ISG Provider Lens™

Cybersecurity – Solutions and Services

A report comparing provider portfolio attractiveness and competitive strengths

BROCHURE | **JANUARY 2024** | **U.S. PUBLIC SECTOR**

Table of Contents

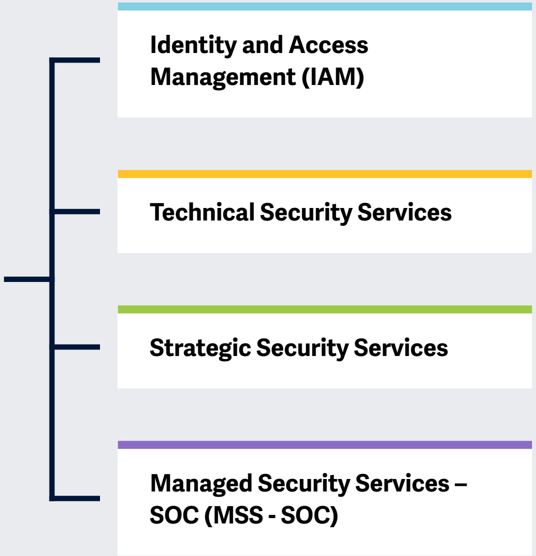
ISG's analysis of 2023 market data indicates an ever-widening range of concerns among CIOs and CISOs in the U.S. Public Sector that include:

- Threats including ransomware, malware and phishing attacks
- An expanding threat horizon arising from remote work environments
- Limited availability of talent
- Inadequately trained or callous employees
- Limitations in data collection and monitoring
- Budget constraints and limited resources

Dealing with these concerns is a challenge for most public sector organizations due to often complex legacy infrastructures, systems and data types that vary by organizations and functions. Also, funding tends to be more limited for them compared with commercial entities. Meanwhile, multiple agencies, both within and outside the public sector, require access to current and historical, and public and private, data generated from an ever-expanding range of devices and technologies.

The rise of AI will be an increasingly significant threat to U.S. public sector agencies.
They need to understand related threats, and opportunities as well as the expected impact of directives by the U.S. government, at the state and federal government level, to manage AI within the agencies and the overall government.

Key focus areas for Cybersecurity – Solutions and Services 2024 – U.S. Public sector



Identity and Access Management (IAM)

Technical Security Services

Strategic Security Services

Managed Security Services – SOC (MSS - SOC)

Simplified Illustration Source: ISG 2024

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
- 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 public sector clients also use information from these reports to evaluate their current vendor relationships and potential engagements.

Definition

This quadrant assesses IAM solution providers for their ability to offer proprietary software and associated services for managing user identities and devices in the U.S. public sector. The quadrant also includes SaaS offerings based on proprietary software. **It does not include pure service providers that do not offer an IAM product (on-premises and/or cloud) based on proprietary software**. Depending on organizational requirements, providers deploy their offerings on-premises, on the cloud (managed by a customer) or as an as-a-service model or a combination thereof.

IAM solutions are aimed at managing (collecting, recording and administering) user identities and related access rights and also include specialized access to critical assets through privileged access management (PAM), allowing access based on pre-defined policies. For handling existing and new application requirements, IAM solution suites are increasingly embedded with secure mechanisms, frameworks and automation (for example, risk analysis functions) to undertake real-time user and attack profiling. Solution providers are also expected to provide additional functionalities related to social media and mobile use to address specific security needs that go beyond traditional web and contextual rights management to include machine identity management.

Eligibility Criteria

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

Definition

This quadrant assesses technical security services (TSS) providers offering integration, maintenance and support for both IT and OT security products or solutions. TSS encompass all security products, including antivirus, cloud and data center security, IAM, data loss prevention (DLP), network security, endpoint security, unified threat management (UTM), OT security and secure access service edge (SASE).

TSS providers offer standardized playbooks and roadmaps that aid in transforming an existing security environment with best-of-breed tools and technologies, improving a security posture and reducing threat impact. Their portfolios are designed to enable the complete or individual transformation of an existing security architecture with relevant products across domains such as networks, cloud, workplace, OT, IAM, data privacy and protection, risk and compliance management and SASE. 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 portfolios. This quadrant also encompasses classic managed security services that include the ones provided without a security operations center (SOC).

This quadrant examines service providers that are not exclusively focused on proprietary products and can implement and integrate products or solutions from other vendors.

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the U.S. public sector
2. **Have authority granted 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

Definition

This quadrant assesses strategic security services (SSS) providers that offer IT and OT security consulting services, covering security audits, compliance and risk advisory, security assessments, security solution consulting, and awareness and training. These services are used to assess security maturity and risk posture and define tailored cybersecurity strategies for the U.S. public sector.

SSS providers engage security consultants that have extensive experience in planning, developing and managing end-to-end security programs for the public sector. Given the increased focus on cyber resiliency, providers offering SSS formulate business continuity roadmaps and identify and prioritize business-critical applications for recovery. They also conduct periodic tabletop exercises and cyber drills for board members, key business executives and employees to foster cyber literacy and establish best practices to better respond to actual threats and cyberattacks. Adept with security technologies and products in the market, they advise on choosing the products and vendors best suited for the specific requirements of agencies.

This quadrant examines service providers that do not exclusively focus on proprietary products or solutions. The services analyzed here cover all security technologies, including OT security and secure access service edge (SASE).

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessment, vendor selection, solution consulting and risk advisory**
2. **Offer at least one of the above** strategic security services in the U.S. public sector
3. Ability to offer **security consulting services using frameworks** is an advantage
4. **Do not focus** solely on **proprietary products** or solutions

Definition

This quadrant assesses providers in the managed security services - SOC (MSS - SOC) space, offering services related to the continuous monitoring of IT and OT security infrastructures and the management of the IT infrastructure for one or several customers through a security operations center (SOC). **This quadrant examines service providers that do not exclusively focus on proprietary products but can manage and operate best-of-breed security tools**. They can handle the entire security incident lifecycle, from identification to response.

The U.S. public sector is increasingly focusing on enhancing overall security and maximizing the effectiveness of security programs in the long term with continuous improvement and is seeking providers to bring this to fruition. To accomplish this, MSS-SOC providers are combining traditional managed security services with innovation to fortify their clients with integrated cyber defense mechanisms. They are also offering the services of experts – skilled in threat hunting and incident management, with capabilities in delivering managed detection and response (MDR) services and equipped with the latest technologies – to support agencies to actively detect and respond through threat mitigation and containment. Owing to growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence and making significant investments in technologies such as automation, big data, analytics, AI and machine learning. These sophisticated SOCs can support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Offer typical services such as **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures and penetration testing** to provide ongoing, real-time protection without compromising on business performance
2. Provide security services such as prevention and **detection, security information and event management (SIEM)** and security advisory and auditing support remotely or at a client's site
3. Possesses **accreditations** from security tools vendors
4. **Manage own SOCs**
5. Maintain **staff with** certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models

Quadrants by Region

As part of this ISG Provider Lens™ quadrant study, we are introducing the following four quadrants on Cybersecurity – Solutions and Services 2024 - U.S. Public Sector:

Quadrant	U.S. Public Sector
Identity and Access Management (IAM)	✓
Technical Security Services (TSS)	✓
Strategic Security Services (SSS)	✓
Managed Security Services – SOC (MSS - SOC)	✓

Schedule

The research phase falls in the period between January and February 2024, during which surveying, evaluation, analysis and validation will take place. The results will be presented to the media in July 2024.

Milestones	Beginning	End
Survey Launch	Jan 8, 2024	
Survey Phase	Jan 8, 2024	Feb 22, 2024
Sneak Preview	May 2024	
Press Release & Publication	July 2024	

Please refer to the link to view/download the ISG Provider Lens™ 2024 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 provided in the invitation email to generate a new password. We look forward to your participation!

Research Production Disclaimer:

ISG collects data for the purposes of writing 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^{TM} 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 "Voice of the Customer" concept. 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 the 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:
ISG.star@isg-one.com

Contacts For This Study

Phil
Hassey

Lead Analyst – U.S. Public Sector

Bhuvaneshwari
Mohan

Research Analyst

Shreemadhu
Rai B

Project Manager

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 participate actively in this research.

* Rated in the previous iteration

Accenture*

ActioNet*

AT&T Cybersecurity*

Avatier*

AWS*

Beta Systems*

Broadcom*

Capgemini*

CGI*

Cisco*

CyberArk*

Deloitte*

DXC Technology*

Eviden (Atos)*

EY*

ForgeRock*

Fortinet*

Fortra*

Fujitsu*

FusionAuth*

Hashicorp*

HCLTech*

IBM*

Infosys*

KPMG*

Kudelski Security*

Leidos*

ManageEngine*

Microsoft*

Nok Nok Labs*

NTT DATA*

Okta*

One Identity (OneLogin)*

OpenText*

Ping Identity*

RSA*

SailPoint*

Saviynt*

TCS*

Tech Mahindra*

Trustwave*

Unisys*

Verizon Business*

Wipro*

Zensar*

About Our Company & Research

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.

ISG Provider Lens™

JANUARY, 2024

BROCHURE: CYBERSECURITY – SOLUTIONS AND SERVICES