

Cybersecurity – Solutions and Services

Managed Security Services - SOC

A research report comparing provider strengths,
challenges, and competitive differentiators

Customized report courtesy of:



Executive Summary	03	Managed Security Services - SOC	17 – 23
Provider Positioning	06	Who Should Read This Section	18
Introduction		Quadrant	19
Definition	14	Definition & Eligibility Criteria	20
Scope of Report	15	Observations	21
Provider Classifications	16	Provider Profile	23
Appendix			
Methodology & Team	25		
Author & Editor Biographies	26		
About Our Company & Research	29		

Report Author: Phil Hassey

The U.S public sector needs to have proactive management to handle cyber threats

Research by Comparitech shows that the total cost of data breaches faced by the U.S. government in 2022 was \$26 billion. This amount could have been spent on education, healthcare, defense or justice if cyberattacks were managed well. The research shows that such attacks impact approximately two-thirds of U.S. citizens. The downtime for a breach in local government was five months. In terms of the attack targets, the top five states are Texas, Georgia, California, Florida and Pennsylvania.

The cost and impact of cyberattacks are increasing in both public and private sectors globally. Hence, the U.S. government is increasing its focus on effectively managing cybersecurity issues. However, legislative and regulatory responses to such threats must be accelerated.

Federal government issues are crucial; the U.S. federal government is the most prominent target globally for apparent reasons. Despite having a low profile, state, local and education (SLED) agencies are still threat targets.

As a result of this, stakeholder education, investment and capability need to improve. ISG has identified successful examples of agencies leveraging a broad range of provider solutions targeting the sector. Some providers can offer a wide scope of product and service-based solutions, while others have narrower but specific capabilities. Nevertheless, they all play a part in providing solution portfolios to be integrated by clients.

Apart from the apparent threat issues, a broad set of technology and provider trends impact the market's characteristics.

Government agencies continue investing in cloud solutions across their application, infrastructure and business requirements. As a result, there is an increased need for robust and consistent cloud security measures to prevent data from being accessed by the wrong party.

Leveraging AI-based tools is driving the successful response to security threats



Executive Summary

Cloud providers are increasingly engaged in this, with integrated offerings from significant hyperscalers becoming increasingly visible with each release. This will only continue as agencies and their enterprise counterparts realize where the responsibility lies for security, data backup and recovery.

In volume, 2022 saw a reduction in ransomware attacks bucking a growing trend. However, they remain a major threat. Ransomware attacks are increasingly sophisticated, posing an ongoing and significant threat to public sector organizations. This has increased investment in ransomware protection measures, such as data backup and recovery strategies. It has also led to legislative changes, with states including North Carolina and Florida introducing legislation that banned government entities' payment of ransom money.

External ransomware attacks, state-based hacking and other high-profile issues sometimes gain attention; the always underrated security threat is from within. In some cases, this activity is nefarious, and in other instances, it is just a user error resulting from ignorance, poor training or simple carelessness. It still presents

significant issues, so there is an increased role for training, access control development and consistency, along with monitoring capabilities. It is worth noting the connection between technology security and physical security. Agencies that leave doors unlocked and do not manage access passes are likelier to be vulnerable in their technology security. This is due to the simple fact that attitude toward security is critical. Any lax approaches in either realm will inevitably spill over.

AI has become a high-profile application of technology. This has built up over several years, but from the consumer or employer perspective, the actual use of AI has become fundamental in consumer tools such as our suggested viewing on Netflix, listening on Spotify, and shopping on Amazon. ChatGPT has burst out of the blocks, making generative AI the buzzword of 2023 to date, with substantial uncertainty over the technology's positive benefits and adverse outcomes. From a security point of view, AI and ML are central in applications across the spectrum of technology and security requirements. It is most pertinent in datasets with strongly structured data levels;

hence, threat protection is paramount. Many vendors are building out capabilities, and it is reasonable to assume that these will quickly become attractive to government agencies in the U.S. and globally.

We have identified that zero trust is becoming a fundamental approach for agencies and more than a perimeter-based approach is needed. This is a complex migration for some, particularly in a world of diverse devices mixed between the company and privately owned. Still, it is essential, and strong identity management tools help enable the IAM tools to be a mechanism for zero-trust.

Ownership of security within the government agency is a real challenge. Each agency has a different structure depending on its services, location, size and scale, but the bottom line is that the head of the agency or university must consider investments and outcomes of cybersecurity under their range of responsibilities. A chief information security officer (CISO), if they exist, cannot operate in isolation. Some agencies and their private sector counterparts risk delineating data between internal and external (or customer)

data. Cybersecurity risks are too high to have this fragmented approach. Training requirements must be prioritized more explicitly across all levels of the organization; as highlighted, humans are the source of error on so many occasions.

From the vendor perspective, every year is different for security. 2023 is continuing in this vein. XDR and other technologies, such as IAM, are rapidly evolving, and cloud-based and edge/IoT-based tools are accelerating. As highlighted, this growth comes from prominent established vendors, well-funded start-ups and services companies. Consolidation continues to happen across all offerings. Some service companies consider acquiring product companies to boost engagement and capabilities, while others seek to broaden services. In some respects, the U.S. government is not directly involved, as accessing the enterprise client base is the primary acquisition driver. However, it is still relevant, and activity is swirling around government-focused solutions and service providers.



For government buyers of security technology, there are three key takeaways.

1. Education and employee awareness of the holistic requirements for security, from locking the front door to adhering to password protocols, must be met.
2. Investment in solutions driven by analytics, AI and ML at the core to improve threat detection and risk management.
3. Leadership from the highest level of the agency down to the newest employee has to be embedded. Leaders must prioritize the issue and invest appropriately, and all employees must understand their role in keeping their agency or institution safe.

The U.S. public sector is a prime global target for bad actors in the cybersecurity space. A response to this threat requires an integrated approach across a range of cutting-edge technology products and solutions to ensure that citizens, government and businesses can be assured that their data is safe.



Provider Positioning

Page 1 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	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
AWS	Market Challenger	Market Challenger	Not In	Not In	Not In	Not In
Beta Systems	Contender	Not In	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
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger



Provider Positioning

Page 2 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Check Point	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
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
DXC Technology	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Elastic Security	Not In	Contender	Not In	Not In	Not In	Not In
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In




Provider Positioning

Page 3 of 8


	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
eSentire	Not In	Contender	Not In	Not In	Not In	Not In
Eviden (Atos)	Leader	Not In	Not In	Leader	Leader	Product Challenger
EY	Not In	Not In	Not In	Leader	Leader	Leader
Fidelis Cybersecurity	Not In	Product Challenger	Not In	Not In	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortinet	Market Challenger	Leader	Product Challenger	Not In	Not In	Not In
Fortra	Contender	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Contender	Contender
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In



 Provider Positioning


	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Hashicorp	Market Challenger	Not In	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Product Challenger	Leader	Leader
HPE (Aruba)	Not In	Not In	Rising Star ★	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
Infinite Networks	Not In	Not In	Contender	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Leader	Leader	Leader
KPMG	Not In	Not In	Not In	Product Challenger	Leader	Rising Star ★
Kudelski Security	Not In	Not In	Not In	Contender	Contender	Not In
Leidos	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger



 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Lookout	Not In	Not In	Contender	Not In	Not In	Not In
ManageEngine	Leader	Contender	Not In	Not In	Not In	Not In
Mandiant	Not In	Contender	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Not In	Not In	Not In	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In
NetWitness	Not In	Product Challenger	Not In	Not In	Not In	Not In
Nok Nok Labs	Contender	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



 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In
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	Contender	Not In	Not In	Not In
Ping Identity	Product Challenger	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	Rising Star ★	Not In	Not In	Not In	Not In	Not In




Provider Positioning

Page 7 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Secureworks	Not In	Leader	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In
SilverSky	Not In	Contender	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	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	Product Challenger
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Contender	Product Challenger
Trellix	Not In	Product Challenger	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger



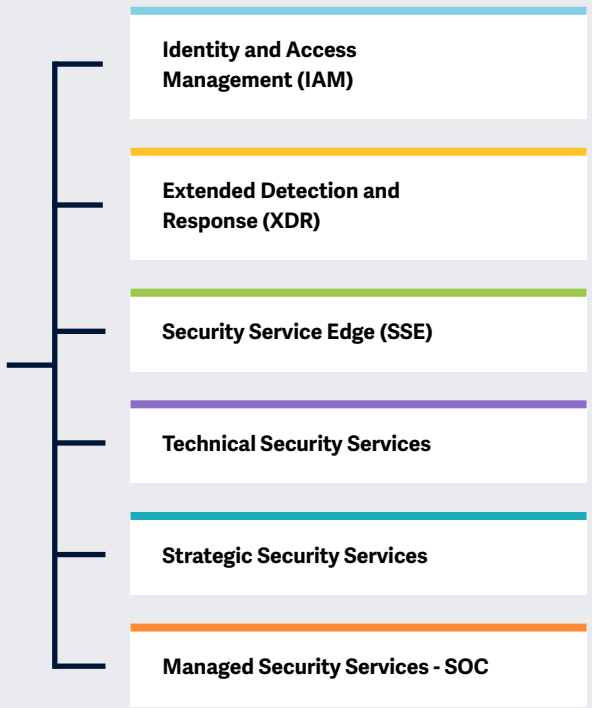
 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Unisys	Not In	Not In	Not In	Leader	Market Challenger	Leader
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
VMware	Not In	Leader	Contender	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Rising Star ★	Product Challenger	Product Challenger
Zensar	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 Cybersecurity Solutions and Services 2023

Simplified Illustration; Source: ISG 2023



Definition

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritized relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

From an enterprise perspective, even small businesses understood the impact of cyber threats and realized that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident. Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of the cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

These prompted businesses to invest in capabilities such as identity and access management (IAM), managed detection and response (MDR) and securing cloud and endpoints. The market is shifting toward integrated solutions, such as extended detection and response (XDR), which leverage the best tools and human expertise and are augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.



Scope of the Report

In this ISG Provider Lens™ quadrant report, ISG covers the following 6 (number of quadrants) quadrants for services/solutions: Identity and Access Management (IAM), Extended Detection and Response (XDR), Security Service Edge (SSE), Technical Security Services, Strategic Security Services, and Managed Security Services - SOC.

Vendors offering Security Service Edge (SSE) solutions are analyzed and positioned from a global perspective, rather than by individual regions, as the market is yet in the early stages of maturity.

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

- Transparency on the strengths and weaknesses of relevant providers/software vendors
- A differentiated positioning of providers by segments (quadrants)
- Focus on the U.S. public sector market

Our study serves as the basis for important decision-making in terms of positioning, key relationships, and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing vendor relationships and potential engagements.

Provider Classifications

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

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

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

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).





Provider Classifications: Quadrant Key

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

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.





Managed Security Services - SOC

Who Should Read This Section

This report is relevant to the U.S. public sector enterprises across industries for evaluating service providers specializing in managed security services (MSS), thereby helping enterprises combat security threats. It also provides insights into how each provider addresses critical market challenges.

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

In the U.S. public sector, MSS have emerged as a key strategy to meet the increasing cybersecurity needs and keep pace with the ever-evolving threat landscape. These services allow federal and state agencies to leverage the expertise of providers with specialized skills and resources to deal with sophisticated attacks. Providers strategically invest in cybersecurity services to expand and strengthen their MSS portfolios. Enterprises increasingly demand cloud-native security solutions and SaaS platforms to improve their overall security

posture. Additionally, an increased focus is on enhancing SOC's managed detection and response (MDR) capabilities and using incident response (IR) retainers to increase resiliency. SOC's MDR capabilities offer continuous monitoring, threat detection and response services. In contrast, IR retainers ensure that agencies have immediate access to expert assistance in the event of a cybersecurity incident and are better prepared to respond quickly and effectively to a security breach. Such security measures help minimize the impact of the incident and reduce the risk of data loss or theft. The integration of threat intelligence with endpoint protection and security management automation is also gaining momentum.



Cybersecurity professionals should read this report to understand the emerging trends and immediate threats to aid their strategic decision-making, enhance productivity and reduce security complexity.

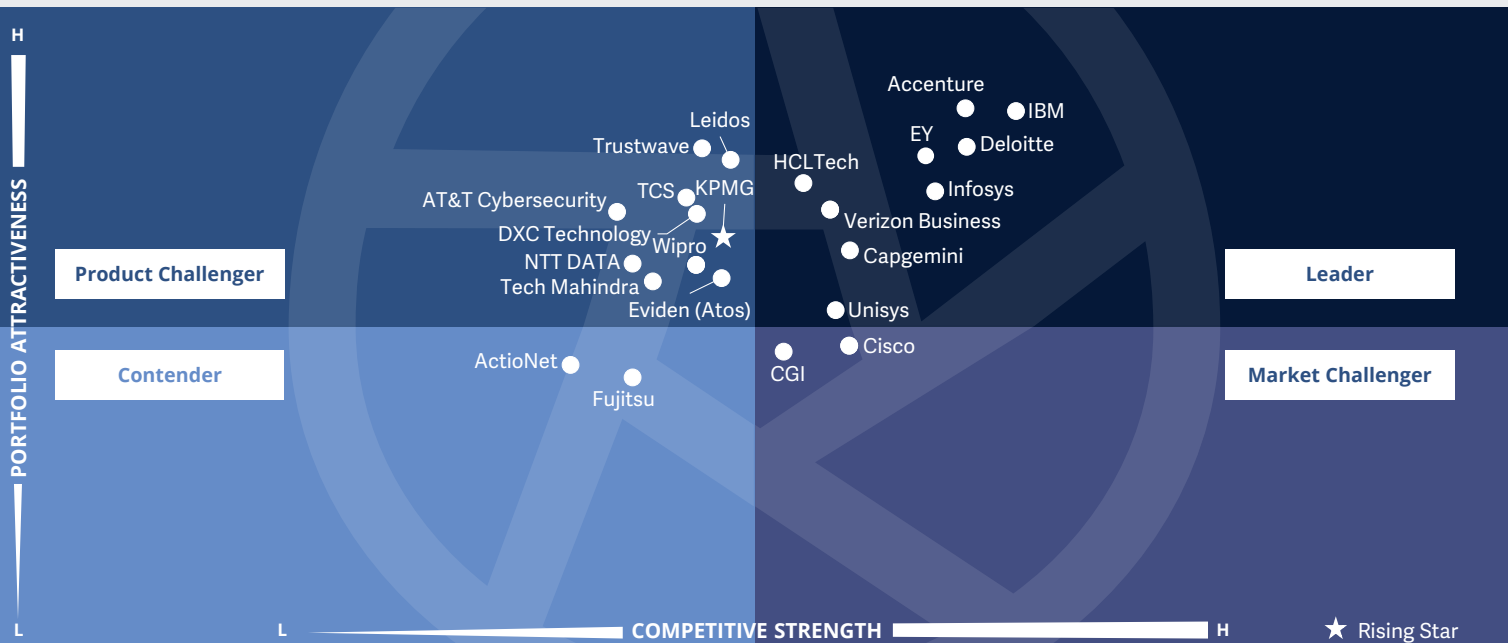


Technology professionals should read this report to keep pace with the changing security landscape, as it provides insights on emerging trends, tailored security platforms and strategic objectives.



Business professionals should read this report to gain valuable insights on simplifying security operations. It also offers practical solutions to reduce complexity and enhance efficiency.





Managed security services (MSS) bind together complex and sustainable cybersecurity over time. Government agencies will need help in efficiently selecting and managing changing combinations of technologies, tools, software and services.

Phil Hassey



Managed Security Services - SOC

Definition

The providers assessed in the Managed Security Services – SOC (MSS – SOC) quadrant offer services related to the operations and management of IT and OT security infrastructures for one or several customers by a security operations center (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, from identification to resolution.

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximizing the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS (SOC) providers must combine traditional managed security services with innovation to fortify their clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies, infrastructure, and experts skilled in threat

hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI, and machine learning. These sophisticated SOCs should support expert-driven security intelligence response, while offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, identity, and access management (IAM) operation services, data leakage/loss prevention (DLP) operations** and all other operating services to provide ongoing, real-time protection, without compromising on business performance. In particular, secure access service edge (SASE) is included
2. Ability to provide security services, such as **detection and prevention; security information and event management (SIEM)** and security advisor and auditing support, remotely or at a client's site
3. Possesses **accreditations** from security tools vendors
4. SOCs ideally owned and managed by the provider and not predominantly by partners
5. Maintains **certified staff**, for example with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)



Observations

While overall managed services are not new for the public sector, it has been limited in the market due to restrictions that are in place in some jurisdictions. In the current economic and political environment, a new approach for the U.S. public sector has emerged with budget limitations and increased private enterprise-based service delivery. At the same time, as highlighted repeatedly, the security threats faced by agencies at all government levels, are only increasing, and for some, the sector can provide a potential vulnerability.

As we work with public sector clients, ISG sees the following key MSS needs recurring:

- Threat management: Like any other organization, public sector entities need protection from vulnerabilities; detection and management of threats; and mitigation.
- Security transformation assistance: As digital changes outside of public sector agencies force them to consider their digital transformation, most require assistance with transforming IT security capabilities and management.

- An extended team adaptive approach: Most public sector entities will require significant investment by their provider partners in services that augment, complement and extend the entity's own environment and staff. Adaptable services and contracting will become standard expectations among public sector buyers.
- Scoped, scalable managed security: Providers will be expected to offer a broad scope of services that can be scaled in size and complexity as clients learn their capabilities and needs.
- Leverage emerging technology: Security technology is changing daily with innovation. At the same time, cloud, IoT, AI and other mechanisms are changing the way in which technology is used. As a result, MSS providers need to ensure that their solutions are equally on the cutting edge.

From the 261 companies assessed for this study, 23 have qualified for this quadrant with nine being Leaders and one Rising Star.

accenture

Accenture has a strong presence in the U.S. federal government and is increasingly investing in state and local agencies, along with educational institutions. It has a rich history of offering a comprehensive range of managed services across the technology spectrum, and security is no exception.

Capgemini

Capgemini's MSS offerings include client-centric, sector-specific requirements, risk profiles, critical data assets, and current security strategies and levels of protection. The services are delivered on-premises, offshore or via a hybrid delivery model.

Deloitte.

Deloitte has strong capabilities in the MSS space. It made major acquisitions in 2022 to expand its available services. It also drives client engagement through a focus on the end-to-end business processes.

EY

EY is relatively new to the MSS space. It is, however, backed by a rich legacy of solutions for enterprise clients and government agencies in the security space. This strong programmatic capability enables it to be a leader in the space.

HCLTech

HCLTech is an established provider of MSS for clients globally across a range of technology areas. It focuses on expanding its offerings and increasing investments in the state and federal government.

IBM effectively invented managed services and outsourcing, thereby gaining a leadership position in this space. With its proprietary offerings and third-party products, it can offer a strong portfolio of solutions.



Managed Security Services - SOC



Infosys has a full suite of security-related offerings for clients. Managed services are part of an ongoing cycled approach of design, run and optimize, backed by a broad range of partners and are part of an innovative ecosystem.



Unisys has established itself in the market with its long heritage of offering managed services to government agencies. The success of this offering for clients is increasingly being measured in terms of business outcomes.



Verizon Business has access to the largest network in the U.S., which is fundamental to its cybersecurity offerings for the public sector entities. With thought leadership and dedicated teams, it provides managed services to clients.



KPMG (Rising Star) is relatively new to the MSS space. It leverages its capabilities in the adjacent ecosystems, along with its overall cyber experience, to strengthen its MSS offerings.





“Unisys is a credible and reliable provider of MSS solutions for clients in the U.S. public sector, making it a leader in this space.”

Phil Hassey

Unisys

Overview

Unisys is headquartered in Pennsylvania, U.S. and operates in 28 countries. It has more than 16,200 employees across 71 global offices. In FY22 the company generated \$2.0 billion in revenue, with Enterprise Computing Solutions as its largest segment. The public sector is one of the key industry focus areas for Unisys globally, but particularly in the U.S., where it has a deep history of providing hardware, software and services in security and other technology domains.

Strengths

Deep and broad public sector roots and presence:

Unisys is involved in practically every aspect of state and municipal government operations. Primary domains served by Unisys include transportation, justice, human services and administration, including financial organizations.

Strong partnerships for advanced solutions:

Through the partnership with Cylance, Unisys provides a platform for advanced endpoint protection using AI and ML. It also leverages LogRhythm’s SIEM technology for cross-platform, enterprise-wide monitoring, and detection and response.

SDM solution: Designed to manage and optimize security technology infrastructures, Unisys’ SDM manages edge, mobile and traditional on-premises device security, and data compliance issues via its network of global delivery centers provide a set of flexible support options based on client needs.

Solid MSS portfolio: Unisys’ MSS portfolio includes advanced endpoint protection services, SIEM and security device management (SDM). The company offers unified services supporting on-premises and multicloud environments.

Caution

Unisys needs to ensure that it continuously offers cutting-edge MSS solutions. Innovation has arguably slowed since the launch of Stealth; hence, it needs to ensure that the market is aware of its new offerings and innovation.





Appendix

The ISG Provider Lens™ 2023 – Cybersecurity – Solutions and Services report 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.

Lead Author:

Phil Hassey

Editor:

Sajina B

Research Analyst:

Bhuvaneshwari Mohan

Data Analysts:

Rajesh Chillappagari and Shilpashree N

Consultant Advisor:

Alex Perry

Project Manager:

Donston Sharwin

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research™ programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of April 2023, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars (\$US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Solutions and Services market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
 - * Strategy & vision
 - * Tech Innovation
 - * Brand awareness and presence in the market
 - * Sales and partner landscape
 - * Breadth and depth of portfolio of services offered
 - * CX and Recommendation



Author & Editor Biographies



Author

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 Kumar Sampath
Assistant Director and Principal Analyst

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients’ requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.



Author & Editor Biographies

Co-Author



Bruce Guptill
Distinguished Analyst and Executive Advisor

Bruce Guptill brings more than 30 years of technology business and markets experience and expertise to ISG clients. Bruce has helped develop and lead ISG's enterprise research development and delivery, global ISG Research operations, and Research client support. His primary research and analysis for ISG clients has focused on IT services market development, disruption, adaptation and change. He currently leads U.S. Public Sector research for ISG's Provider Lens global research studies, and also leads IPL studies in procurement and software vendor partner ecosystems.

Bruce holds a Masters' degree in Marketing and Finance, and a B.A. combining business and mass media communication psychology. He also holds certifications in a wide range of software, hardware, and networking technologies, as well as in mechanical and electrical engineering disciplines.

Research Analyst



Bhuvaneshwari Mohan
Senior Research Analyst

Bhuvaneshwari is a senior research analyst at ISG responsible for supporting and co-authoring Provider Lens™ studies on Banking, Cybersecurity, Supply Chain, ESG and Digital Transformation. She supports the lead analysts in the research process, authors the global summary report and develops content from an enterprise perspective.

Her core areas of expertise lie in Cybersecurity, Cloud & Data transformation, AI/ML, Blockchain, IoT, Intelligent Automation and Experience Engineering. She has 7 years of hands-on experience and has delivered insightful reports across verticals.

She is a versatile research professional having experience in Competitive Analysis, Social Media Analytics, Glassdoor Analysis and Talent Intelligence. Prior to ISG, she held research positions with IT & Digital Service Providers and was predominantly part of Sales Enablement teams.





IPL Product Owner

Jan Erik Aase
Partner and Global Head – ISG Provider Lens™

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

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



ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens™ research, please visit this [webpage](#).

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: [Public Sector](#).

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.





JUNE, 2023

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES