

Cybersecurity – Solutions and Services

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

Customized report courtesy of:

Atos



Executive Summary 3

Provider Positioning 7

Introduction

Definition 16

Scope of Report 18

Provider Classifications 18

Appendix

Methodology & Team 55

Author & Editor Biographies 56

About Our Company & Research 58

Identity and Access Management (IAM) 20 - 26

Who Should Read This 21

Quadrant 22

Definition & Eligibility Criteria 23

Observations 24

Provider Profiles 26

Data Leakage/Loss Prevention (DLP) and Data Security 27 - 32

Who Should Read This 28

Quadrant 29

Definition & Eligibility Criteria 30

Observations 31

Technical Security Services 33 - 39

Who Should Read This 34

Quadrant 35

Definition & Eligibility Criteria 36

Observations 37

Provider Profiles 39

Strategic Security Services 40 - 46

Who Should Read This 41

Quadrant 42

Definition & Eligibility Criteria 43

Observations 44

Provider Profiles 46

Managed Security Services 47 - 53

Who Should Read This 48

Quadrant 49

Definition & Eligibility Criteria 50

Observations 51

Provider Profiles 53

*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:
 - o Frequently outdated language and terms
 - o Responsibilities that may not reflect current or emerging operations and solutions
 - o 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


	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
ActionNet	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


	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



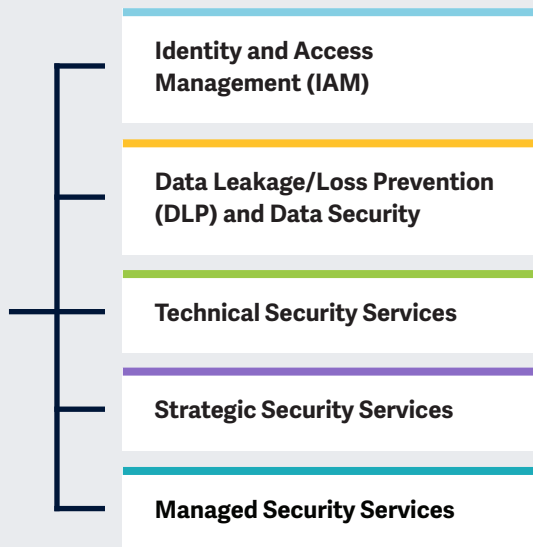
 Provider Positioning

	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.

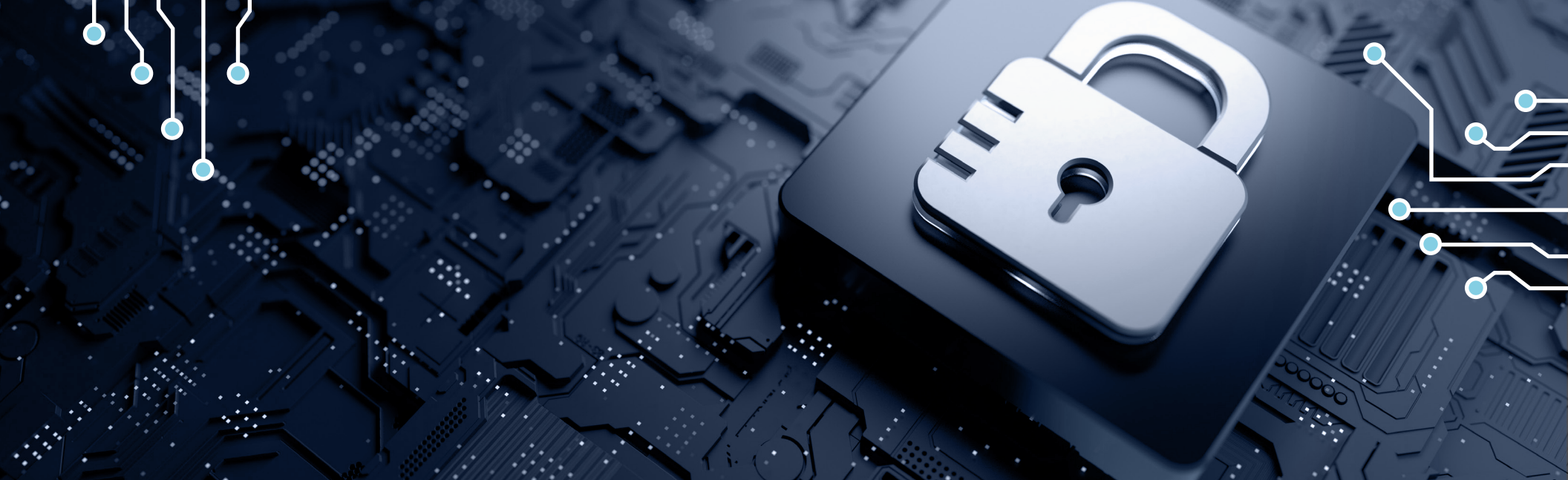
Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/services and a follow sensible market approach with a goal of becoming a Product or 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.





Identity and Access Management (IAM)

Who Should Read This

This report is relevant to public sector enterprises in the U.S. for evaluating providers that offer solutions that integrate multiple features, addressing security concerns arising from changes in work patterns and increased digitalization.

In this quadrant report, ISG highlights the current market positioning of identity and access management (IAM) solution providers that help mitigate security threats in the U.S. public sector, and how each provider addresses key challenges in this sector.

The number of data breaches in the U.S. public sector has been on the rise, and unmanaged privileges and accounts have become increasingly vulnerable to cyberattacks.

In August 2021, the Office of Management and Budget issued mandates, necessitating the use of essential software, thereby compelling federal agencies to outline their privileged access management (PAM) plans in order to comply with the executive order and stay ahead of potential risks. Hence, the adoption of IAM solutions in the U.S. public sector is becoming increasingly important.



Chief information security officers should read this report to understand how IAM solution providers address the significant challenges of compliance and security, while maintaining a seamless experience for enterprise clients

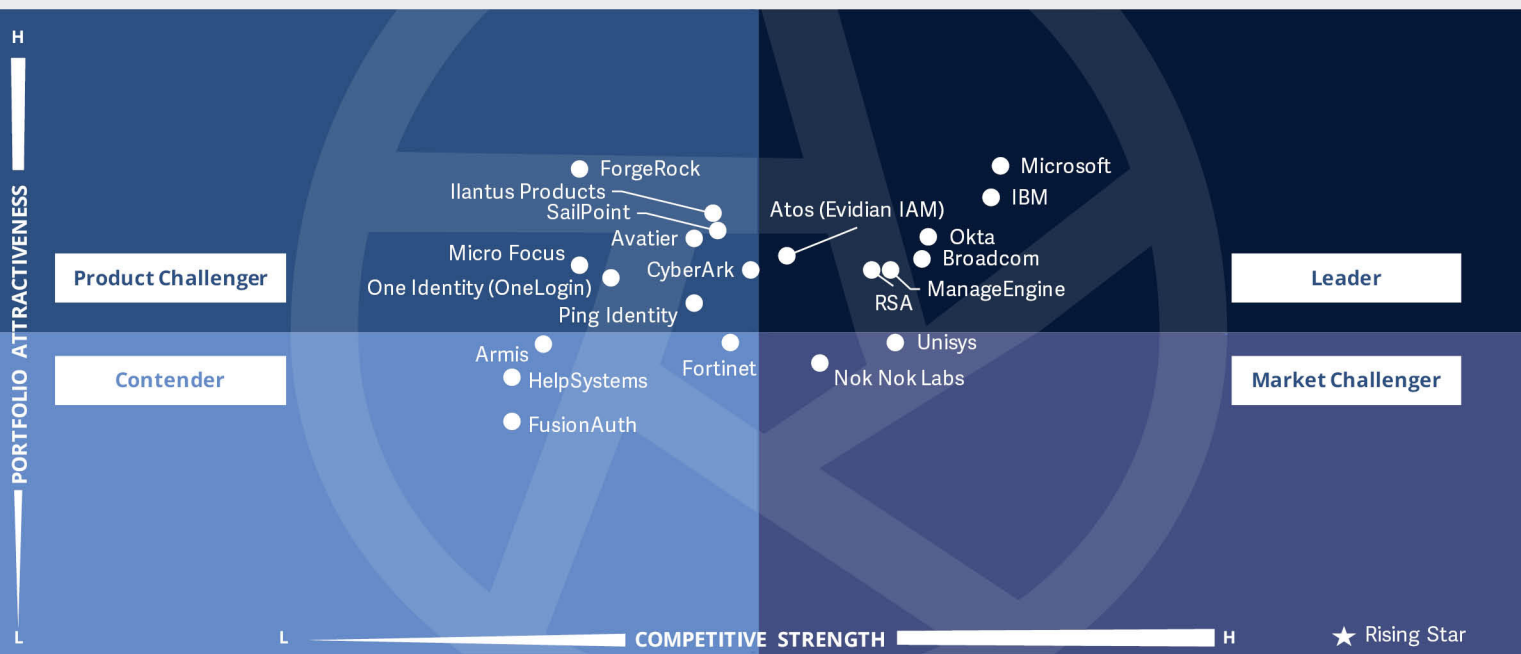


Chief strategy officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting the evolving customer demands.



Chief data officers and data privacy officers should read this report to understand how a provider offers information protection and privacy, information governance, data quality and data lifecycle management





IAM solutions ensure that **access rights are granted based on defined policies, which align with governance and compliance requirements and increasingly enable real-time attack profiling.** Increasingly desired proficiencies include expanded edge, mobile and IoT capabilities.

Bruce Guptill



Identity and Access Management (IAM)

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services for securely managing enterprise user and device identities. This quadrant also includes Software as a Service, based on proprietary software. Pure service providers that do not offer an IAM product based on proprietary software are not included here. Depending on unique organizational requirements, these solutions could be deployed in several ways — on-premises, in the cloud (managed by the customer), as an as-a-service model or a combination thereof.

IAM solutions are aimed at collecting, recording and administering identities and related access rights, as well as specialized access to critical assets, including privileged access management (PAM). They ensure that access rights are

granted based on defined policies that align with governance and compliance requirements.

To handle existing and new application requirements, IAM solutions are increasingly embedded with security mechanisms, frameworks and automation (for example, risk analyses) within their management suites to provide real-time attack profiling functionalities. Solution providers are also expected to provide additional features that address the security needs of mobile users and a variety of workplace and edge devices that go beyond traditional web and context-related rights management.

Eligibility Criteria

For our assessments in this report, IAM solutions considered should be capable of the following (among other capabilities):

1. Being deployed as, or in a combination of, on-premises, cloud, identity as a service (IDaaS) and managed (third-party) models
2. Supporting authentication either, or by a combination of, single-sign on (SSO), multifactor authentication (MFA), passwordless authentication, and risk-based and context-based models
3. Supporting role-based access and PAM
4. Supporting legacy and newer

IAM standards, including, but not limited to, SAML, OAuth, OpenID Connect, FIDO2, WebAuthn, WS-Federation, WS-Trust and SCIM

5. Supporting identity lifecycle management for provisioning and managing credentials

Additionally, the IAM vendor should be able to provide access management for one or more enterprise needs such as cloud, endpoints, mobile devices, application programming interfaces (APIs) and web applications.

Finally, the overall portfolio should offer one or more of the following: directory solutions, dashboard or self-service management, and identity lifecycle management (migration, sync and replication).



Identity and Access Management (IAM)

Observations

Increasing complexity of working environments in the public sector, such as remote work, virtualized organizations and digital business evolution (internally as well as with suppliers and constituents), has accelerated and expanded the need for effective and reliable IAM.

The IAM building blocks for most have been MFA and SSO. These continue to be the default solution approaches for most public organizations. This is because these also tend to be at the core of the most advanced, current public sector data protection regulation requirements.

ISG sees interest among public sector agencies in more advanced security policies, practices and technologies. However, the sector does tend to lag commercial markets in such regard. For example, passwordless-based, zero-trust and least-privilege access approaches are

gaining ground among enterprises, but not (yet) among most public agencies. As more digital business relationships emerge in the public sector, CISOs also should be investigating more advanced contextual and adaptive data analytics associated with core control capabilities. Commercial IAM, PAM and DLP solutions alike are integrating these and other advanced capabilities to ensure globally compliant protection levels.

ISG also sees continued expansion in the use of biometric identification, and some blockchain-based IAM. However, it will likely be after 2023 before widespread adoption occurs among the U.S. state and municipal government agencies. When it does, solutions offered by the Leaders in this quadrant should be more than capable.

From the more than 70 companies assessed for this study, 21 have qualified for this quadrant, with 7 being identified as Leaders.

Atos Evidian

Atos Evidian Identity Governance and Administration product suite is a comprehensive, integrated digital identity lifecycle management solution well suited to the U.S. state and municipal government organizations.

Broadcom

Broadcom's Symantec Cyber Security business unit offers endpoint, identity, information and network security software products. Symantec software is embedded into thousands of U.S. state and municipal organizations' IT environments.

IBM

IBM's Security Verify IAM suite builds around outside user/consumer IAM, inside user/workforce IAM, hybrid multicloud IAM, privileged access management (PAM), identity governance and administration, zero trust, and blockchain for digital identity and credentials.

ManageEngine

ManageEngine is the IT management software and services division of Zoho, and is expanding its services to serve state and municipal agencies, as well as other public sector entities. ManageEngine offers 12 IAM products organized into three sub-portfolios: Active Directory (AD) management, identity governance and administration and PAM.



Identity and Access Management (IAM)

Microsoft

Microsoft Azure AD offers traditional IAM features that fit public sector environments built around Microsoft Windows and Office applications. Features include SSO, Lightweight Directory services, rights management, certificate services and federation services. It also offers a combination of PAM, MFA and identity governance in on-premises, hybrid and cloud.

Okta

Okta Identity Governance IAM offers self-service identity governance and administration through a single platform. Okta's Integration Network addresses four important areas of public sector IAM: risk and fraud, customer data orchestration, data privacy and compliance, and software development lifecycle.

RSA

RSA's technologies, solutions and products are ubiquitous in cybersecurity. Its SecureID IAM has more than 1,156 product integrations, of which 128 are cloud/SaaS integrations. It also has more than 565 technology partners, of which 186 is associated to cloud.



Atos



“Atos’ strong presence in the U.S. public sector and expertise make it a Leader in the IAM space.”

Bruce Guptill

Overview

Atos is headquartered in Bezons, France, and operates in 71 countries. It has more than 111,000 employees across 220+ global offices. In FY21, the company generated \$11 billion in revenue, with infrastructure and data management as its largest segment. Atos’ Evidian Identity Governance and Administration product suite is a comprehensive, integrated digital identity lifecycle management solution well suited to the U.S. state and municipal government organizations.

Strengths

Significant, global public sector presence and experience: Atos’ global Public Sector and Defense business unit offers cybersecurity solutions and services in the U.S. public sector. This business unit comprises defense, space and homeland security; public administrations and central governments; and public community services and education operating units.

Substantial cybersecurity resources: Atos cites 6,500 cybersecurity experts and 29 security operations and innovation centers worldwide, including two major facilities in the U.S.

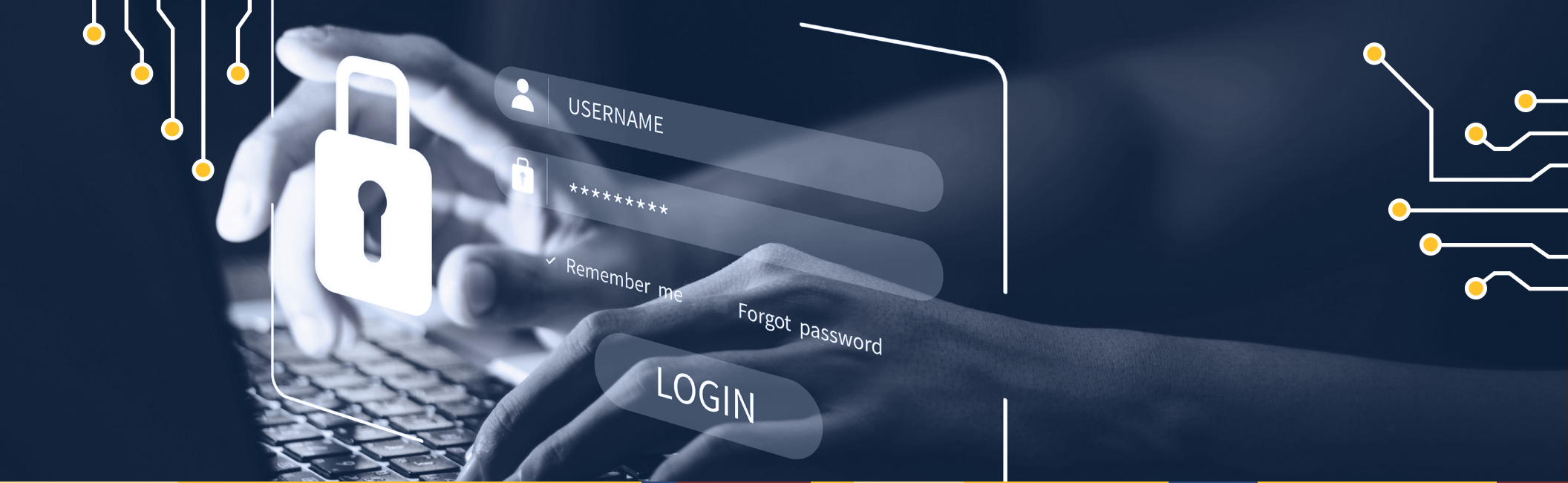
Broad and deep solution portfolio:

Atos’ overall solution portfolio includes advanced detection and response, data protection and governance, digital workplace security, hybrid cloud security, IoT and edge security, and trusted digital identity management. Its Evidian IAM-specific portfolio includes organization-wide SSO, a web access manager to optimize access from and between on-premises and cloud applications and data resources, a self-service password reset function, substantial authentication management, and a high-availability directory server capability.

Caution

Compared to other leaders in this quadrant, Atos has a relatively limited presence in the U.S. but is making significant inroads. Since 2020, ISG has seen a significant increase in Atos’ U.S. public sector investment and activity.





Data Leakage / Loss Prevention (DLP) and Data Security

Who Should Read This

This report is relevant to enterprises across the public sector in the U.S., for evaluating providers offering solutions that integrate multiple features, addressing security concerns arising from changes in work patterns and increased digitalization.

In this quadrant report, ISG highlights the current market positioning of data leakage/loss prevention (DLP) and data security solution providers that help mitigate the security threats for enterprises in the U.S. public sector. The report also shows how each provider addresses key challenges in the sector.

With an increase in cybersecurity threats, there is increased demand for optimized DLP solutions. It is also driven by other factors such as availability of DLP as a service, DLP capabilities extending to the cloud, and the growing need for advanced threat protection against these data breaches. The need to meet regulatory and compliance requirements and the increasing shift of data to public and private clouds has prompted the adoption of DLP solutions.



Chief information security officers

should read this report to understand how DLP solution providers address the significant challenges of compliance and security while maintaining a seamless experience for enterprise clients



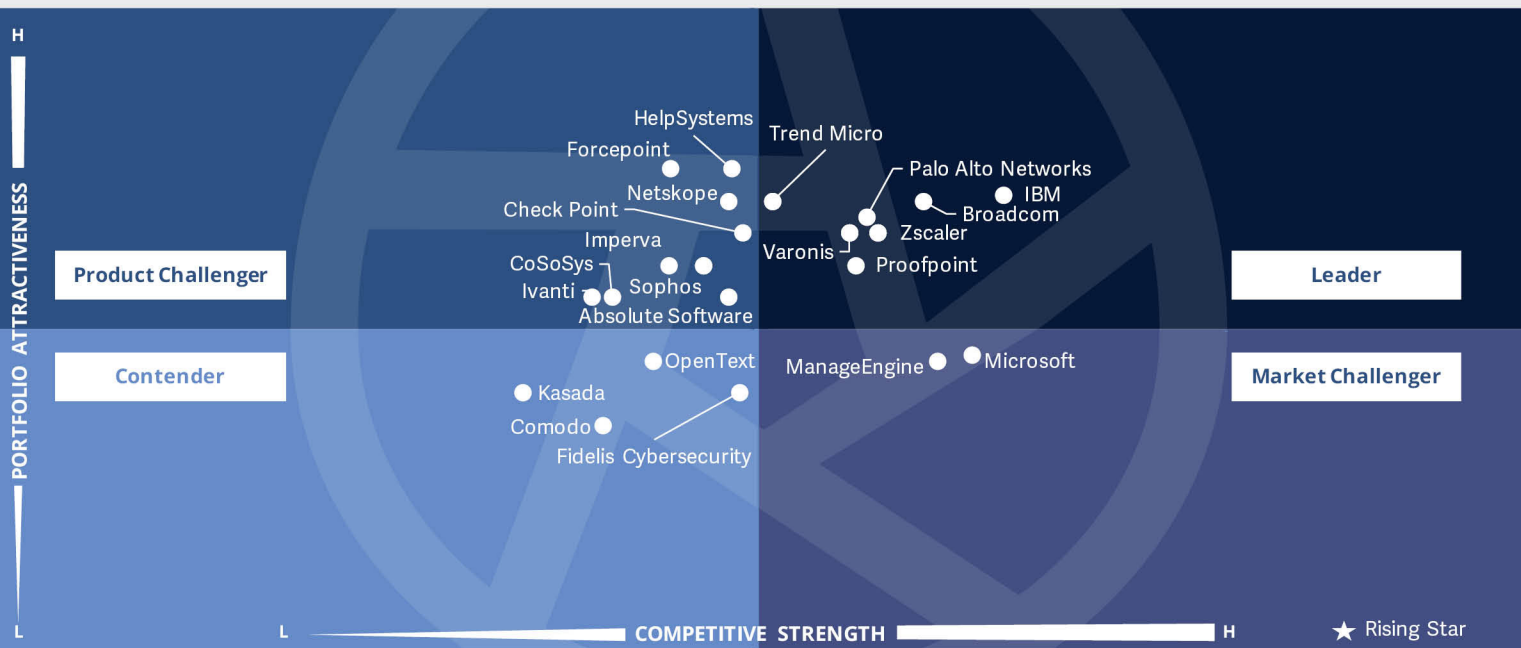
Chief executive officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



Chief data officers and data privacy officers

should read this report to understand how providers offer information protection and privacy, information governance, data quality and data lifecycle management





DLP solutions identify and monitor sensitive data and **prevent data leakage by monitoring and managing data access and use.** The most desired characteristics include data identification, policy enforcement, traffic monitoring and regulatory-plus-policy compliance enforcement.

Bruce Guptill



Definition

Data Leakage/Loss Prevention (DLP) and Data Security vendors and solution providers are characterized by their ability to offer proprietary software and associated services. This quadrant also includes Software as a Service based on proprietary software. Pure service providers that do not offer a DLP product, based on proprietary software are not included here. DLP solutions are offerings that can identify and monitor sensitive data, provide access to only authorized users and prevent data leakage. Vendor solutions in the market are characterized by a mix of products, capable of providing visibility and control over sensitive data residing in cloud applications, endpoints, networks and other devices.

These solutions should be able to identify sensitive data, enforce policies, monitor traffic and improve data compliance. They are gaining considerable importance

because it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile, that are used to store data is increasing in companies. These are mostly equipped with an Internet connection and can send and receive data without passing it through a central Internet gateway. The devices are supplied with a multitude of interfaces, such as USB ports, Bluetooth, wireless local area network (WLAN) and near-field communication (NFC), which enable data sharing. Data security solutions protect data from unauthorized access, disclosure or theft.

Eligibility Criteria

For our assessments in this report, DLP offerings should be based on proprietary software and not on a third-party software, and the vendor must have measurable presence in the designated market.

The solution should be offered with adequate standard management support, including, but not limited to, reporting, policy controls, installation and maintenance and advanced threat detection functionalities.

Further, DLP solutions considered should be capable of the following (among other capabilities):

1. Supporting DLP across any architecture such as the cloud, network, storage or endpoint
2. Handling sensitive data protection across structured or unstructured data, text or binary data



Observations

As cloud-based applications, systems and data become the de facto IT standard for public sector. As data privacy regulations evolve, more data needs to be protected for (and from) more users in more locations for more reasons. DLP solutions use business rules to classify and protect data so that users cannot accidentally, or maliciously, share it.

The most effective DLP solutions enable the following:

- **Classifying data by content and context:** Associating data with its source application, relevant data store and/or the user who created the data enables excellent visibility for monitoring and control.
- **Classifying risk by context and location:** Robust DLP solutions interpret data mobility, including when and where it might be at risk (e.g., at endpoints or attached to messages).
- **Monitoring data behavior:** Effective DLP solutions monitor not only where data is and where it has been, but how it is being used at each location.
- **Developing controls, training, adapting and communicating:** Top solutions and providers enable robust data controls that are readily implemented and adapted to changing work environments. They also provide strong means of communicating these controls to users, including how to adapt to control changes. Solutions that prompt and guide users and managers regarding changes – not just warn or prevent use without guidance – are the most effective.
- **Phasing/staging control implementations:** Beginning with starter data sets and work environments is usually preferable to a big bang type of implementation. Training and communication are important here as well.

From the more than 70 companies assessed for this study, 26 have qualified for this quadrant, with 7 being identified as Leaders.

Broadcom

Broadcom's Symantec Cyber Security business unit offers endpoint, identity, information and network security software products, including market-leading DLP. Broadcom/Symantec software is embedded into thousands of U.S. state and municipal organizations' IT environments.

IBM

IBM's deep U.S. public sector presence reaches from small city governments through hundreds of state agencies to complex federal systems. IBM's core DLP offering is its Guardium data protection software.

Palo Alto Networks

Palo Alto Networks' U.S. public sector presence builds around edge, IoT and networked IT. Its primary offering in this quadrant is its cloud-based Enterprise DLP. The solution is engineered to work within and between customers' on-premises, public and private cloud, and mobile environments.



Data Leakage/Loss Prevention (DLP) and Data Security

Proofpoint

Proofpoint's Enterprise DLP solution monitoring, analysis and reporting emphasize context involving user behavior, content, location and threats. It adopts what it calls "people-centric insight" into data loss prevention. The company offers DLP solutions for U.S. federal, state and municipal government agencies.

Trend Micro

Trend Micro's Integrated DLP is part of the company's multifaceted data protection portfolio, which includes endpoint encryption, DLP and email encryption. It seeks to ensure broad coverage of interconnected data protection across endpoints, email, web, cloud storage, SaaS applications and mobile devices.

Varonis

Varonis' U.S. public sector presence includes federal, state, and municipal government agencies and higher education institutions. The company's DLP is enabled and supported via multiple offerings, including Varonis' DatAdvantage, DatAlert, DatAdvantage Cloud, and Data Classification Engine software and services.

Zscaler

Zscaler's Government Cloud portfolio (including IAM) is FedRAMP-authorized and designed to enable lower-cost and simplified security management in a user-friendly manner. The company serves several U.S. public sector clients, including government agencies, defense/military and higher education institutions.





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.



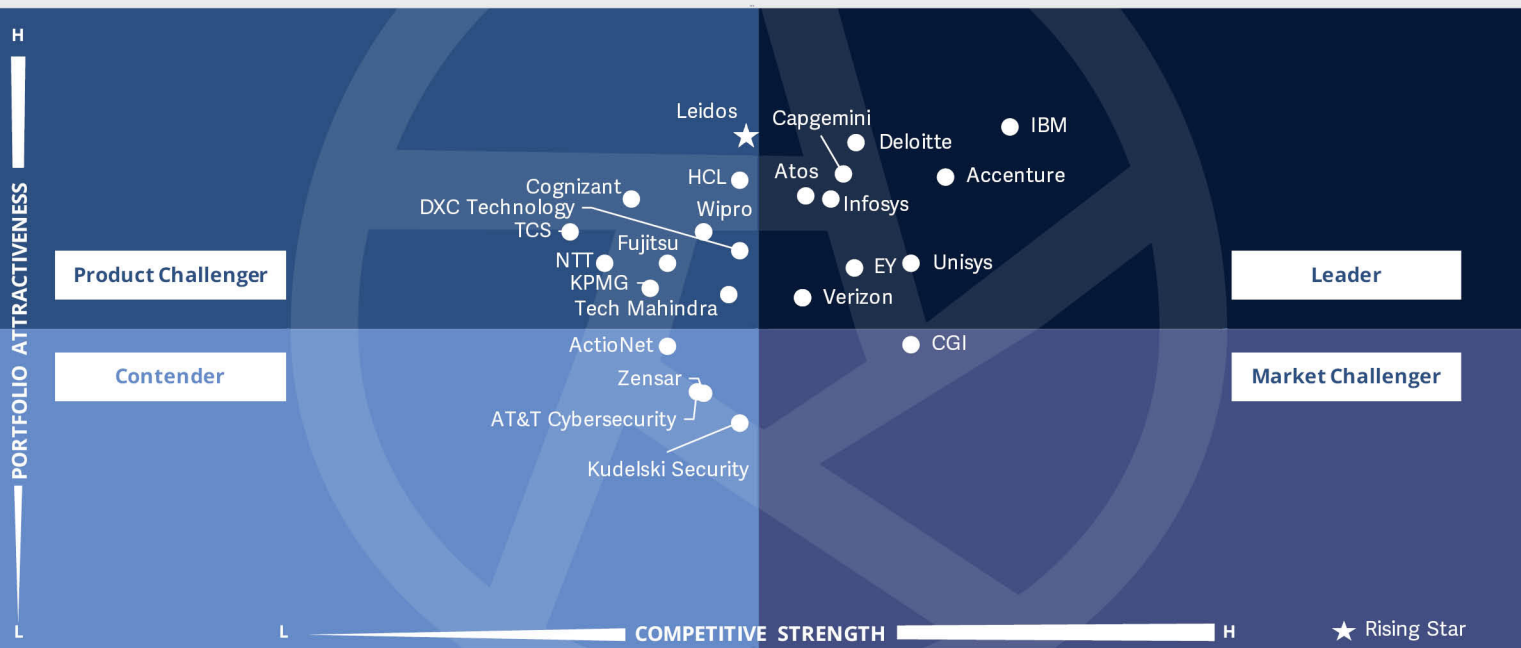
Chief strategy officers should read this report to understand the relative positioning and capabilities of service providers and collaborate with them to develop effective cybersecurity services. Also, this report can be

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.





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



Technical Security Services

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.



Technical Security Services

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 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.





“Atos’ growing presence and strong expertise make it a Leader in the TSS space.”

Bruce Guptill

Atos

Overview

Atos is headquartered in Bezons, France, and operates in 71 countries. It has more than 111,000 employees across 220+ global offices. In FY21, the company generated \$11 billion in revenue, with infrastructure and data management as its largest segment. Atos’ U.S. public sector offerings are part of its Public Sector and Defense business unit.

Strengths

Extensive experience and strong presence in the public sector: In addition to significant presence in the federal government and defense sectors, Atos’ U.S. public sector cybersecurity practice areas include state and local/municipal government, education and public safety. Globally, Atos supports several public sector client organizations.

Cyber Recovery ransomware platform: Released in 2021, Atos’ Cyber Recovery end-to-end platform enables clients to quickly recover from ransomware and other kinds of destructive cyberattacks. The platform’s technologies and

services help clients identify critical data assets and automate the protection of recovery copies within a cyber vault.

Substantial cybersecurity resources: Atos has more than 6,500 cybersecurity experts and 29 security operations and innovation centers worldwide, including two major facilities in the U.S.

Strong network of partners: Atos’ ecosystem of technology and solution partners enable relatively rapid cybersecurity technology integrations for traditional and nontraditional use cases.

Caution

Atos does not offer administrator and user training or field services teams for its security services. Also, the company does not offer TSS for DLP and associated data security.





Strategic Security Services

Who Should Read This

This report is relevant to enterprises across industries in the U.S public sector for evaluating providers offering services that integrate multiple features that address security concerns arising from changing work patterns and increasing digitalization.

In this quadrant, ISG focuses on the current market positioning of providers of strategic security services that help mitigate security threats for enterprises in the U.S public sector. It also highlights how each provider addresses the key challenges.

Strategic security services help organizations build security programs that are relevant to business needs and have a lasting impact. Recent cyberattacks on the U.S. public sector have increased the demand for strategic security services because they enable federal agencies to

respond to incidents when or before they occur. Organizations in the U.S. public sector are seeking services that augment security actions and minimize incidents.



Chief information security officers

should read this report because it gives a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of immediate threats and the security capabilities needed to combat them, thereby assisting in making strategic decisions on these security concerns. This report also provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.



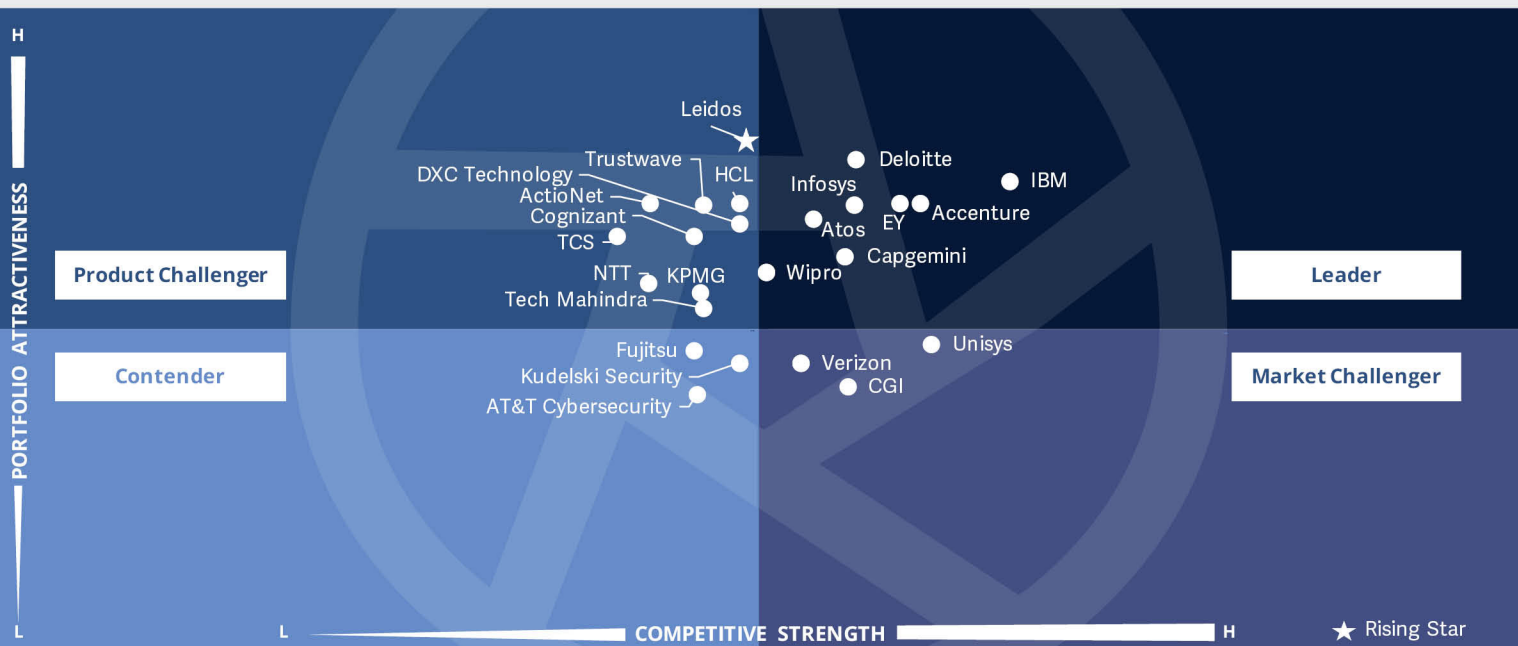
Chief technology officers should read this report to stay apace with the changes in the security landscape of

the U.S. public sector. In addition to determining strategic objectives and creating security platforms to meet marketing needs..



Chief strategy officers should read this report because it examines the relative positioning and capabilities of strategic security service providers in the U.S. public sector. It helps an agency determine its vision and strategy to deal with the growing demand for security in this sector. Additionally, it supports decision-making on collaborations, partnerships and cost-reduction initiatives





Strategic security services provide public sector agencies with immediate and future vision of needs and the expertise to execute upon that vision. **They blend technology and sector knowledge and experience** to frame effective, adaptive cybersecurity strategies.

Bruce Guptill



Definition

This quadrant examines services and providers of Strategic Security Services (SSS) 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, SSS include 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. Service providers should demonstrate abilities in SSS areas such as evaluation, assessments, vendor selection, architecture consulting and risk advisory.

3. Not exclusively focused on proprietary products.
4. Execution of security consulting services using frameworks will be an advantage.

Authorized by vendors to distribute and support security solutions.



Observations

For public sector clients, strategic security services (SSS) are the most important cybersecurity-related services over the long term. Public sector organizations today are pursuing solutions and platforms with a growing sense of urgency. While planning and assessment of course occurs, ISG sees a lack of strategic vision among buyers. Clients seeking immediate improvements tend to make tactical decisions without enough assessment of the strategic costs and other implications.

SSS providers must be able to conceptualize, optimize and frame hundreds of technologies within a broad scope of use cases. To provide a reasonable strategic vision and to execute upon that, SSS providers need to demonstrate in-depth technical expertise, backed by dedicated internal cybersecurity resources and an extensive network of technology partners,

including academia and external security researchers. The knowledge generated by such teams enables innovation, adaptation and application of advanced analytics and automated intelligence, and efficient development of cybersecurity software, cloud platforms, and digital identity, risk and threat operations services, as well as post-breach forensic investigation.

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's strategic cybersecurity consulting practice spans all significant areas assessed by ISG, including identity and governance, cloud/datacenter, industrial and IoT, endpoint and mobile

security, network security, pervasive and predictive security, SIEM, workplace security, SOAR, and OT security.

Atos

Atos is one of the Leaders whose SSS portfolio includes all capabilities considered in ISG's assessment: evaluation and maturity assessment; strategy consulting and roadmap; vendor selection, architecture review and assessment; technology and innovation management; security audits, compliance and risk advisory; security assessments (penetration testing); awareness and training; cyber forensics and data recovery; and cyber policy and operating model development.



Capgemini's wide-ranging recent SSS portfolio investments include DevSecOps, advanced cloud security (including

integration with its Cloud Infrastructure Services), zero trust and SASE, identity management in decentralized environments, planning for converged IT/OT environments and operations, and advanced data security, privacy and compliance.

Deloitte

Deloitte has more than 8,600 dedicated cyber risk service practitioners, which help its combined proprietary and partner-delivered technologies surpass most clients' cybersecurity needs. Its Cybersecurity Intelligence Center Network offers prevention, detection and containment, and remediation and recovery.



Strategic Security Services

EY

EY's next-generation security operations and response services complement its deep portfolio of consulting to implement the next-generation security operations. Its services are backed by more than 20 years of experience and global delivery capabilities. The company has 63 global security centers and more than 7,000 security practitioners in 150 countries.

IBM

IBM focuses on threat management; network protection services; endpoint security; security strategy, risk, and compliance; IAM; and data and application security. Its Security Command Center provides immersive simulations for response and resilience planning and management. Its Hacker Lab allows cybersecurity experts to improve techniques, tools and strategies.



Infosys' SSS approach includes a strong portfolio including all types of services considered as essential by ISG in our assessment, complemented with a unique emphasis on simplified metrics and analysis that enable improved vision into and across complex cybersecurity environments.



Wipro significantly advanced its strategic cybersecurity consulting base through its recent acquisition of Texas-based Edgile. Edgile provides cybersecurity strategy, transformation and risk consulting services for Fortune 500 firms. Wipro's cybersecurity strategy practices include security and risk advisory, cloud and infrastructure security, digital trust, application security, and cybersecurity platforms.

Leidos

Leidos' (Rising Star) strategic cybersecurity 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 accredited testing and evaluation in leading and emerging cybersecurity disciplines.





“Atos’ growing presence and strong expertise make it a Leader in the SSS space.”

Bruce Guptill

Atos

Overview

Atos is headquartered in Bezons, France, and operates in 71 countries. It has more than 111,000 employees across 220+ global offices. In FY21, the company generated \$11 billion in revenue, with infrastructure and data management as its largest segment. Atos’ U.S. public sector offerings are part of its Public Sector and Defense business unit.

Strengths

Comprehensive strategic services portfolio:

Atos’ SSS portfolio includes evaluation and maturity assessment; strategy consulting and roadmap; vendor selection, architecture review and assessment; technology and innovation management; security audits, compliance and risk advisory; security assessments (penetration testing); awareness and training; cyber forensics and data recovery; and cyber policy and operating model development.

Substantial cybersecurity resources: Atos has more than 6,500 cyber security experts and 29 security operations and innovation centers worldwide, including two major

facilities in the U.S.

Cybersecurity technology expertise: Like several other Leaders in this quadrant, Atos’ SSS cover a full range of cybersecurity technology areas, including identity and governance, cloud/datacenter, industrial and IoT, endpoint and mobile security, network security, pervasive and predictive security, SIEM, workplace security, SOAR and OT security.

Extensive experience and strong presence in the public sector: In addition to significant presence in the federal government and defense sectors, Atos’ U.S. public sector cybersecurity practice areas include state and local/municipal government, education and public safety.

Caution

Most Atos’ cybersecurity offerings are provided via its Digital Transformation Factory practice. Government agencies limited in their ability to transform will likely need assistance in navigating through, and negotiating with, Atos to determine and acquire optimal service configurations.





Managed Security Services

Who Should Read This

This report is relevant to public sector enterprises in the U.S. for evaluating providers offering services that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalization.

In this quadrant, ISG focuses on the current market positioning of managed security service providers that help mitigate security threats for public sector in the U.S., and how each provider addresses the key challenges.

The growing demand for optimal citizen services and ignorance about basic security measures among remote employees have made federal institutions more vulnerable to high-profile cyberattacks compared with commercial enterprises. FBI data cite a 300 percent

increase in cyberattacks since the pandemic began, and the count has been increasing.

Public sector managed security service is driven by extended detection and response (XDR), zero trust implementation and security operations centers to prevent, combat, and resolve attacks faster and more confidently. By incorporating the latest security solutions and leveraging public-private partnerships, federal agencies can stay ahead of threats and operate more securely.



Chief information security officers

should read the report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of immediate threats and the security capabilities needed to combat them, and it assists in making strategic business decisions to address existing security concerns. This report provides valuable insights on enhancing productivity and reducing complexity in security operations in the U.S. public sector.



Chief technology officers should read this report to stay apace with changes

in the U.S. public sector's security landscape. In addition to setting strategic objectives and adopting security platforms to meet marketing needs.



Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security service providers in the U.S. public sector. It helps an agency set its vision and strategy to deal with the growing demands in the public sector, while supporting decision making on collaborations, partnerships and cost-reduction initiatives.





Managed security services bind together complex and sustainable cybersecurity over time. Agencies will need help in efficiently selecting and managing changing blends of technologies, tools, software and services.

Bruce Guptill



Definition

MSS comprises the operations and management of IT 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 the best-of-breed security tools. They can handle the entire security incident lifecycle, starting from identification to resolution.

For our assessments in this report, the typical services provided include security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, IAM operation services, DLP operations, and all other operating services to provide ongoing, real-time protection without compromising on business performance.

Eligibility Criteria

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

1. Ability to provide security services such as detection and prevention; security information and event management (SIEM); security advisor and auditing support, remotely, or at the client site
2. Relevance (revenue and number of customers) as an MSS provider in the U.S.
3. Not exclusively focused on proprietary products but can manage and operate the best-of-breed security tools
4. Possess accreditations from vendors of both IT and OT security tools
5. SOCs ideally owned and managed by the provider and not predominantly by partners
6. Maintain certified staff, for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)



Observations

At the core, managed security services (MSS) are outsourced management of IT security. Until recently, this has been problematic for most U.S. public sector organizations, especially municipal and state government agencies. Such agencies often have mandates against outsourcing of what are deemed critical functions and capabilities, or at least restrictions on what may be outsourced.

Economic necessity is forcing re-examination of many such policies. Sudden changes in workforce location, disruption caused by emerging digital constituent and supplier expectations, and increased liability (and associated costs) are reshaping how, when, and how quickly public agencies consider IT security outsourcing.

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

- **Threat management:** Like any other organization, public sector entities need protection from vulnerabilities; detection and management of threats; and mitigation of same.
- **Security transformation assistance:** As digital changes outside of public sector agencies force them to consider their own digital transformation, most require assistance with transforming IT security capabilities and management as well.
- **An extended team adaptive approach:** Most public sector entities will require significant investment by their provider partners in services that augment, complement and extend the entity's own environment and staff. Adaptable

services and contracting will become standard expectations among public sector buyers.

- **Scoped, scalable managed security:** Providers will be expected to offer a broad scope of services that can be scaled in size and in complexity as clients learn their own capabilities and needs.

From more than 70 companies assessed for this study, 26 have qualified for this quadrant, with 9 being identified as Leaders.

accenture

Accenture's MSS portfolio includes managed application security, managed cloud security, managed digital identity, managed security risk, and managed detection and response. Accenture has widespread presence in the U.S. federal government environment and is making

significant investments in expanding further into state and municipal agencies as well.

Atos

Atos MSS center on managed detection and response services providing threat intelligence, threat hunting, security monitoring, incident analysis, and incident response. In addition to significant federal government and defense presence, Atos' U.S. public sector cybersecurity practice areas include state and local/municipal government, education and public safety.

Capgemini

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



Managed Security Services

Deloitte

Deloitte's U.S. public sector expertise builds on decades of financial, organizational and operational consulting knowledge. The company's MSS offerings are delivered via more than 30 SOCs worldwide. Its services span cloud, applications, IoT and Industrial control systems, identity management, and third-party risk management.

EY

EY's U.S. public sector influence builds from decades of extensive business and financial consulting presence. Its cybersecurity MSS offerings are typically paired with consulting services regarding business and organizational strategy, risk, compliance and resilience that leverage EY's extensive business- and sector-specific knowledge.

IBM

IBM is one of very few cybersecurity service providers with a dedicated MSS organization. Its MSS Division provides standard and customized managed services globally leveraging the full IBM Security Services portfolio. IBM's deep U.S. public sector presence reaches from small city governments through hundreds of state agencies to complex federal systems.

Infosys[®]

Infosys Public Services (IPS) is a subsidiary of Infosys, based in the U.S., and working exclusively with North American public sector organizations. IPS is a participating member of the National Association of State CIOs (NASCIO), enabling improved and ongoing communication and understanding of state IT organizations' changing needs.

Unisys

Unisys is one of the best-established IT providers serving state agencies and large municipalities, along with a sizable U.S. federal government presence. Unisys' managed security portfolio includes advanced endpoint protection services, security information and event management (SIEM), and security device management (SDM). The company offers unified services, supporting on-premises and multicloud environments.

Verizon

Verizon offers core MSS around four key areas: identify, protect, detect and respond, and recover. It has business units responsible for selling to, serving, and supporting U.S. state and municipal government clients; separate units support U.S. federal government agencies and higher education institutions.



Atos



“Atos’ strong portfolio and influential presence position it as a Leader in the MSS space.”

Bruce Guptill

Overview

Atos is headquartered in Bezons, France, and operates in 71 countries. It has more than 111,000 employees across 220+ global offices. In FY21, the company generated \$11 billion in revenue, with infrastructure and data management as its largest segment. Atos’ U.S. public sector offerings are part of its Public Sector and Defense business unit.

Strengths

Comprehensive MSS portfolio: Atos’ MSS offering includes services for hybrid and multicloud environments, including perimeter security, platform security, data security, trusted identities, cloud security, threat hunting, threat intelligence, vulnerability management, computer security incident response team (CSIRT) services, managed EDR, network security and managed zero-trust network access.

Intelligent managed detection and response foundation: Atos’ core MSS is a managed detection and response (MDR) service, providing threat intelligence, threat hunting, security monitoring, incident analysis and incident response. Atos’ Alsaac

AI platform enables advanced analytics on endpoints, clouds, user behavior, applications and networks.

Extensive experience and strong presence in the public sector: In addition to significant presence in the federal government and defense sectors, Atos’ U.S. public sector cybersecurity practice areas include state and local/municipal government, education and public safety.

Substantial cybersecurity resources: Atos reports more than 6,500 cybersecurity experts and 29 security operations and innovation centers worldwide, including two major facilities in the U.S.

Caution

Most Atos’ cybersecurity offerings are provided via its Digital Transformation Factory practice. Government agencies, limited in their ability to transform, will likely need assistance in navigating through, and negotiating with, Atos to determine and acquire optimal service configurations.





Appendix

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



Author & Editor Biographies

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.



Author & Editor Biographies



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.



JULY 2022

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES