

# Cybersecurity – Services and Solutions

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



Introduction	3	Contacts for this Study	13
About the Study		Advisor Involvement	
Quadrants Research	4	Advisor Involvement - Program	
Definition	5	Description	14
Quadrants by Regions	8	Advisory Team	14
ISG's Cybersecurity Framework	9		
Schedule	10	Invited Companies	16
Client Feedback		About our Company & Research	17
Nominations	11		
Methodology & Team	12		

### AI — Vanguard and Vulnerability of U.S. Public Sector Cybersecurity

In the U.S. public sector, AI is rapidly transforming cybersecurity, emerging as a powerful defense tool and a threat amplifier. As government institutions integrate AI to enhance operations, they face a dual challenge — using AI to fortify cybersecurity and mitigating the risks posed by its exploitation in cyberattacks.

The breach of National Public Data exposed the sensitive information of nearly 3 billion records, while ransomware attacks compromised the health data of over 3 million Medicare beneficiaries. Legislative efforts such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), advancements in the U.S. National Cybersecurity Strategy and the 2024 executive order to bolster cybersecurity at U.S. ports underscore the urgency of safeguarding vital systems.

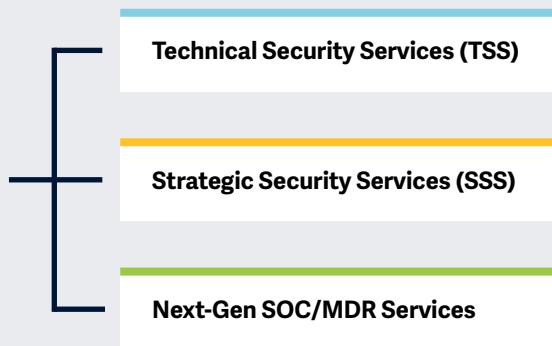
Public institutions must embrace *strategic security* consulting and robust cybersecurity architectures to navigate AI-driven risks. With AI-powered tools, cybercriminals exploit vulnerabilities in critical infrastructure, orchestrating targeted attacks that disrupt operations and compromise national security. This situation highlights the need for *advanced technical security services* to deploy resilient, compliant and scalable defenses tailored to the unique requirements of public institutions.

AI's role as a proactive defender is transformative, with *next-gen SOC and MDR* services powered by AI and ML redefining threat detection, response and mitigation. However, these solutions must evolve to counteract AI-driven adversarial tactics, including deepfake phishing, algorithmic manipulation and autonomous attack models.



## Key focus areas for Cybersecurity – Services and Solutions 2025.

Simplified Illustration Source: ISG 2025



### The ISG Provider Lens™ Cybersecurity — Services and Solutions study offers the following to business and IT decision-makers:

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on the U.S. public sector

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.



## Technical Security Services (TSS)

### Definition

TSS providers assessed in this quadrant offer integration, maintenance and support for IT/OT security solutions. They address diverse security domains, including cloud security, identity and access management (IAM), data loss prevention (DLP), network security, endpoint security, OT security and secure access service edge (SASE), while adhering to regulations, such as FedRAMP, FISMA, GDPR and CJIS, and certifications such as ISO 27001, CMMC and SOC 2.

These providers prioritize government standards and specialized accreditations, enabling the development of security architectures tailored to address public sector challenges. They enhance security environments with playbooks, road maps and optimal tools, ensuring compliance, improved posture and threat reduction. They offer end-to-end services, including security product assessment, design, implementation and transformation, while supporting interoperable and secure operations for critical public services.

The quadrant also includes managed security services without a security operation center (SOC) and evaluates providers' ability to integrate multivendor solutions.

### Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for U.S. public sector entities
2. **Have authority granted by security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** capable of supporting security technologies (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies)
4. **Obtain FedRAMP authorization** to ensure ongoing compliance with security standards and
5. **Comply with and report cyber incidents** promptly to federal agencies such as the Cybersecurity and Infrastructure Security Agency (**CISA**) and share relevant threat information
6. Obtain **additional certifications as necessary** such as Gramm-Leach-Bliley Act (**GLBA**), Criminal Justice Information Services (CJIS), **CMMC** and **GDPR** for cross-border business



## Strategic Security Services (SSS)

### Definition

SSS providers assessed in this quadrant offer IT/OT security consulting. Services include security audits, assessments, and awareness and training aligned with stringent regulatory requirements such as FISMA, FedRAMP, GDPR (for cross-border agencies) and CJIS. These providers also help assess security maturity, define cybersecurity strategies, develop business continuity road maps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to meet the critical operational and compliance needs of public entities.

They employ seasoned consultants with expertise in planning and managing end-to-end security programs, including on-demand expertise for guidance such as virtual CISO (vCISO) services. These providers assist agencies in selecting and evaluating security technologies and vendors while ensuring compatibility with public sector frameworks.

This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.

### Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Display **competence** in the application of **best practices** and market **security frameworks** such as ISO 27000, NIST and CIS
3. **Offer at least one of the above** SSS to U.S. public sector organizations
4. Offer **security consulting services using frameworks**
5. **Obtain FedRAMP authorization** to ensure ongoing compliance with security standards and
6. **Comply with and report cyber incidents** promptly to federal agencies such as the Cybersecurity and Infrastructure Security Agency (**CISA**) and share relevant threat information
7. Obtain **additional certifications as necessary** such as Gramm-Leach-Bliley Act (GLBA), Criminal Justice Information Services (**CJIS**), **CMMC** and **GDPR** for cross-border business



## Next-Gen SOC/MDR Services

### Definition

Service providers in this quadrant deliver continuous monitoring of IT/OT infrastructures through security operations centers (SOCs) designed specifically to meet the unique requirements of public sector agencies. These providers ensure compliance with stringent regulations such as FedRAMP, FISMA, GDPR (for cross-border agencies) and CJIS while adhering to essential certifications, including NIST, ISO 27001 and SOC 2. They specialize in managing and operating optimal security tools and overseeing the entire security incident lifecycle, from detection to response and remediation.

Next-gen SOC providers invest in cutting-edge technologies to deliver advanced managed detection and response (MDR) services, tailored to address the operational challenges of public agencies. These providers invest in capabilities such as threat detection, hunting, intelligence, forensic analysis and incident management, ensuring a proactive and comprehensive approach to mitigating threats.

### Eligibility Criteria

1. Offer standard services, including **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services, to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as **prevention and detection, security information and event management (SIEM)**, security advisory and auditing support, either remotely or at clients' site
3. Demonstrate MDR-specific capabilities, including **advanced threat intelligence and behavior-based and human-led threat hunting** to deliver **offensive and defensive** security capabilities with a **unified view** for reporting and metrics
4. Maintain **staff with** certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
5. Possess **accreditations** from security tool vendors and **federal agencies**
6. **Manage own SOC**s
7. Offer a variety of tiered pricing models



## Quadrants by Region

As a part of this ISG Provider Lens™ quadrant study, we are introducing the following three quadrants on Cybersecurity — Services and Solutions 2025:

Quadrant	U.S. Public Sector
Technical Security Services (TSS)	✓
Strategic Security Services (SSS)	✓
Next-Gen SOC/MDR Services	✓





# ISG's Cybersecurity Framework

## Key characteristics of the proprietary framework:

- Encapsulates what enterprises are doing across the cybersecurity market and helps connect them to digital solutions
- Represents the entire value chain of supply and demand within the market
- Inner tiles represent themes of enterprise objectives
- Outer tiles represent initiatives
- Behind each outer tile is a specific set of capabilities, with unique market leading providers and solutions



The research phase falls in the period between January and February 2025, during which survey, evaluation, analysis and validation will take place. The results will be presented to the media in July 2025.

Milestones	Beginning	End
Survey Launch	January 7, 2025	
Survey Phase	January 7, 2025	February 7, 2025
Sneak Preview	May 2025	June 2025
Press Release & Publication	July 2025	

Collecting client testimonials via the Star of Excellence Program requires early client referrals (no official reference needed) because CX scores have a direct influence on the provider’s position in the IPL quadrant and the awards.

Please refer to the [link](#) to view/download the ISG Provider Lens™ 2025 research agenda.

**Access to Online Portal**

You can view/download the questionnaire from [here](#) using the credentials you have already created or refer to the instructions in the invitation email to generate a new password. We look forward to your participation!

**Buyers Guide**

ISG Software Research, formerly “Ventana Research,” offers market insights by evaluating technology providers and products through its Buyers Guides. The findings are drawn from the research-based analysis of product and customer experience categories, ranking and rating software providers and products to help facilitate informed decision-making and selection processes for technology.

In the course of the Cybersecurity – Solutions and Services IPL launch, we want to take advantage of the opportunity to draw your attention to related research and insights that ISG Research will publish in 2025. For more information, refer to the [Buyers Guide research schedule](#).

**Research Production Disclaimer:**

ISG collects data for the purposes of conducting research and creating provider/vendor profiles. The profiles and supporting data are used by ISG advisors to make recommendations and inform their clients of the experience and qualifications of any applicable provider/vendor for outsourcing the work identified by clients. This data is collected as part of the ISG FutureSource™ process and the Candidate Provider Qualification (CPQ) process. ISG may choose to only utilize this collected data pertaining to certain countries or regions for the education and purposes of its advisors and not produce ISG Provider Lens™ reports. These decisions will be made based on the level and completeness of the information received directly from providers/vendors and the availability of experienced analysts for those countries or regions. Submitted information may also be used for individual research projects or for briefing notes that will be written by the lead analysts.



### ISG Star of Excellence™ – Call for nominations

The Star of Excellence™ is an independent recognition of excellent service delivery based on the concept of “Voice of the Customer.”

The Star of Excellence™ is a program, designed by ISG, to collect client feedback about service providers’ success in demonstrating the highest standards of client service excellence and customer centricity.

The global survey is all about services that are associated with IPL studies. In consequence, all ISG Analysts will be continuously provided with information on the customer experience of all relevant service providers. This information comes on top of existing first-hand advisor feedback that IPL leverages in context of its practitioner-led consulting approach.

Providers are invited to [nominate](#) their clients to participate. Once the nomination has been submitted, ISG sends out a mail confirmation to both sides. It is self-evident that ISG anonymizes all customer data and does not share it with third parties.

It is our vision that the Star of Excellence™ will be recognized as the leading industry recognition for client service excellence and serve as the benchmark for measuring client sentiments.

To ensure your selected clients complete the feedback for your nominated engagement please use the Client nomination section on the Star of Excellence™ [website](#).

We have set up an email where you can direct any questions or provide comments. This email will be checked daily, please allow up to 24 hours for a reply.

Here is the email address:

[star@cx.isg-one.com](mailto:star@cx.isg-one.com)



**ISG Star of Excellence**



The ISG Provider Lens 2025 – Cybersecurity – Services and Solutions research study analyzes the relevant software vendors/service providers in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

**Study Sponsor:**

Heiko Henkes

**Lead Analysts:**

Gowtham Kumar and  
Bhuvaneshwari Mohan

**Research Analyst:**

Sandya Kattimani

**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 study will include data from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. ISG recognizes the time lapse and possible market developments between research and publishing, in terms of mergers and acquisitions, and acknowledges that those changes will not reflect in the reports for this study.

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



## Contacts For This Study

### Study Sponsor



Heiko  
Henkes

Director and  
Principal Analyst



Gowtham  
Kumar

Lead Analyst -  
U.S. Public Sector



Bhuvaneshwari  
Mohan

Lead Analyst -  
U.S. Public Sector



Sandya  
Kattimani

Research  
Analyst



Rajesh  
Chillappagari

Data Analyst



Laxmi  
Sahebrao

Data Analyst



Shreemadhu  
Rai B

Project  
Manager



### ISG Provider Lens Advisors Involvement Program

ISG Provider Lens offers market assessments incorporating practitioner insights, reflecting regional focus and independent research. ISG ensures advisor involvement in each study to cover the appropriate market details aligned to the respective service lines/technology trends, service provider presence and enterprise context.

In each region, ISG has expert thought leaders and respected advisors who know the provider portfolios and offerings as well as enterprise requirements and market trends. On average, three consultant advisors participate as part of each study's quality and consistency review process.

The consultant advisors ensure each study reflects ISG advisors' experience in the field, which complements the primary and secondary research the analysts conduct. ISG advisors participate in each study as part of the consultant advisors' group and contribute at different levels depending on their availability and expertise.

The consultant advisors:

- Help define and validate quadrants and questionnaires,
- Advise on service provider inclusion, participate in briefing calls,
- Give their perspectives on service provider ratings and review report drafts.

## ISG Advisors to this study



Doug  
Saylor

**Partner, Co-lead ISG  
Cybersecurity**



David  
Gordon

**Principal Consultant  
Cybersecurity**



Anas  
Barmo

**Senior Consultant  
Cybersecurity**

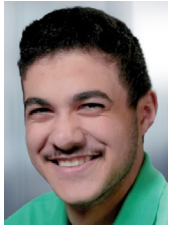


Brendan  
Prater

**Consulting Manager  
Cybersecurity**



## ISG Advisors to this study



Marco  
Ezzy

**Consultant  
Cybersecurity**



Tim  
Merscheid

**Consulting Manager  
Cybersecurity**



Christophe  
de Boisset

**Consulting Manager  
Cybersecurity**



## Invited Companies

**If your company is listed on this page or you feel your company should be listed, please contact ISG to ensure we have the correct contact person(s) to actively participate in this research.**

\* Rated in previous iteration

Accenture*	Infosys*
ActioNet*	KPMG*
AT&T Cybersecurity* (LevelBlue)	Kroll
Beta Systems*	Kudelski Security*
Booz Allen Hamilton	Leidos*
Capgemini*	NTT DATA*
CGI*	Raytheon Technologies
CyberProof	TCS*
Deloitte*	Tech Mahindra*
DXC Technology*	Trustwave*
Eviden (Atos)*	Unisys*
EY*	Verizon Business*
Fujitsu*	Wipro*
HCLTech*	Zensar*
IBM*	





### 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](mailto:contact@isg-one.com), call +1.203.454.3900, or visit [research.isg-one.com](http://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](http://isg-one.com).





**JANUARY, 2025**

---

**BROCHURE: CYBERSECURITY – SERVICES AND SOLUTIONS**