analysis, ransomware decryption and data recovery
5. Demonstrate **partnership** with relevant product vendors and MSS providers to gather threat intelligence, dark web monitoring, and SOC capabilities to mitigate advanced persistent and sophisticated threats.



Digital Forensics and Incident Response

Observations

Organizations will increasingly rely on DFIR services to have a robust incident response plan, investigate and mitigate security incidents effectively and meet compliance requirements. The U.S. market is experiencing significant growth fueled by several key factors listed below:

Organizations are moving beyond reactive incident response to proactive threat hunting, identifying and neutralizing potential security breaches before they occur.

Data privacy regulations such as GDPR and CCPA necessitate stricter data breach reporting requirements, driving demand for DFIR services for investigations and evidence collection.

With organizations migrating to cloud environments, the need for cloud-based forensics capabilities and expertise is rising.

Enterprise challenges necessitating DFIR deployments:

Complexities of investigating incidents across diverse landscapes with on-premises, cloud and hybrid setups.

Skills gap makes it difficult for enterprises to build and maintain in-house DFIR teams.

Lack of specialized expertise for swift response and recovery efforts to minimize downtime and data loss.

Complexities of collecting and preserving digital evidence that meets legal and regulatory requirements in the event of a cyberattack.

Differentiation and characteristics of DFIR providers:

Available to deploy DFIR teams around the clock, as rapid response capabilities are crucial

Services that help develop and test incident response plans and train employees on best practices

Access to advanced forensic tools for efficient evidence collection, analysis and reporting, including cloud environments

Understanding the legal nuances of evidence collection and chain of custody procedures with clear communication throughout the investigation process

From the 78 companies assessed for this study, 22 qualified for this quadrant, with eight being Leaders and a Rising Star.

accenture

Accenture partners with Palo Alto Networks to help maximize value for organizations. The partnership helps identify risk exposure in OT networks and benefits from real-time intelligence and responses, simplified security and reduced costs.

Deloitte.

Deloitte's alliance with Akamai offers Zero Trust micro-segmentation and incident response services. This alliance combines Deloitte's cybersecurity, network forensics and security expertise with the Akamai Guardicore Segmentation solution.

EY

EY's forensics crisis management services team of over 4,000 forensic and technology professionals helps clients navigate various crises and helps organizations proactively protect against risks and manage a situation that disrupts businesses.

IBM

IBM Security X-Force® Incident Response Retainer offers a subscription-based service with tiered response plans, granting access to a team of trusted experts trained to assist in effectively responding to threats and potential attacks with flexibility and pricing options.



Digital Forensics and Incident Response



KPMG's cybersecurity response services team helps detect, respond to and recover from cyber breaches through immediate response services with expertise in investigations, digital forensics and recovery, enabling organizations to mitigate risks.

Kroll

With services such as device and server reimaging, directory rebuilding, network fortification and segmentation, hardware enhancements and patch management, **Kroll's** incident response team accelerates systems recovery and minimizes operational disruptions.



PwC's cybersecurity incident response and digital forensics team adopts a comprehensive, reactive, proactive and predictive approach to restore operations, pinpoint the root cause and recommend measures to prevent the recurrence of security breaches.




TCS' digital forensics and incident response services encompass a comprehensive range of capabilities to pinpoint deficiencies in the current security infrastructure and aid businesses in anticipating, detecting and mitigating security incidents.



Capgemini's (Rising Star) Computer Emergency Response Team (CERT-C) performs digital forensics activities, including endpoint forensics, memory forensics, smartphone forensics, network forensics, cloud forensics and malware analysis activities.





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.



Appendix

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 Saylor

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 & Editor Biographies

Author



Gowtham Sampath
Senior Manager, ISG Provider Lens™

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.

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.





JULY, 2024

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES