

Cybersecurity – Solutions and Services

Technical Security Services

A report comparing provider portfolio
attractiveness and competitive strengths

Customized report courtesy of:



Executive Summary	03
Provider Positioning	09
Introduction	
Definition	17
Scope of Report	18
Provider Classifications	19
Appendix	
Methodology & Team	30
Author & Editor Biographies	31
About Our Company & Research	34
Star of Excellence	27
Customer Experience (CX) Insights	28

Technical Security Services	20 – 26
Who Should Read This Section	21
Quadrant	22
Definition & Eligibility Criteria	23
Observations	24
Provider Profile	26

*Report Author: Phil Hassey,
Dr. Maxime Martelli, and
Gowtham Sampath*

U.S. public sector agencies must fight increasingly sophisticated attacks on a constant basis

Data breaches are costly. The average U.S. cybersecurity breach cost across the public and private sectors is \$9.5 million per breach. U.S. government agencies are not exempt from this, despite the government spending substantial sums on cybersecurity. At the federal level, the budget for 2024 is projected at \$12.7 billion. The largest allocation is for the Department of Homeland Security (DHS), with a budget of over \$3 billion. The federal government funds the State and Local Cybersecurity Grant Program (SLCGP), which allocates funds to states. The budget for this program was \$400 million in 2023. This amount is typically matched by state funding for cybersecurity projects, reflecting the high degree of spending

required to allow agencies to stand still from a cybersecurity perspective.

Research shows that cyberattacks impact approximately two-thirds of U.S. citizens.

Downtime for one breach in the local government was five months. When examining the attack targets, the top five states are Texas, Georgia, California, Florida and Pennsylvania.

This should be a concern for anyone closely monitoring the U.S. government, cybersecurity and geopolitics. Globally, across public and private sectors, cybersecurity represents a fundamental issue that can challenge the viability of organizations, regardless of their culture, safeguards and capabilities. The positive sign is that the U.S. government's focus on managing cybersecurity issues is improving; however, legislative and regulatory responses must be accelerated to keep pace. It is also evident that there is a significant divergence across government agencies regarding preparedness quality, vulnerability level, staff training and the successful defense and response to attacks. Small local agencies

**No agency operates
in isolation;
integrated
capability is critical
to fight cyber
threats.**



can be incredibly vulnerable and provide an entry point for hostile actors to more lucrative data-rich agencies and those that manage the critical infrastructure and data properties of the U.S. local, state and federal governments.

New potential threats arising from emerging technologies: Technology and innovation are essential for government agencies to build their capabilities and solutions for stakeholders. At the same time, new technology presents new opportunities for exploitation. GenAI is the latest example of this. GenAI will provide substantial benefits for agencies by optimizing service delivery for stakeholders, engaging in new technology, and maximizing the value of the data generated. At the same time, GenAI represents the latest end-to-end threat to government cybersecurity. This is going to be particularly true for those agencies that still lack a strong capacity for investing in robust systems from a cybersecurity perspective. GenAI could quickly turn from a value driver to a risk crisis point if an ill-considered investment is made.

Furthermore, the deployment of GenAI-based tools and large language models will drive the exploitation of government agencies. It is a

compelling arms race; the more innovation occurs, the more the risks and threats increase for both the public and private sectors, and the more that can be done to help mitigate threats. One of the challenges for government agencies in this environment is that they are forced constantly to look in their rear-view mirror. It is not easy to get ahead of the market, particularly at a time of frugality in a large proportion of government agencies at all levels of government.

Investment in skills will be accelerated. Over the next five years, a growing number of new jobs are needed to support the rising demand for cybersecurity services in the U.S. public sector. In addition, any government employee with any connection or contact with data and technology will need increasing training in cyber awareness and basic governance requirements. This is an expensive undertaking and one that will challenge many agencies. Any shortcomings in this will ensure that aggressive parties identify and exploit vulnerabilities.

Significance of education in addressing internal threats: External ransomware attacks, state-based hacking and other high-profile

issues often gain attention. However, the always underrated security threat is from within. In some cases, this activity is nefarious, and in other instances, it is merely a result of user error stemming from ignorance, poor training or simple carelessness. Such issues still present significant challenges, underscoring the increased role of training, access control development and consistency alongside monitoring capabilities. It is worth noting the connection between technology security and physical security. Agencies that leave doors unlocked and fail to manage access passes are likely to be more vulnerable in their technology security. This is due to the simple fact that attitude toward security is critical; any lax approaches in either domain will inevitably spill over.

Fundamentals of zero trust: Many agencies in the U.S. public sector and key regulators require a zero trust approach to cybersecurity. This approach requires mandates to protect critical infrastructure. Additionally, there is an increasing demand for simplicity and flexibility to be aligned with effective security solutions. Cybersecurity providers must develop more

comprehensive offerings that target an increasingly diverse customer base across the breadth of the sector while also adapting to their rapidly changing needs.

Accelerating vendor consolidation: Unsurprisingly, vendor consolidation is accelerating, driven by several related factors. It represents a natural shift where larger vendors acquire smaller firms to fill critical offering gaps, acquire skills or enter new markets. At the same time, this trend is also being driven by demand in both the public and private sectors. It is evident that proactive cyber management is becoming more challenging with each passing day. Integration issues are rampant, sometimes even within a single provider's set and across the many platforms required to manage a secure agency successfully. The increased cost of service delivery and managing a range of security providers has enabled consolidation to make management more accessible for clients and achieve the long-held goal of an integrated capacity for security.

More sophisticated U.S. government agencies are proactively looking to increase investments in incidence response automation to reduce



their level of investment and skills required for attack containment and remediation. As highlighted, AI has been a hot topic of discussion for both offensive and defensive actions in the U.S. public sector; automation represents a means of reducing human interaction on recurring tasks. Increasingly, there is a requirement for effective validation and analysis to accompany threat-hunting exercises.

Challenges of security ownership in

government agencies: Each agency has a different structure depending on its services, location, size and scale. However, the bottom line is that the head of the agency or university has to take investments and outcomes of cybersecurity within their scope of responsibilities. A chief information security officer (CISO), if one exists, cannot operate in isolation. Data is data; some agencies, and their private sector counterparts, risk delineating data between internal and external (or customer) data. Cybersecurity risks are too high to adopt this fragmented approach. Training requirements must be more explicitly prioritized across all levels of the organization, as humans are the source of error on many occasions.

Budget constraints are a major concern for U.S. government agencies dealing with increased threats from cyber actors. This constraint enhances the need to optimize outcomes and clearly identify and mollify risk vectors.



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 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
ActioNet	Not In	Not In	Not In	Contender	Product Challenger	Contender
AT&T Cybersecurity	Not In	Not In	Not In	Contender	Contender	Product Challenger
Avatier	Product Challenger	Not In	Not In	Not In	Not In	Not In
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Product Challenger	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Contender	Not In	Not In	Not In	Not In
BlackBerry	Not In	Contender	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader





Provider Positioning

Page 2 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Market Challenger	Market Challenger	Contender
Check Point Software	Not In	Product Challenger	Not In	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Market Challenger
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader





Provider Positioning

Page 3 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
DXC Technology	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In
Eviden	Product Challenger	Not In	Not In	Product Challenger	Leader	Product Challenger
EY	Not In	Not In	Not In	Leader	Leader	Leader
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In
Fortinet	Contender	Leader	Product Challenger	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Contender	Contender	Contender
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Rising Star ★	Leader	Leader





	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
HPE (Aruba)	Not In	Not In	Contender	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Leader	Leader	Leader
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Product Challenger	Leader	Leader
Kroll	Not In	Not In	Not In	Not In	Contender	Not In
Kudelski Security	Not In	Not In	Not In	Contender	Contender	Not In
Kyndryl	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In
Leidos	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger





Provider Positioning

Page 5 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Lookout	Not In	Not In	Contender	Not In	Not In	Not In
Lumen Technologies	Not In	Not In	Not In	Not In	Not In	Contender
ManageEngine	Leader	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In
Nok Nok Labs	Market Challenger	Not In	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Okta	Leader	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In





Provider Positioning

Page 6 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
OpenText	Product Challenger	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In
Perimeter 81	Not In	Not In	Market Challenger	Not In	Not In	Not In
Ping Identity	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In
Saviynt	Product Challenger	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Product Challenger	Not In	Not In	Not In	Not In





Provider Positioning

Page 7 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Rising Star ★	Not In	Not In	Not In
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Rising Star ★
Tech Mahindra	Not In	Not In	Not In	Contender	Contender	Product Challenger
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In
Thales	Market Challenger	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Rising Star ★	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In





Provider Positioning

Page 8 of 8

	Identity and Access Management	Extended Detection and Response	Security Service Edge	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Trustwave	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
Unisys	Not In	Not In	Not In	Leader	Market Challenger	Market Challenger
Verizon Business	Not In	Not In	Not In	Leader	Market Challenger	Leader
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Rising Star ★	Product Challenger
Zensar Technologies	Not In	Not In	Not In	Contender	Not In	Not In
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In



Key focus areas for the Cybersecurity – Solutions and Services 2024.

Simplified Illustration Source: ISG 2024



Definition

Cybersecurity in the Age of AI

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

In this ISG Provider Lens™ quadrant report, ISG covers the following six quadrants for services/solutions: Identity and Access Management, Technical Security Services, Strategic Security Services, Managed Security Services - SOC, vendors offering Security Service Edge, Extended Detection and Response solutions are analysed and positioned from a global perspective rather than individual regions, as the market is still in its early stages and yet to mature.

The ISG Provider Lens™ Cybersecurity – Solutions and Services report offers the following to business and IT decision-makers:

- Transparency on the strengths and weaknesses of relevant providers/software vendors
- A differentiated positioning of providers by segments (quadrants)
- Focus on regional market

Our study serves as an important decision-making basis for positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current 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:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).





Provider Classifications: Quadrant Key

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

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.





Technical Security Services

Technical Security Services

Who Should Read This Section

US Public sector enterprises should prioritize reading this report due to its relevance in evaluating technical security service (TSS) providers specializing in implementing and integrating security solutions. With the increasing complexity of security threats, government and federal agencies need to assess TSS providers adept at integrating solutions from multiple vendors alongside their proprietary products.

Adoption trends within the US Public sector indicate a growing reliance on TSS providers to bolster their security posture. These agencies require comprehensive solutions that can address diverse security challenges while integrating seamlessly with existing infrastructure. TSS providers play a crucial role in meeting these needs by offering tailored services that leverage a combination of proprietary and third-party solutions.

By understanding the current market positioning of TSS providers, US Public sector enterprises can make informed decisions about their security investments. The report highlights

each provider's approach to addressing key security challenges, enabling agencies to identify vendors that align with their specific requirements and objectives.

Furthermore, TSS providers serve US Public sector enterprises by offering expertise in integrating security products and solutions. They help agencies navigate the complexities of modern security environments by designing and implementing robust security architectures tailored to their unique needs. Additionally, TSS providers offer ongoing support and maintenance to ensure the effectiveness of implemented solutions.

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.



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



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

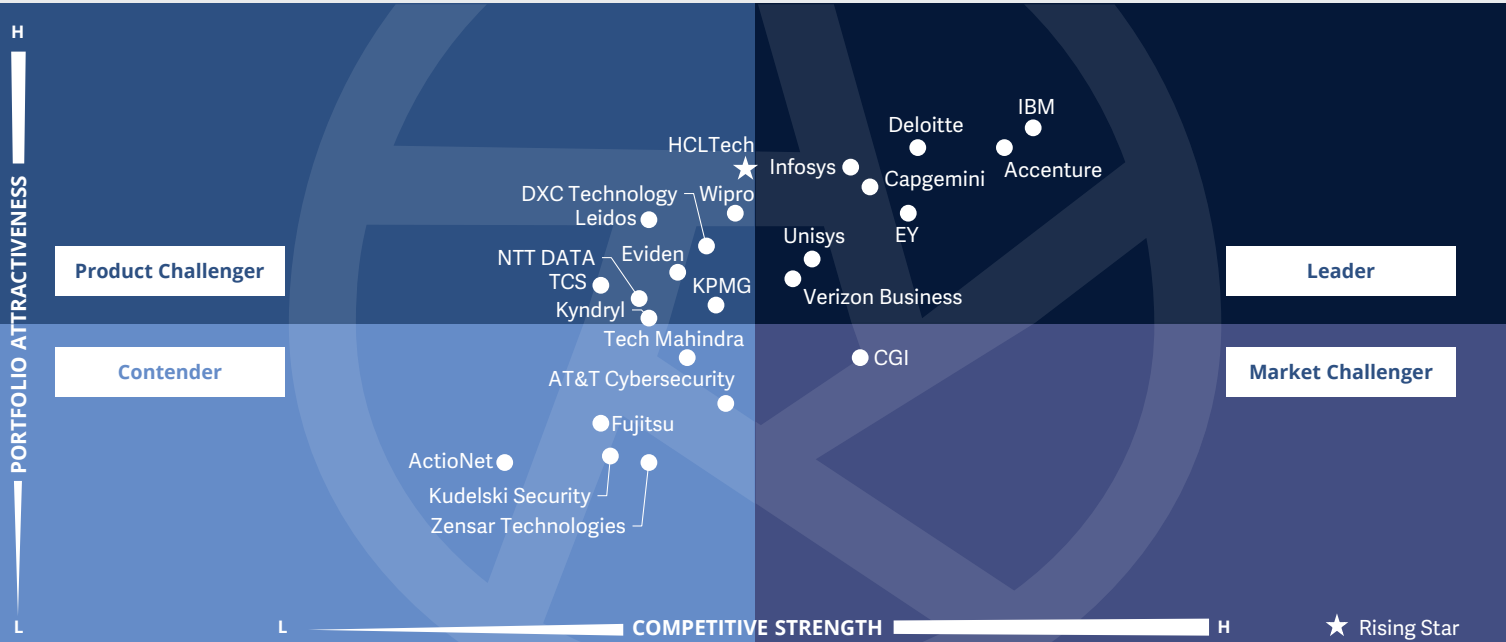


Business professionals should read this report to balance data security, customer experience and privacy amidst digital transformation at the forefront of businesses today.



Cybersecurity – Solutions and Services
Technical Security Services

U.S. Public Sector 2024



This quadrant assesses **technical security** service (TSS) providers that offer **integration, maintenance and support** services for IT security products or solutions; it requires a depth of integration of a range of products to maximize client outcomes.

Phil Hassey



Technical Security Services

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 roadmaps that aid in transforming an existing security environment with best-of-breed tools and technologies, improving security posture and reducing threat impact. Their portfolios are designed to enable 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 managed security services 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

Observations

The overall security posture for U.S. government agencies has changed in recent years. As is constantly highlighted throughout the report, threats are becoming more significant, consequences more profound and the ability of enterprises or government agencies to manage them is reduced further. As a result, a government or higher education institute at every level is only as strong as its weakest link. Unfortunately, the distributed nature of the U.S. public sector means that there are many links that could be improved. This is where the growth in TSS services is aligned. Budgets are tight, and skills are hard to find; thus, the evolution of TSS and security services to more of an automation focus with an alignment to risk and compliance is critical.

This alignment to automation and risk is also apparent among the vendors included in the leadership for this grid. While the traditional SIs are primarily present, the Big 4 audit firms contribute to the market through their security push and alignment with GRC.

Security solutions are overwhelming. They are among the few technologies or business markets that are fragmented. As a result, they have inbuilt integration challenges and overall skill access issues, regardless of the services model deployed. The key providers must assure that agencies have the necessary skills and that the specific requirements of the U.S. public sector can be met.

From the 47 companies assessed for this study, 24 qualified for this quadrant, with eight being Leaders and a Rising Star.

accenture

Accenture has the combination of scale, partnerships and processes to provide clients with a differentiated capability for TSS solutions.

Capgemini

Capgemini excels in delivering disciplined outcomes for clients' investments in cybersecurity, both strategically and technically, ensuring their resources are maximized and risks are minimized.

Deloitte.

Deloitte strategically utilizes its many acquisitions, bolstering the technical capability necessary to offer top-tier solutions for clients in the TSS space. It also harnesses the power of key partnerships, further enhancing its offerings.

EY

EY provides services to clients that are focused on risk. Security is a vital aspect of the portfolio for these solutions, enabling it to provide increased depth to clients.

IBM

IBM offers a comprehensive range of services and software solutions to clients. It has a long history of providing services to U.S. public sector organizations.

Infosys

Infosys, with its substantial investments in recent years, has been able to develop security solutions and strengthen its presence in the U.S. public sector. This growth trajectory positions TSS as a sweet spot for the company.



Technical Security Services



Unisys is a long-term TSS provider for U.S. public sector clients. It has maintained a strong presence in the market by consistently delivering services that meet clients' goals and business objectives.

Verizon Business

Verizon Business provides TSS solutions that can connect security and network requirements. The company can leverage its strong history of providing thought leadership for the security market.



HCLTech (Rising Star) is increasingly leveraging a range of security capabilities to ensure clients have access to innovative and reliable solutions.



Unisys



“Unisys has a clear legacy of providing secure cyber-aligned business outcomes for clients in the U.S. public sector.”

Phil Hassey

Overview

Unisys is headquartered in Pennsylvania, U.S., and has more than 16,200 employees across 57 offices in 27 countries. In FY23, the company generated \$2.0 billion in revenue, with Enterprise Computing Solutions as its largest segment. The public sector is one of Unisys’s key industry focus areas globally, particularly in the U.S., where it has a deep history of capability across hardware, software and services in security and other technology domains.

Strengths

Extensive engagement in public sector operations: Unisys is involved in practically every aspect of state and municipal government operations. Transportation, justice, human services, administration and financial organizations are the primary domains that Unisys serves.

Advancement through AI investments: Unisys has undertaken various AI-related investments to drive customer outcomes. These include secure digital bill of material (DBoM) technology for safe, policy-based sharing of vulnerability data, lifecycle management and authenticity, as continuous monitoring and threat exposure management with threat prediction and vulnerability through anomaly detection.


Tailored accelerators for critical challenges:

Unisys has developed a broad accelerator portfolio to meet clients’ security requirements. These accelerators align with the client’s technology portfolio. From a foundational security perspective, it has developed accelerators that address critical challenges for agencies, such as zero trust assessment, methodology and architecture; Attack Surface Discovery framework and assessment; Cyber Recovery reference architecture; and XDR and DIAM Platform engineering design and ecosystem extensions.

Caution

Unisys has never disappeared from clients’ radar, but it needs to aggressively highlight the strength of its offerings in cybersecurity; otherwise, its visibility will not grow enough to meet the potential market opportunity.





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.

Customer Experience (CX) Insights

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

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

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

Client Business Role

- ▲ **Most satisfied**
Information Technology
- ▼ **Least satisfied**
Human Resources

Region

- ▲ **Most satisfied**
Africa
- ▼ **Least satisfied**
Eastern Europe

Industry

- ▲ **Most satisfied**
Chemicals
- ▼ **Least satisfied**
Public sector

Industry Average CX Score



- ▲ Highest CX: 91.0
- ▼ Lowest CX: 64.8

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

Most Important CX Pillar

Execution and Delivery

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





Appendix

The ISG Provider Lens 2024 – Cybersecurity – Solutions and Services research study analyzes the relevant software vendors/service providers in the U.S. PS, Global markets, 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:

Phil Hassey, Gowtham Sampath and Dr. Maxime Martelli

Editor:

Ananya Mukherjee

Research Analyst:

Monica K

Data Analysts:

Rajesh Chillappagari and Laxmi Sahebrao

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

Phil Hassey
Strategic Advisory Analyst

Phil has an enviable reputation for understanding, assessing and communicating insight into the increasingly diverse and complex technology sector as it attempts to tightly integrate to business requirements. He is constantly “tilting the world view” with unique but grounded perspectives for clients.

He has worked for some of the largest, and smallest enterprises in the world to help them understand the role of the intersection of technology and business. At the same time he has also worked with technology and business providers to help ensure they place the customer requirements at the centre of their business.

He has undertaken research and strategy projects on every continent, and for every possible application of technology and business.



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 & Editor Biographies

Author



Dr. Maxime Martelli
Consulting Manager

Dr. 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 Specialis

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.



Author & Editor Biographies



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