ISG Provider Lens™

Cybersecurity – Solutions and Services 2023

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

BROCHURE | JANUARY 2023 | GLOBAL

Table of Contents

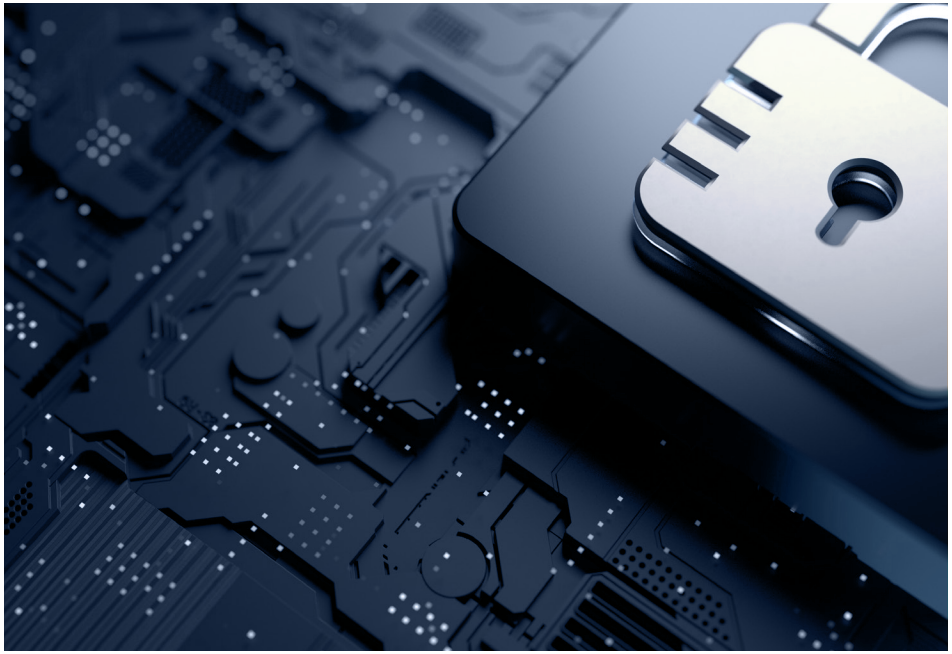
Introduction

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritized relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

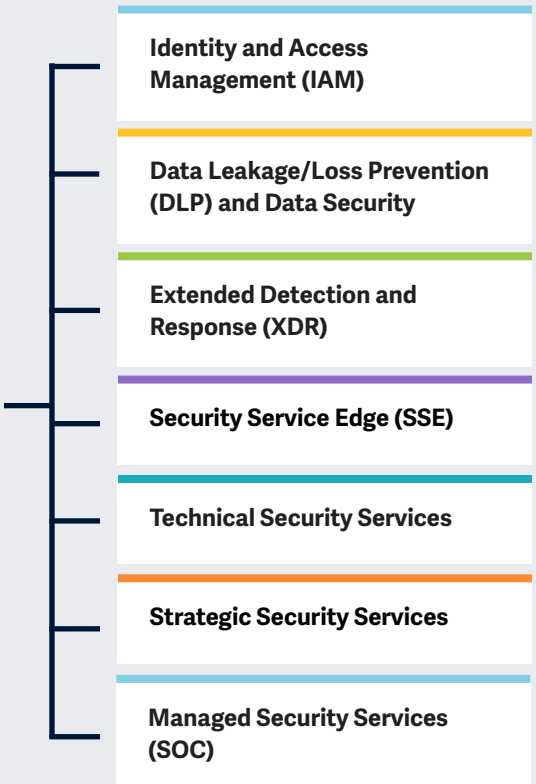
From an enterprise perspective, even small businesses understood the impact of cyber threats and realized that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident. Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of the cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

These prompted businesses to invest in capabilities such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR) and securing cloud and endpoints. The market is shifting toward integrated solutions, such as security service edge (SSE) and extended detection and response (XDR), which leverage the best tools and human expertise and are augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.



Key focus areas for Cybersecurity Solutions and Services 2023.



Simplified Illustration Source: ISG 2023

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

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on different markets, including the U.S., the U.K., Nordics, Germany, Switzerland, France, Brazil, Australia, Singapore & Malaysia and the U.S. public sector. The SSE topic will be analyzed for the global market.

Our study serves as an important decision-making basis for positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current vendor relationships and potential engagements.

Definition

IAM vendors and solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services for managing enterprise user identities and devices. This quadrant also includes SaaS offerings based on proprietary software. It does not include pure service providers that do not offer an IAM product (on-premises and/or cloud) based on proprietary software. Depending on organizational requirements, these offerings could be deployed in several ways such as on-premises or in the cloud (managed by a customer) or as an as-a-service model or a combination thereof.

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

Eligibility Criteria

1. The solution should be capable of **deployment** as an **on-premises, cloud, identity-as-a-service** (IDaaS) and a managed third-party model.
2. The solution should be capable of **supporting authentication** as a combination of **single-sign on (SSO), multi-factor authentication (MFA)**, risk-based and context-based models.
3. The solution should be capable of **supporting role-based access** and PAM.
4. The IAM vendor should be able to provide **access management** for one or more enterprise needs such as **cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications**.
5. The solution should be capable of **supporting one or more legacy and new IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM.
6. To support secure access, the portfolio should include one or more of the following – **directory solutions, dashboard or self-service management** and lifecycle management (migration, sync and replication) solutions.

Definition

The DLP vendors and solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services. This quadrant also includes SaaS solutions based on proprietary software. It does not include pure service providers that do not offer a DLP product (on-premises or cloud-based) based on proprietary software. DLP solutions can identify and monitor sensitive data, provide access for only authorized users and prevent data loss/leakage. Vendor solutions in this space include a mix of products capable of providing visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers (more than a third of data violations are from an internal source). The number of devices, including mobile devices, used to store data is increasing in companies. Equipped with an Internet connection, these devices can send and receive data without passing it through a central Internet gateway. Data security solutions protect data from unauthorized access, disclosure or theft by prioritizing, classifying and monitoring data (when at rest and in transit), while allowing organizations to report on and improve the security of their data at risk.

Eligibility Criteria

1. The DLP offering should be based on **proprietary software** and not third-party software.
2. The solution should be capable of supporting DLP **across any architecture such as the cloud, network, storage or endpoint**.
3. The solution should be capable of **handling sensitive data protection across structured or unstructured** data, text or binary data.
4. The solution should be offered with **basic management support**, including, but not limited to, **reporting, policy controls,** installation and maintenance and advanced threat detection functionalities.
5. The solution should be able to **identify sensitive data, enforce policies**, monitor traffic and improve data compliance.

Definition

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

Eligibility Criteria

1. The XDR offering should be based on **proprietary software** and not on third-party software.
2. An XDR solution needs to have two primary components: **XDR front end and XDR back end**.
3. The front end should have **three or more solutions or sensors,** including, but not limited to, **endpoint detection and response, endpoint protection platforms**, network protection (firewalls, IDPS), **network detection and response**, identity management, email security, mobile threat detection, cloud workload protection and identification of deception.
4. The solution provides **comprehensive and total coverage and visibility of all endpoints** in a network.
5. The solution demonstrates **effectiveness in blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware.
6. The solution leverages **threat intelligence**, and analyzes and offers **real-time insights on threats** emanating across endpoints.
7. The solution should include **automated response features**.

Definition

The SSE solution providers assessed for this quadrant offer cloud-centric solutions that combine proprietary software, and/or hardware and associated services, enabling secure access to cloud services, SaaS applications, web services and private applications. Vendors offer SSE solutions as an integrated security service through globally positioned points of presence (PoP) with support for local data storage that combines individual solutions such as zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS). SSE can also include other security solutions such as data loss/leakage prevention (DLP), browser isolation and next-generation firewall (NGFW) to offer secure access to applications on the cloud and on-premises.

Vendors showcase experience in satisfying local, regional and domestic laws (such as for data sovereignty) for global clients.

The network components of secure access secure edge (SASE), such as SD-WAN or micro-segmentation, are not included in this quadrant but are covered in the Network - Software Defined Solutions and Services study.

SSE solutions strongly focus on user-centricity, delivering security to end users at the edge or devices through the cloud — rather than allowing users to centrally access enterprise applications and databases — over dedicated networks. ZTNA creates exclusive connectivity between a user and an application, using context-based behavioral analysis to control access. CASB offers visibility, enforces security policies and compliance, and allows control of shadow IT cloud usage, while FWaaS and SWG prevent malicious threats and access to infected websites and applications. Typically, an SSE solution has a unified console for visibility and governance, and assesses user experience with advanced automation.

Eligibility Criteria

1. The SSE should be offered as an **integrated solution** and must have these essential components: **zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS).**
2. The above components must be **predominantly based on proprietary** software, they may **partially rely on partner solutions but cannot completely rely on third-party** software.
3. Vendors should have **globally located PoPs** to deliver these solutions.
4. The solution should be capable of **delivering SSE to both cloud and on-premises** environments (including hybrid environments).
5. The solution should exhibit **contextual and behavioral evaluations and analysis (user entity and bevavior analytics/ UEBA)** to detect and prevent malicious or suspicious intent.
6. The solution should be offered with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities.
7. The solution should be **fully and globally available**.

Definition

The Technical Security Services (TSS) providers assessed for this quadrant cover integration, maintenance and support for both IT and operational technology (OT) security products or solutions. They also offer DevSecOps services. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, SASE and others.

TSS providers offer standardized playbooks and roadmaps that aid in transforming an existing security environment with best-of-breed tools and technologies, improving security posture and reducing threat impact. Their portfolios are designed to enable the complete or individual transformation of an existing security architecture with relevant products across domains such as networks, cloud, workplace, OT, IAM, data privacy and protection, risk and compliance management and SASE, among others. The offerings also include product or solution identification, assessment, design and development, implementation, validation, penetration testing, integration and deployment. The providers also leverage sophisticated solutions that enable comprehensive vulnerability scanning across applications, networks, endpoints and individual users to uncover weaknesses and mitigate external and internal threats.

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

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

Eligibility Criteria

1. Demonstrate experience in **implementing cybersecurity solutions** for companies in the respective country.
2. **Authorized by security technology vendors** (hardware and software) to distribute and support security solutions.
3. Providers should **employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies.

Definition

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

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

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

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

Eligibility Criteria

1. Service providers should demonstrate abilities in SSS areas such as evaluation, assessments, vendor selection, architecture consulting and risk advisory.
2. Service providers should offer at least one of the above strategic security services in the respective country.
3. The ability to execute security consulting services using frameworks will be an advantage.
4. No exclusive focus on proprietary products or solutions.

Definition

The providers assessed in the Managed Security Services (SOC) (MSS (SOC)) quadrant offer services related to the operations and management of IT and OT security infrastructures for one or several customers by a security operations center (SOC). **This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools.** These service providers can handle the entire security incident lifecycle, from identification to resolution.

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximizing the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS (SOC) providers must combine traditional managed security services with innovation to fortify their clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies, infrastructure and experts skilled in threat hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI and machine learning. These sophisticated SOCs should support expert-driven security intelligence response, while offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations** and all other operating services to provide ongoing, real-time protection, without compromising on business performance. In particular, secure access service edge (SASE) is included.
2. Ability to provide security services, such as **detection and prevention; security information and event management (SIEM)** and security advisor and auditing support, remotely or at a client's site.
3. Possesses **accreditations** from security tools vendors.
4. **SOCs ideally owned and managed by the provider** and not predominantly by partners.
5. Maintains **certified staff,** for example with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

Quadrants By Region

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

Quadrants	U.S.	U.K.	Nordics	Germany	Switzerland	France	Brazil	Australia	Singapore & Malaysia	U.S. Public Sector	Global
Identity and Access Management (IAM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Data Leakage/Loss Prevention (DLP) and Data Security				✓	✓						
Extended Detection and Response (XDR)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Security Service Edge (SSE)											✓
Technical Security Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services (SOC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Schedule

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

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

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

Access to Online Portal

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

Research Production Disclaimer:

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

ISG Star of Excellence™ – Call for nominations

The Star of Excellence is an independent recognition of excellent service delivery based on the concept of "Voice of the Customer." The Star of Excellence is a program, designed by ISG, to collect client feedback about service providers' success in demonstrating the highest standards of client service excellence and customer centricity.

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

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

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

To ensure your selected clients complete the feedback for your nominated engagement please use the Client nomination section on the Star of Excellence website.

We have set up an email where you can direct any questions or provide comments. This email will be checked daily, please allow up to 24 hours for a reply. Here is the email address: ISG.star@isg-one.com

Contacts For This Study

Frank Heuer

Lead Analyst - Germany, Switzerland

Benoit Scheuber

Lead Analyst - France

David Pereira

Lead Analyst - Brazil

Deepika B

Research Analyst

Gawtham Kumar

Lead Analyst - U.S.

Dr. Maxime Martelli

Lead Analyst - France

Phil Hassey

Lead Analyst - U.S. Public Sector

Gabriel Sobanski

Research Analyst

Arun Kumar Singh

Lead Analyst - U.K., Nordics

Andrew Milroy

Lead Analyst - Australia

Bhuvaneshwari Mohan

Research Analyst

Ridam Bhattacharjee

Project Manager

ISG Provider Lens Advisors Involvement Program

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

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

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

The QCRT advisors:

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

ISG Advisors to this study

Doug Saylors

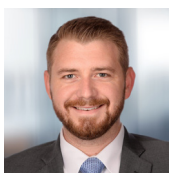
Co-lead, ISG Cybersecurity

Anand Balasubramanium

Senior Consultant

Roger Albrecht

Co-lead, ISG Cybersecurity



Alex Perry

Director

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

* Rated in previous iteration

Solution Providers

Absolute Software*
Acronis*
Akamai*
Aruba
Attivo Networks*
Avatier*
Axis Security
Barracuda Networks
BAYOONET*
Beta Systems*
Bitdefender*
Blackberry (Cylance)*
Brainloop*
Broadcom*
Cato Networks
Check Point*
Cisco*
Cloudflare*
CoSoSys*
CrowdStrike*
CyberArk*
Cybereason*
DriveLock*
Elastic
Ergon*
Ericom Software
ESET*
Fidelis Cybersecurity*
FireEye*
Forcepoint*
ForgeRock
Fortinet
GBS
Google
HelpSystems
IBM
iboss
Ilantus Products*
Infinite Networks
itWatch*
Kaspersky*
Lookout*
Matrix42*
Menlo Security
Micro Focus*
Microsoft*
Netskope*
Nevis*
Nexus
NordLayer
OGiTiX*
Okta*
Omada*
One Identity (OneLogin) *
Open Systems*
OpenText*
Oracle*
Palo Alto Networks*
Perimeter 81

Invited Companies

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

* Rated in previous iteration

Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
Senhasegura*
SentinelOne*
SolarWinds*
Sophos*
Tehtris
Thales*
Trellix*
Trend Micro*
United Security Providers*
Varonis*
Versa Networks
VMWare Carbon Black*
WithSecure
Zscaler

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

* Rated in previous iteration

Service Providers

Accenture*
Adarma
Alice&Bob.Company*
All for One Group*
AT&T Cybersecurity*
Atea
Atos*
Avanade Inc.
Aveniq*
Axians*
Bechtle*
Booz Allen Hamilton
Bridewell Consulting
BT Security
CANCOM*
Capgemini*
CGI*
Cognizant*
Computacenter*
Controlware*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
DXC Technology*
Edge UOL*
EY*
Fujitsu*
Getronics*
glueckkanja-gab*
Happiest Minds*
HCLTech*
IBM*
iC Consult*
Indevis*
InfoGuard*
Infosys*
Insight UK
ISH Tecnologia
ISPIN*
KHIPU Networks
KPMG*
Kudelski Security*
Logicalis*
LTIMindtree
Lumen*
Mphasis*
MW Group
NCC Group*
Netic
Nixu*
NTT*
Orange Cyberdefense*
Performanta
Persistent Systems*
Proact IT Group
PwC*
Sapphire
Satisnet

Invited Companies

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

* Rated in previous iteration

Secureworks*
SecurityHQ
Siemens
Six Degrees
Softcat
Sopra Steria*
Stefanini
Sunny Valley
suresecure*
Swisscom*
Syntax*
Talion
Talion
Tata Communications*
Tata Consultancy Services (TCS) *
Tech Mahindra*
Telia Cygate
Tempest*
terreActive*
Tesserent*
Thales*
Tietoevry*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
UST Global
Venzo Group
Verizon*
Wipro*
Zensar*

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens research, please visit this webpage.

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ISG Provider Lens™

JANUARY, 2023

REPORT: CYBERSECURITY - SOLUTIONS AND SERVICES