ISG Provider Lens™

# Cybersecurity – Solutions and Services 2023

An analysis of the cybersecurity market, comparing provider portfolio attractiveness and competitive strengths

**BROCHURE | JANUARY 2023 | U.S. PUBLIC SECTOR**

Table of Contents

# Introduction

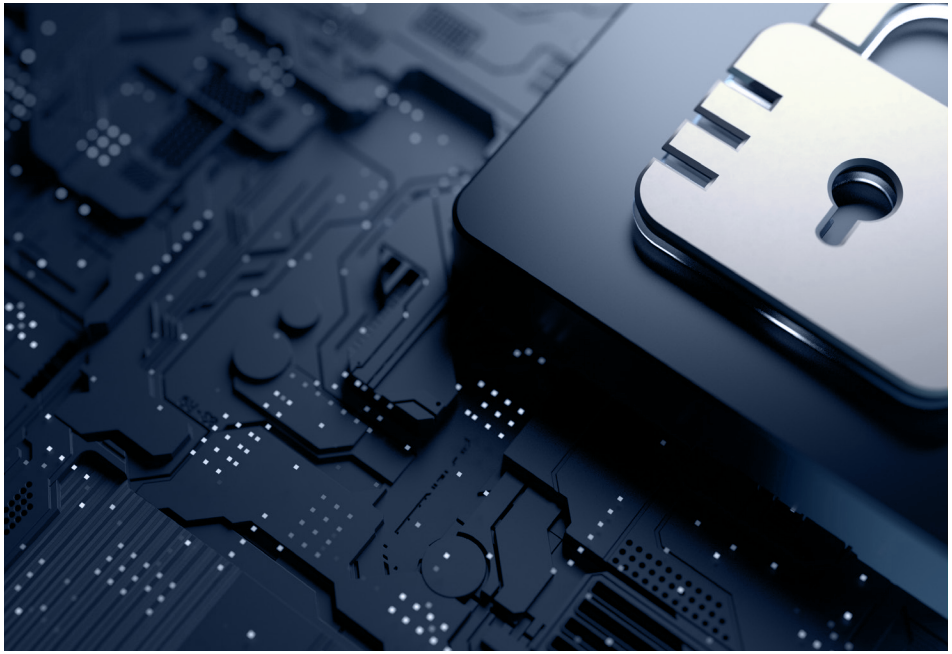
ISG's analysis of 2022 market data indicates an ever-widening range of concerns among U.S. Public Sector CIOs and CISOs, including:

- Threats including ransomware, malware and phishing attacks
- Expanding threat horizons from remote work environments
- Limited resources
- Inadequately trained or careless employees
- Limited data collection and monitoring
- Budget constraints and resource limits

Dealing with these concerns is more challenging for most public sector organizations due to often-complex legacy infrastructures, systems and data types that vary based on organizational and functional requirements. Funding tends to be more limited than in most commercial circumstances. Meanwhile multiple entities inside and outside public agencies require access to current and historical as well as public and private data through an ever-expanding range of devices and technologies.

This ISG Provider Lens™ U.S. Public Sector Cybersecurity Solutions and Services 2023 study supports government and non-government IT decision-makers in their evaluation of providers, services and solutions by offering the following:

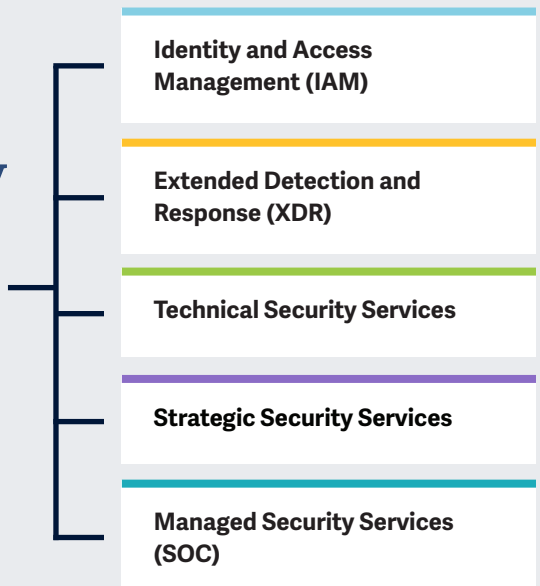
- Segmentation and assessment of solutions and services by critical offering type
- Transparency on the strengths and weaknesses of relevant providers
- Differentiated positioning of providers by market segments



# Introduction

For IT services providers and solution vendors, this study serves as an important decision-making basis for positioning key relationships and go-to-market considerations. ISG advisors, enterprises and public sector clients are able to leverage the information from ISG Provider Lens™ reports, while evaluating their current vendor relationships and potential engagements.

# Key focus areas for **Cybersecurity – Solutions and Services** 2023 – U.S. Public sector




Simplified Illustration Source: ISG 2023

## Definition

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 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.

## Definition

IAM vendors and solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services for managing enterprise user identities and devices. This quadrant also includes SaaS offerings based on proprietary software. **It 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, these offerings could be deployed in several ways such as on-premises or in 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), where access is granted based on defined policies. To handle existing and new application requirements, IAM solution suites are increasingly embedded with secure mechanisms, frameworks and automation (for example, risk analysis) to provide real-time user and attack profiling functionalities. Solution providers are also expected to provide additional functionalities related to social media and mobile use to address specific security needs beyond traditional web and contextual rights management. Machine identity management is also included here.

### Eligibility Criteria

1. Established presence and experience in public sector entities
2. Solutions deployable as **on-premises, cloud, identity-as-a-service** (IDaaS) and a managed third-party model.
3. Support for **authentication** as a combination of **single-sign on (SSO), multi-factor authentication (MFA),** in risk-based and context-based models.
4. Capable of **supporting role-based access** and PAM.
5. Able to provide **access management** for one or more enterprise needs such as **cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.**
6. Capable of **supporting one or more legacy and new IAM standards,** including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM.
7. Portfolio including one or more of the following: **directory solutions, dashboard or self-service management** and lifecycle management (migration, sync and replication) solutions.

## Definition

The XDR solution providers assessed for this quadrant are characterized by their ability to offer a platform that integrates, correlates and contextualizes data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-delivered technology, comprising multiple-point solutions. It uses advanced analytics to correlate alerts from multiple sources, including from weak individual signals to enable accurate detections. XDR solutions consolidate and integrate multiple products and are designed to provide comprehensive workspace security, network security or workload security. Typically, XDR solutions are aimed at vastly improving visibility and improving context to the identified threat across the enterprise. Therefore, these solutions include specific characteristics, including telemetry and contextual data analysis, detection and response. XDR solutions comprise multiple products and solutions integrated into a single pane of glass to view, detect and respond with sophisticated capabilities. High automation maturity and contextual analysis offer unique response capabilities tailored to the affected system, and prioritize alerts based on severity against known reference frameworks. **Pure service providers that do not offer an XDR solution based on proprietary software are not included here.** XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expense, and are particularly suitable for security operations teams that have difficulty in managing a best-of-breed solutions portfolio or getting value from a security information and event management (SIEM) or security, orchestration, automation and response (SOAR) solution.

### Eligibility Criteria

1. Established presence and experience in public sector entities
2. Offering should be based on **proprietary software** and not on third-party software.
3. Primary components including **XDR front end and XDR back end**.
4. The front end should have **three or more solutions or sensors**, including, but not limited to, **endpoint detection and response,** endpoint protection platforms, network protection (firewalls, IDPS), network detection and response, identity management, email security, mobile threat detection, cloud workload protection and identification of deception.
5. **Comprehensive and total coverage and visibility** of all endpoints in a network.
6. Demonstrated **effectiveness in blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware.
7. Ability to leverage **threat intelligence** and analyze and report real-time insights on threats emanating across endpoints.
8. **Automated response capabilities.**

## Definition

The Technical Security Services (TSS) providers assessed for this quadrant cover integration, maintenance and support for both IT and operational technology (OT) security products or solutions. They also offer DevSecOps services. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, 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 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, among others. The offerings also include product or solution identification, assessment, design and development, implementation, validation, penetration testing, integration and deployment. The providers also leverage sophisticated solutions that enable comprehensive vulnerability scanning across applications, networks, endpoints and individual users to uncover weaknesses and mitigate external and internal threats.

TSS providers invest in establishing partnerships across security technology, cloud, data and network domains to gain specialized accreditations and expand the scope of their work and portfolios. This quadrant also encompasses classic managed security services, i.e. those provided without a security operations center (SOC).

**This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.**

### Eligibility Criteria

1. Established presence and experience in public sector entities
2. Demonstrated experience in **implementing cybersecurity solutions** for companies in the respective country.
3. **Authorized by security technology vendors** (hardware and software) to distribute and support security solutions.
4. **Valid certification** regarding capabilities supporting security technologies.

## Definition

The Strategic Security Services (SSS) providers assessed for this quadrant offer consulting for IT and OT security. The services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategies for enterprises (tailored to specific requirements).

SSS providers should employ security consultants that have extensive experience in planning, developing and managing end-to-end security programs for enterprises. With the growing need for such services among SMBs and the lack of talent availability, SSS providers should also make these experts available on-demand through vCSIO (virtual chief security information officer) services.

Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity roadmaps and prioritize business-critical applications for recovery. They should also conduct periodic tabletop exercises and cyber drills for board members, key business executives and employees to help them develop cyber literacy and establish best practices to better respond to actual threats and cyberattacks. They should also be adept with security technologies and products available in the market and offer advice on choosing the best product and vendor suited to an enterprise's specific requirements.

**This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.** The services analyzed here cover all security technologies, especially OT security and SASE.

### Eligibility Criteria

1. Established presence and experience in public sector entities
2. Demonstrated abilities in SSS areas such as **evaluation, assessments, vendor selection, architecture consulting and risk advisory.**
3. Ability to execute **security consulting services using frameworks** will be an advantage.
4. Demonstrated **focus and capability beyond proprietary products** or solutions.

## 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. Established presence and experience in public sector entities
2. Portfolio enabling ongoing, real-time protection, without compromising on business performance. Offerings may include s**ecurity 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 secure access service edge (SASE).
3. 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.
4. **Staff and technological accreditation/certification** from security tools vendors.
5. **SOCs ideally owned and managed by the provider** and not predominantly by partners.

## Quadrants By Region

As part of this ISG Provider Lens™ quadrant study, we are introducing the following seven quadrants on Cybersecurity - Solutions and Services 2023 - U.S. Public sector:

| Quadrants | U.S. Public Sector |
|---|---|
| Identity and Access Management (IAM) | ✔ |
| Extended Detection and Response (XDR) | ✔ |
| Technical Security Services | ✔ |
| Strategic Security Services | ✔ |
| Managed Security Services (SOC) | ✔ |

# Schedule

The research phase falls in the period between January and February 2023, during which surveying, evaluation, analysis and validation will take place. The results will be presented to the media in July 2023.

| Milestones | Beginning | End |
|---|---|---|
| Survey Launch | Jan 12, 2023 | |
| Survey Phase | Jan 12, 2023 | Feb 13, 2023 |
| Sneak Previews | May 2023 | |
| Press Release & Publication | Jul 2023 | |

Please refer to the link to view/download the ISG Provider Lens™ 2023 research agenda

### Access to Online Portal

You can view/download the questionnaire from here using the credentials you have already created or refer to 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 crea ting 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 rec eived 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: ISG.star@isg-one.com

# Contacts For This Study

Phil
Hassey

**Lead Analyst**

Deepika
B

**Research Analyst**

Bruce
Guptill

**Co-Lead Analyst**

Ridam
Bhattacharjee

**Project Manager**

Bhuvaneshwari
Mohan

**Research Analyst**

**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 advisors participate as part of each study's quality and consistency review team (QCRT).

The QCRT ensures 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 QCRT group and contribute at different levels depending on their availability and expertise.

The QCRT 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

Alex Perry

**Director**

# 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

2Secure
Absolute Software*
Accenture*
Actifio
ActioNet*
Acuity Risk Management
ADT Cybersecurity (Datashield)
Advenica
AlgoSec
Amazon Web Services
Aqua Security Software
Arcserve
Armis*
Ascentor
AT&T Cybersecurity*
Atomicorp
Atos*
Authy
Avatier*
Axis Security
Barracuda Networks
BCG
BehavioSec
Bell Techlogix
BetterCloud
BigID
Bittium
BlueSteel Cybersecurity
BluVector
BoldonJames
Booz Allen Hamilton
Bricata
Bridewell Consulting
Broadcom*
Capgemini*
Censornet
CGI*
Check Point*
Chronicle Security (Google)
CI Security
Cigniti
Cisco*
Claroty
Clavister
Cloud Range
CloudCodes
Cloudflare
CloudPassage
Code42
Cognizant*
ColorTokens
Column Information Security (Now Majorkeytech)
Comodo*
Confluera
Contrast Security
Core
Coromatic
CorpFlex
CoSoSys*

# 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

CSIS Security Group
CTR Secure Services
Cyber 1
Cyber Swiss
CyberArk*
Cybercom Group (now Knowit)
Cynet
Cypher
Datadog
deepwatch
Deloitte*
Digicert
Duo Security, Inc (part of Cisco)
DXC Technology*
Efecte
Elastic
Encore
Entrust
EY*
Fidelis Cybersecurity*
Forcepoint*
Forescout Technologies
ForgeRock*
Fortinet*
Fujitsu*
FusionAuth*
HCL*
HelpSystems*
Hexagon
Hexaware
IBM*
Ilantus Products*
Imperva*
Infosys*
Ivanti*
Kasada*
KPMG*
Kudelski Security*
Leidos*
Logicworks
ManageEngine*
Masergy
McKinsey
Micro Focus*
Microsoft*
Netskope*
Nok Nok Labs*
Nozomi Networks
NTT*
Okta*
One Identity (OneLogin)*
OpenText*
Opswat
Palo Alto Networks*
Ping Identity*
Proofpoint*
Rackspace
RSA*
SailPoint*
Salesforce

# 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

Sectigo
Software AG
SoftwareOne
Sophos*
Synoptek
Sysdig
TCS*
Tech Mahindra*
Trend Micro*
Trianz
Trustwave*
Unisys*
Utimaco
Varonis*
Verizon*
Wipro*
XenonStack
Yubico
Zacco
Zensar*
ZeroFOX
Zscaler*

## 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 800 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 1,300 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 www.isg-one.com.

ISG Provider Lens™

**JANUARY, 2023**

# REPORT: CYBERSECURITY - SOLUTIONS AND SERVICES