ISG Provider Lens™

Cybersecurity – Solutions and Services

Technical Security Services

A research report comparing services provider and software vendor strengths, challenges, and competitive differentiators

Customized report courtesy of:

Infosys® Public Services

QUADRANT REPORT | JULY 2022 | U.S. PUBLIC SECTOR

Table of Contents

Report Authors: Bruce Guptill, Keao Caindec

A historical sense of urgency to improve

State and municipal agencies in the U.S. are actively seeking new types of solutions across critical areas of organization, function and technology. From cybersecurity and procurement to digital workspace and HR, public agencies seek immediate operational and cost improvements with long-term operational and system stability, the combination of which usually requires significant investments in new technology and considerable change in organization and IT operation and management.

Such changes are a historic turning point for government agencies and associated organizations, as they are bounded by established policies and procedures that prescribe functionality according to traditional and regulated market and operational structures.

This quest for rapid improvement is also creating exceptional opportunity for services and software providers. However, many providers are uncertain about how to respond.

Core market disruptions and drivers

ISG market analysis indicates this interest and activity in immediate organizational and IT change and improvement is widespread and growing. We see a consistent set of U.S. public sector economic, social and tech factors driving the same. These include the following:

1. **Overwhelming cost and constituent pressures:** Pressures on public agencies to reduce operational

The best solutions focus on proven technologies that can be **effective for public sector organizations**

costs have been increasing for years; COVID-19 disruptions accelerated and increased these demands. Additionally, the public sector has reached a tipping point where a critical mass of citizens, suppliers and other constituencies increasingly expect digital experience and engagement with elected officials and governmental institutions. Cybersecurity, a critical enabler and element of this digital demand, has struggled to keep pace.

2. **End of useful life for expanding core IT:** Public agencies are accelerating their efforts to embrace technology adoption and adaptation. This is fueled by the significant reliance on end of life traditional, on-premises software and servers. But even those that embraced cloud-based IT are finding early-generation SaaS can be challenging to keep pace with the scope of digital experience expectations from constituencies. Legacy-perimeter-focused cybersecurity is no longer enough to mitigate cyber threats and protect stakeholder data.

3. **Stabilizing remote/digital operational environments:** Mobile and remote work was already advancing prior to 2020, but COVID-19-induced massive workforce location and IT use changed for public agencies. This is beginning to stabilize, enabling IT agencies and operational leaders to better conceive and develop suitable strategies and solutions. As the workforce and workplace become clearer, public agencies are looking to engage with providers for effective implementation and management of cybersecurity services and tools.

4. **Inability to use and secure data effectively and efficiently:** The public sector is facing increased inefficiencies in data utilization and a growing range of data security challenges. As older systems were continually patched and as more users were connected from more locations in different ways, risk and inefficiencies grew, further pushing the need for newer, more capable, more secure and less operationally expensive options.

5. **Lack of skilled labor:** Another public sector trend witnessed before 2020 was massively accelerated by COVID-19 developments and staff shortage. The great retirement trend widely noted in late 2021 in the U.S. market was partly rooted in massive retirements among state and municipal government workers. Federal labor statistics indicated that the there was an increase in new job vacancies in 2021 among state and municipal government organizations. The U.S. public sector reported new job vacancies of more than 11 percent in Q42021. The need for more efficient cybersecurity, requiring less human involvement, is the new norm and growing rapidly.

Public agencies, especially many state and municipal agencies, have been prevented from making significant change or improvement in IT due to budgetary issues and competing demands from public leaders and professionals. The above factors, coupled with increased federal, state and local funding, are forcing agencies to act quickly and effectively. Doing nothing is no longer an option.

How can providers best serve the public sector?

The software vendors and services providers best positioned for this new, aggressively seeking improvement in the U.S. public sector have dedicated resources, robust partnerships and solutions tailored to sector requirements. This is because:

- Faced with insufficient staff and urgency of needs, there is a lack of strategic, holistic vision among buyers, which hampers long-term efficiency improvements
- Public sector professionals want to act fast and desire immediate improvement, but must navigate political and budget uncertainty and complex regulatory requirements and processes
- Buyers and sellers alike must manage slow sales cycle times and have exhaustive evaluation criteria when spending public funds
- Incumbent providers tend to have significant advantages based on available renewal options, as the longstanding regulatory and procurement processes are lengthy and require significant effort for both buyers and sellers
- Significant contracting communication issues need to be managed or prevented, including:
  - Frequently outdated language and terms
  - Responsibilities that may not reflect current or emerging operations and solutions
  - Interpretations of performance and delivery that may quickly become obsolete by new solutions, new organizations and other market/sector changes

Even those providers with robust presence in U.S. federal government sector are often challenged to compete at the state and municipal levels. They lack needed market intelligence, contracting experience and support resources, which tend to differ significantly from the federal government. Several influential providers currently focused on federal government sector are well-positioned to serve state and municipal clients, but will require strategic investment to qualify as Leaders in ISG's assessment.

Expected market conditions in 2023

ISG expects the following conditions to influence public sector buyer and seller cybersecurity activity in 2023 and likely beyond:

1. **Public sector organizations will leapfrog from legacy tech to next-generation capabilities:** The accelerating disappearance of traditional staff, combined with strained legacy IT and exceptionally backwards compatible new solutions, will push public agencies to adopt and adapt more leading-edge solutions. This, in turn, creates the need for more effective training in security awareness, policy and management.
2. **A boom in solutions, especially in integrative platforms:** As noted in several 2022 ISG Provider Lens studies, software solution platforms can enable significant immediate benefits in operational efficiency and security (including reducing the need for traditional skills), while providing a solid foundation for ongoing improvement. Security platforms that integrate, provide visibility into and

enable policy management across solutions and use points will thrive.

3. **Limited BPO/ITO growth:** While many U.S. public agencies could benefit from outsourcing business processes, it remains a sensitive concept, especially for those in municipal governments. ISG expects this perception to slowly shift as public sector entities look to maintain critical services in challenging circumstances. Additionally, as economic and labor complexities evolve and as the value of strategic, technical and managed security services becomes more apparent to public sector organizations, more BPO/ITO growth is expected in the coming years.

4. **A mostly tactical approach:** While newer tech minimizes many traditional technology and functional barriers, public sector organizational and operational structures resist change. Regulations and accepted practices will perpetuate core organizational, cultural and functional silos, which, in turn, will:

- Reduce operational and functional point costs while increasing long-term costs
- Inhibit data standardization and sharing and system interoperability
- Feed long-term and growing needs for systems integration, security and master data management

The above should result in rapidly expanding demand for the following through 2024:

- **Systems, services, and data integration and management:** The U.S. public sector, especially state and municipal government agencies, will seek security services providers and platform vendors that focus on integration and unified management of systems and data.
- **Strategic consulting and training – organizational, operational, and technological:** The above market conditions will create more demand for strategic security consulting services, including organizational and structural change, function and operation change management (including business process re-engineering), and core IT strategy and management change.

Bottom-line guidance: The U.S. public sector buyers and users should look for providers and vendors with significant, relevant public sector experience and their solutions must be adapted, bundled or tailored to current and expected requirements. The best solutions focus on proven technologies that can be effective for public sector organizations . New technology used in new ways may be more capable, but until proven to be effective at a lower cost overall, they are rarely worth pursuing.

> Doing nothing is no longer an option.

Provider Positioning

Page 1 of 9

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	Not In	Product Challenger	Not In	Not In	Not In
Accenture	Not In	Not In	Leader	Leader	Leader
ActioNet	Not In	Not In	Contender	Product Challenger	Contender
Armis	Contender	Not In	Not In	Not In	Not In
AT&T Cybersecurity	Not In	Not In	Contender	Contender	Product Challenger
Atos	Leader	Not In	Leader	Leader	Leader
Avatier	Product Challenger	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Broadcom	Leader	Leader	Not In	Not In	Not In
Capgemini	Not In	Not In	Leader	Leader	Leader
CGI	Not In	Not In	Market Challenger	Market Challenger	Market Challenger
Check Point	Not In	Product Challenger	Not In	Not In	Not In
Cisco	Not In	Not In	Not In	Not In	Market Challenger
Cognizant	Not In	Not In	Product Challenger	Product Challenger	Contender
Comodo	Not In	Contender	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
CoSoSys	Not In	Product Challenger	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Leader	Leader	Leader
DXC Technology	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
EY	Not In	Not In	Leader	Leader	Leader
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In
Forcepoint	Not In	Product Challenger	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In
Fortinet	Contender	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Product Challenger	Contender	Contender
FusionAuth	Contender	Not In	Not In	Not In	Not In
HCL	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
HelpSystems	Contender	Product Challenger	Not In	Not In	Not In
IBM	Leader	Leader	Leader	Leader	Leader

Provider Positioning

Page 5 of 9

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Ilantus Products	Product Challenger	Not In	Not In	Not In	Not In
Imperva	Not In	Product Challenger	Not In	Not In	Not In
Infosys	Not In	Not In	Leader	Leader	Leader
Ivanti	Not In	Product Challenger	Not In	Not In	Not In
Kasada	Not In	Contender	Not In	Not In	Not In
KPMG	Not In	Not In	Product Challenger	Product Challenger	Contender
Kudelski Security	Not In	Not In	Contender	Contender	Not In

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Leidos	Not In	Not In	Rising Star ★	Rising Star ★	Product Challenger
ManageEngine	Leader	Market Challenger	Not In	Not In	Not In
Micro Focus	Product Challenger	Not In	Not In	Not In	Not In
Microsoft	Leader	Market Challenger	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Not In	Not In
Nok Nok Labs	Market Challenger	Not In	Not In	Not In	Not In
NTT	Not In	Not In	Product Challenger	Product Challenger	Product Challenger

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Okta	Leader	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In
OpenText	Not In	Contender	Not In	Not In	Not In
Palo Alto Networks	Not In	Leader	Not In	Not In	Not In
Ping Identity	Product Challenger	Not In	Not In	Not In	Not In
Proofpoint	Not In	Leader	Not In	Not In	Not In
RSA	Leader	Not In	Not In	Not In	Not In

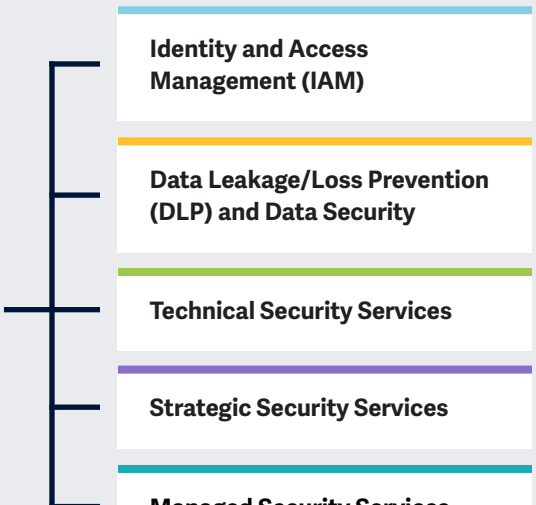
Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Sailpoint	Product Challenger	Not In	Not In	Not In	Not In
Sophos	Not In	Product Challenger	Not In	Not In	Not In
TCS	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Tech Mahindra	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Trend Micro	Not In	Leader	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Product Challenger	Product Challenger
Unisys	Market Challenger	Not In	Leader	Market Challenger	Leader

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Technical Security Services	Strategic Security Services	Managed Security Services
Varonis	Not In	Leader	Not In	Not In	Not In
Verizon	Not In	Not In	Leader	Market Challenger	Leader
Wipro	Not In	Not In	Product Challenger	Leader	Product Challenger
Zensar	Not In	Not In	Contender	Not In	Not In
Zscaler	Not In	Leader	Not In	Not In	Not In

This study focuses on what ISG perceives as most critical in 2022 for **cybersecurity services and solutions for U.S. public sector agencies,** including state and municipal governments, public utilities, health services, and educational organizations.



Simplified Illustration Source: ISG 2022

Definition

Public sector entities in the U.S., including state and municipal governments, public utilities, public safety, educational institutes and non-governmental organizations (NGOs), increasingly face cyberthreats as they adapt to different ways of working.

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

- Threats from external hacking organizations, including foreign governments and the general hacking community
- Expanding threat horizons from increasing remote work environments
- Reduced ability and time to respond to cyber threats
- Inadequately trained or careless employees in an organization
- Threats from ransomware, malware, and phishing attacks
- Inadequate data collection and monitoring
- Budget constraints and resource limits

Dealing with these concerns becomes more challenging due to the nature of public sector work and IT in the U.S. Organizations often have complex legacy infrastructures, systems, and data types that vary based on organizational and functional requirements. Multiple entities inside and outside public agencies require access to current and historical, public and private data. Meanwhile, organizations are struggling to implement, extend, and support the still-emerging digital remote

work reality, which, in turn, can vary by worker role; organizational function; and local, state, and federal regulations.

This ISG Provider Lens™ U.S. Public Sector Cybersecurity Solutions & Services 2022 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

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.

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following 5 quadrants on cybersecurity software solutions and services:

Identity and Access Management (IAM), Data Leakage/Loss Prevention (DLP) and Data Security; Technical Security Services (TSS), Strategic Security Services (SSS), and Managed Security Services (MSS).

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

1. Transparency on the strengths and weaknesses of relevant services providers and software vendors
2. A differentiated positioning of providers by segments
3. Focus on the U.S. Public Sector

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 US$20 million and US$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 US$1 billion, with activities worldwide, and globally distributed decision-making structures.

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

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

Provider Classifications: Quadrant Key

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

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.

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.

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not in means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.

Technical Security Services

Who Should Read This

This report is designed to help public sector enterprises in the U.S. to evaluate providers that are not exclusively focused on their proprietary products but can implement and integrate other vendors' products or solutions. The report covers integration of IT security products or solutions.

In this quadrant, ISG defines the current market positioning of providers that implement and integrate IT security services in the U.S. public sector. It also describes how each provider addresses the key challenges. Organizations in the U.S. public sector evaluate if the services implemented can address the latest attacks, enabling federal organizations to prepare against them and respond swiftly to circumvent any adverse impact of ransomware and malware on their sensitive information.

Considering the volatile security landscape, technical security services are in high demand in the U.S public sector, compared to private enterprises. In keeping with the requirements of the public sector, service providers deliver reliable and effective solutions, incorporated with the latest technologies and tools, to foster efficiency and productivity. For the smooth implementation of a solution, federal agencies prefer vendors with a highly skilled workforce, a large portfolio of capabilities and a global presence in the security space.

Chief information security officers should read this report because, with digital transformation at the forefront of businesses today, they need to find a balance between data security, customer experience and privacy. They need to have a thorough understanding of the leading service providers in the market that assist with integrating IT security services, and they need deep insight into provider capabilities.

Chief strategy officers should read this report to understand the relative positioning and capabilities of service providers and collaborate with them to develop effective cybersecurity services. Also, this report can be used to implement an effective data protection strategy. CTOs can build public-private partnership strategies to enhance competitiveness.

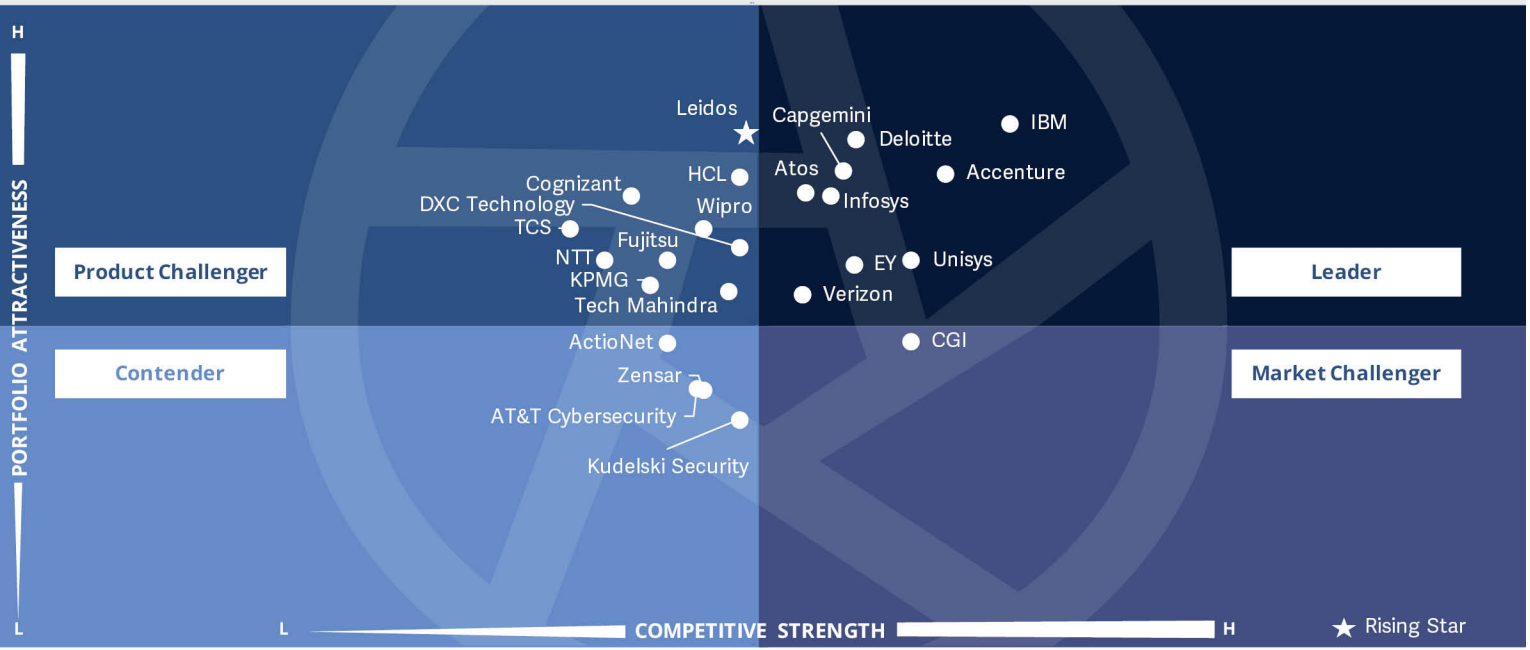
Security analysts should read this report to understand how providers adhere to the security and data protection mandates in the U.S. public sector to stay apace with market trends. In addition, it also supports decision-making on collaborations, partnerships and cost-reduction initiatives.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Technical Security Services

Source: ISG RESEARCH

U.S. Public sector 2022



Technical security services (TSS) are critical for **developing, adapting, and innovating with cybersecurity solutions, tools and services.** Proven **public sector expertise** is key to satisfying buyer and user needs in this segment.

Bruce Guptill

Definition

This quadrant examines services and providers of technical security services (TSS) serving the U.S. public sector, especially state and municipal government agencies, along with higher education institutions and public services and utilities.

For our purposes, TSS includes integration, maintenance and support for IT security products or solutions. TSS addresses all security products, including anti-virus, cloud, and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM) and more.

Eligibility Criteria

Eligibility and assessment criteria used by ISG for services and providers in this quadrant include the following:

1. Established presence and relevance among U.S. public sector clients
2. Not exclusively focused on proprietary products
3. Authorized by vendors to distribute and support security solutions.
4. Certified experts to support included security technologies
5. Ability to participate (desirable, not mandatory) in local security associations and certification agencies

Observations

As noted at the beginning of this report, ISG expects cybersecurity solutions and platforms to be adopted and adapted more widely and sooner than outsourcing via MSS. Outsourcing of any key IT capability is still an uncertain prospect, especially among U.S. state and municipal government agencies.

Given this expectation of solution and platform adoption and adaptation, ISG sees a large and rapidly growing demand for TSS in several years to come. TSS providers help in solution or platform selection, customization, implementation and optimization. They also partner with relevant MSS and SSS providers to enable cybersecurity in the U.S. public sector.

There are many providers developing cybersecurity architectures that are repeatable and adaptable across multiple types of public agencies and domains. This is expected to expand and accelerate as public agencies require more advanced cybersecurity while largely holding off from outsourcing security as a service. The result will include a growing number and range of solution architectures optimized for specific public sector entity domains such as licensing, taxation and public health services.

Therefore, ISG sees TSS providers' engineering, architecture and integration skillsets as being of equal importance as the functionality of their technologies and tools, as well as of any solutions that they offer.

From the more than 70 companies assessed for this study, 25 have qualified for this quadrant, with 9 being identified as Leaders and 1 identified as a Rising Star.

accenture

Accenture's TSS offering includes attack-surface reduction, digital identity management, cloud/infrastructure security and data security, among others. Accenture demonstrates in-depth understanding of threat actors' tactics, techniques and procedures, including the capability of reverse engineering malware.

Atos

Atos reports more than 4,500 cybersecurity experts and 29 security operations and innovation centers worldwide, including two major facilities in the U.S. Released in 2021, Atos' Cyber Recovery end-to-end platform enables clients to quickly recover from ransomware and other kinds of destructive cyberattacks.

Capgemini

Capgemini's TSS portfolio enables clients to adopt or adapt solutions that address business goals while protecting critical data, systems and users. Services are tailored to client-specific circumstances, typically based on the findings of Capgemini's business and cybersecurity consulting and assessment services.

Deloitte

Deloitte focuses on data privacy, including technologies and services aimed at privacy regulation compliance, as well as data breach notification. The company's TSS capabilities are enhanced through its extensive public sector knowledge developed over decades of business, financial and operational consulting. The company can address sector-specific strategy, operational and organizational needs.

EY

EY's TSS advantages build from its security architecture, security engineering and emerging technologies practice teams. These teams design, build, customize and manage next-generation security operations and response for clients. Specialty areas include risk management, data protection and privacy, and IAM.

IBM

IBM has established its own tech development expertise for more than 10 decades, especially in large and complex IT systems. Its extensive security technology and services partner network complements this. Its TSS offerings emphasize development and advancement of solutions for accelerating adoption and use of zero-trust approaches, cloud security (including CASB), and governance, risk and compliance.

Infosys

Infosys has significantly advanced its TSS portfolio in recent months. It rolled out SASE as a service in partnership with Zscaler, Palo Alto and Cisco. Working with several partners, Infosys also enhanced its IoT OT Security offerings and developed a zero-trust architecture for secure cloud transformation. The company also has brought to market CyberBOX, a service aggregation construct for standardization, acceleration, and amplification of cybersecurity operations.

Unisys

Unisys' core cybersecurity technology focus remains constant throughout its MSS, TSS and SSS offerings. It offers advanced endpoint protection services, SIEM and SDM. The company also offers unified services supporting on-premises and multicloud environments.

Verizon

Verizon offers core security services around four key areas: identify, protect, detect and respond, and recover. Its portfolio includes managed IDS/IPS, firewalls, web gateway, monitoring, identity management, incident management, proactive penetration testing, threat detection and response, vulnerability assessments, management, resolution, analytics, managed SIEM, security orchestration automation and response (SOAR), and MDR.

Leidos

Leidos' (Rising Star) approach enables adaptive defense strategy, sustainable threat protection and a mature security posture. Services include zero-trust planning, security operations center development and operation, cyber resiliency, risk management framework development, cyber analytics, information assurance, insider threat policy and practices, and testing and evaluation in cybersecurity disciplines.

Leader

"A strong portfolio and dedicated resources in the U.S. position Infosys as a Leader in the TSS space."

Bruce Guptill

Infosys

Overview

Infosys is headquartered in Bengaluru, India, and operates in 50 countries. It has more than 279,617 employees across 234 global offices. In FY21, the company generated $13.6 billion (+10.7 percent YoY) in revenue, with financial services as its largest segment. Infosys Public Services focuses exclusively on the North American public sector organizations (federal, state, municipal agencies and NGOs).

Strengths

Significant TSS investment through 2022: Infosys has been making significant advancements in its TSS portfolio from the beginning of 2022, including SASE as a service, in partnership with Zscaler, Palo Alto and Cisco. The company, with its partners, has also enhanced its IoT OT Security offerings and developed a zero-trust architecture for secure cloud transformation. It offers CyberBOX, a service aggregation construct for standardization, acceleration and amplification of cybersecurity operations.

TSS collaborations: Infosys extended its partnership with Purdue University for training its staff in advanced and emerging cybersecurity technologies. It works with education provider, NIIT, in a sponsored M.Tech program and staff training. It is also a subscriber to Cybrary cybersecurity training and certification, which provides access to SOC/CDC playbooks.

Dedicated business unit in the U.S. public sector: Infosys Public Services (IPS) is a subsidiary of Infosys, based in the U.S. It works exclusively with North American public sector organizations. IPS takes advantage of Infosys' more than 40 years of cross-industry IT and business services experience in the U.S. public sector.

Caution

As an India-based firm, IPS' parent company, Infosys, is subject to multinational economic and political disruption, but less so than most other large services providers.

Appendix

Methodology & Team

The ISG Provider Lens 2022 – Cybersecurity – Solutions and Services research study analyzes the relevant software vendors/service providers in the U.S. Public Sector market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Lead Authors:
Bruce Guptill, Keao Caindec

Editors:
Sajina B, Mark Brownstein

Research Analyst:
Monica K

Data Analyst:
Rajesh Chillappagari

Consultant Advisor:
Alex Perry

Project Manager:
Ridam Bhattacharjee

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 June 2022, 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

Lead Author

Bruce Guptill
Principal Analyst

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.

Contributing Author

Keao Caindec
Distinguished Analyst

Keao Caindec has more than 25 years of experience in telecommunications, cloud, and cybersecurity. He also advises senior executives on digital transformation, risk, governance, enterprise information security, OT cybersecurity, DevSecOps, and IT procurement. Keao also helps OEMs improve product security and address supply chain risks. As a Lead Analyst at ISG, Keao is responsible for overseeing the ISG Provider Lens™ Report for U.S. Public Sector Cybersecurity Solutions & Services. He has held executive positions at NTT, Dimension Data, Reliance Communications, and other service providers and technology companies. Keao is a member of ISA99, contributor to the IEC 62443 cybersecurity standard, and a co-chair of the Security Working Group of the Industrial Internet Consortium.

Research Analyst

Monica K
Research Specialist

Monica K is a research specialist and a digital expert at ISG. She supports and co-authoring Provider Lens™ studies on the Internet of Things (IoT), Digital Business Transformation, Blockchain, Enterprise Application as a Service, and Cybersecurity. She has created content for the aforementioned Provider Lens™ studies, as well as content from an enterprise perspective, and she is the author of the global summary report. Monica K brings over 8 years of experience and expertise in technology, business, and market research for ISG clients. Prior to ISG, Monica worked for a research firm specialising in technologies such as IoT and product engineering, as well as vendor profiling and talent intelligence. She has also been in charge of delivering end-to-end research projects and collaborating with internal stakeholders on various consulting projects.

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.

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™

JULY 2022

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES