ISG Provider Lens™

Cybersecurity – Solutions and Services

Analyzing the cybersecurity market, comparing provider portfolio attractiveness and competitive strengths

BROCHURE | JANUARY 2024 | AUSTRALIA, BRAZIL, FRANCE, GERMANY, SWITZERLAND, U.K., U.S., U.S. PUBLIC SECTOR AND GLOBAL

Table of Contents

Cybersecurity in the Age of AI

The current cybersecurity landscape is dynamic, with changes occurring rapidly due to emerging threats, technological advancements, and evolving regulatory environments.

The year 2023 could be termed as tumultuous from a cybersecurity perspective; the year saw significantly increased sophistication and severity in the attacks. Enterprises responded by increasing their investments in cybersecurity and prioritizing relevant initiatives to prevent attacks and improve their security posture. Learnings from prior attacks in 2022 led to executives and businesses of all sizes and across industries investing in measures countering cyberthreats. AI brings both challenges and opportunities to cybersecurity, offering automation for analysis and detection while posing risks of bias and misuse.

From an enterprise perspective, even small businesses realized their vulnerability to cyber threats, fueling demand for (managed) security and cyber resiliency services that would enable recovery and operation restoration post-cyber incidents. Therefore, service providers and vendors are offering services and solutions that help enterprises ensure recovery and business continuity.

Security services providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats, understanding the transformative impact of technologies such as AI and ML, and staying attuned to evolving regulatory frameworks on data protection, such as NIS-2, in the European Union.

Cybercriminals exploited large-scale vulnerabilities, persistently using ransomware to disrupt business activities, specifically healthcare, supply chain and public sector services.

Consequently, businesses started to invest in solutions such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR), and cloud and endpoint security. 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 augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.

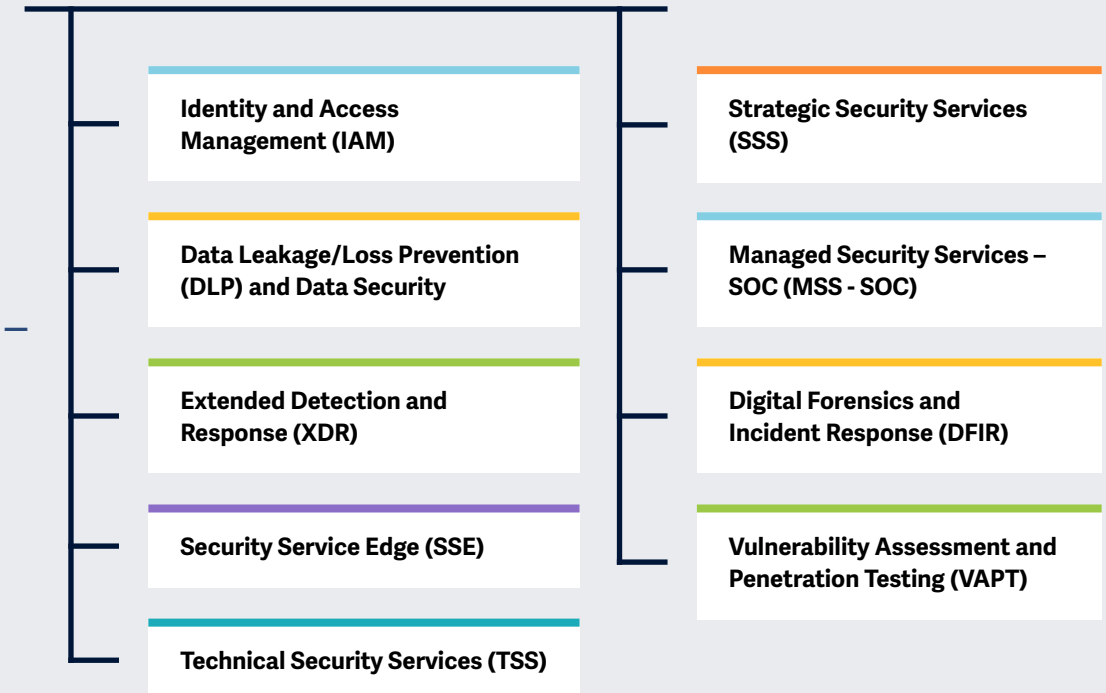
Cybersecurity Services: 2024

Quadrants	Attributes		Application Security	Cloud and Data Center Security	Network Security	Data Security	Endpoint Security
Strategic Security Services	Security Consulting	Compliance and Risk Advisory Services					
	Security Assessments and Audits	Awareness and Training					
Technical Security Services	Security Solutions Implementation	Architecture and roadmap					
	Expertise and Technical Support	Security Tools and Technologies Maintenance					
Managed Security Services - SOC	Security Monitoring	Advanced Security Analytics					
	Orchestration and Automation	Managed Detection and Response					
Digital Forensics and Incident Response	Response Planning	Investigation					
	Analysis	Incident Mitigation					
Vulnerability Assessment and Penetration Testing	Vulnerability Detection	Analysis					
	Reporting	Escalation					

Cybersecurity Solutions: 2024

Quadrants	On-Premises or SaaS Offering based on Proprietary Software		Application Security	Cloud and Data Center Security	Network Security	Data Security	Endpoint Security
Identity and Access Management	Identity Management	Privileged Access Management					
	Access Management	Zero Trust					
Extended Detection and Response	Unified Endpoint Management	Network Detection and Response					
	Threat Intelligence	Endpoint Detection, Protection and Response					
Security Service Edge (SSE)	Zero Trust Network Access	Cloud Access Security Broker					
	Secure Web Gateways	Firewall as a Service					
Data Leakage/Loss Prevention (DLP) and Data Security	Data Identification and Classification	Data Protection					
	Data Monitoring	Enforce Policies					

Key focus areas for Cybersecurity – Solutions and Services.



Simplified Illustration Source: ISG 2024

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

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness
- Focus on different markets, including the U.S., the U.K., Germany, Switzerland, France, Brazil, Australia and the U.S. Public Sector. The SSE and the XDR topics will be analyzed for the global market.
- To consider country-specific characteristics in this global study, XDR's analysis extends to Brazil, while Germany exclusively analyzes DLP. The introduction of DFIR will be piloted in the U.S. and France, and the new topic of Vulnerability Assessment and Penetration Testing will debut in Brazil.

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 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 excludes 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, customer-managed clouds or as-a-service models or a combination thereof.

IAM solutions aim to manage (collect, record and administer) user identities and related access rights and 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 offer additional functionalities for social media and mobile use to address specific security needs beyond traditional web and contextual rights management. This quadrant also includes machine identity management.

Eligibility Criteria

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

Data Leakage/Loss Prevention (DLP) and Data Security

Definition

The DLP solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services, including SaaS solutions. This quadrant **excludes 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 providing visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

These solutions are gaining considerable importance due to companies' escalating challenges in controlling data movements and transfers, with over a third of data violations originating internally. The number of devices, including mobile devices, used for data storage amplifies these concerns. Internet connectivity allows these devices to exchange data without passing through a central 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 data security.

Eligibility Criteria

1. Offer DLP solutions based on **proprietary software** and not third-party software
2. Demonstrate capability of supporting DLP **across any architecture, such as the cloud, network, storage or endpoint**
3. Showcase ability of **handling sensitive data** protection **across structured or unstructured**, text or binary data
4. Offer solution with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance and advanced threat detection functionalities
5. Offer solution capable of **identifying sensitive data, enforcing policies**, monitoring traffic and improving 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 weak individual signals, to enable accurate detections. XDR solutions consolidate and integrate multiple products, providing comprehensive security for workspaces, networks and workloads. Typically, XDR solutions are aimed at vastly improving visibility and context understanding of identified threats across the enterprise. Characteristics of these solutions include telemetry and contextual data analysis for detection and response. XDR solutions comprise multiple products integrated into a single pane of glass for sophisticated viewing, detection and response capabilities. Their high automation maturity and contextual analysis offer tailored responses to affected systems, prioritizing alerts based on severity against known reference frameworks. This quadrant excludes **pure service providers that do not offer an XDR solution based on proprietary software**. XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expenses. They are particularly suitable for security operations teams struggling to manage diverse solution portfolios or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

Eligibility Criteria

1. Offer XDR solutions based on **proprietary software** and not on third-party software
2. Ensure an XDR solution has two primary components: **XDR front end and XDR back end**
3. Offer front end with **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. Provide solution with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solution capable of **blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware
6. Provide solution using **threat intelligence** and **real-time insights on threats** emanating across endpoints
7. Offer solution including **automated response features**

Definition

The SSE solution providers assessed for this quadrant offer cloud-centric solutions combining proprietary software or hardware and associated services, enabling secure access to the cloud, SaaS, 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 secure access to both cloud and on-premises applications.

Vendors showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients.

This quadrant excludes the network components of secure access service edge (SASE), such as SD-WAN, which are covered in the ISG Provider Lens™ Network – Software Defined Solutions and Services 2024 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 access enterprise applications and databases — over dedicated networks centrally. ZTNA creates exclusive connectivity between users and applications, using context-based behavioral analysis to manage access. CASB offers visibility, enforces security policies and compliance, and controls 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, with advanced automation to assess UX.

Eligibility Criteria

1. Provide SSE as an **integrated solution** with **zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**
2. Offer solutions **predominantly based on proprietary** software, they may **partially rely on partner solutions** while avoiding **complete dependency on third-party** software
3. Maintain **globally located PoPs** to deliver these solutions
4. **Deliver SSE to both cloud and on-premises** environments (including hybrid environments)
5. Exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/UEBA)** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **globally availability of the solution**

Definition

The TSS providers assessed for this quadrant cover integration, maintenance and support for both IT and OT security products or solutions. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security and 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 complete or individual transformations of existing security architectures 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.

TSS providers invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio scope. This quadrant also encompasses classic managed security services provided without a security operations center (SOC).

This quadrant examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other vendors.

Eligibility Criteria

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

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting, and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with 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 vCISO (virtual Chief Information Security 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, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. **Offer at least one of the above** strategic security services in the respective country
3. Provide **security consulting services using frameworks**
4. **No exclusive focus** on **proprietary products** or solutions

Definition

The providers assessed in the MSS-SOC quadrant offer services related to the continuous monitoring of IT and OT security infrastructures and management of IT infrastructure 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 response.

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional managed security services with innovation to fortify 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 and infrastructure. They must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, 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** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, Security Information and Event Management (SIEM) services**, security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. Manage own SOCs
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models

Digital Forensics and Incident Response (DFIR)

Definition

Providers assessed in the DFIR quadrant offer services related to threat response activities while preserving evidence against attackers.

This quadrant examines service providers that provide proven DFIR techniques, methodologies and are able to work with best-of-breed tools to respond to cybersecurity incidents. DFIR involves the identification, investigation, containment, and remediation of cybersecurity incidents. The escalation in frequency and severity of cybersecurity incidents has added to the adoption of DFIR services. Service providers should showcase in-depth and hands-on capabilities in addressing digital forensics, electronic discovery, predefined criteria-based triage, timeline analysis, log analysis, malware analysis and artifact examination. Following a breach, DFIR plays a vital role in uncovering data loss and damage specifics.

DFIR services help establish effective threat response, utilizing sophisticated incident response playbooks and forensics to understand threat actor behavior and root causes. DFIR providers should possess experience in assisting enterprises with litigation support for insurance claims and post-breach regulatory audits. They are adept in using in-house and third-party tools such as security information and event management (SIEM), security orchestration, automation and response (SOAR), endpoint detection and response (EDR), and extended detection and response (XDR).

Eligibility Criteria

1. Must have a **dedicated incident response team** (CERT or CSIRT) of experts with relevant certifications such as GCFA, GCFE and CISSP, showcasing their expertise and commitment to maintaining industry standards
2. Possess experience and expertise in **handling a variety** of SIEM, SOAR, EDR and XDR solutions
3. The DFIR services will **not only identify the breach** but also create the timeline, root cause and impact of the breach
4. **Possess capabilities** in malware analysis, ransomware decryption and data recovery
5. Demonstrate **partnership** with relevant product vendors and managed security services providers to gather threat intelligence, dark web monitoring, and SOC capabilities to mitigate advanced persistent and sophisticated threats

Vulnerability Assessment and Penetration Testing (VAPT)

Definition

Providers of VAPT services are characterized by offering refined technical skills that require a high degree of updating, not only on known and daily discovered gaps, but also on increasingly elaborate approaches and mechanisms to circumvent established lines of defense.

The year 2023 was highlighted by the access to generative AI tools, allowing an unlimited number of people the ability to identify and exploit vulnerabilities in technology assets, especially those directly exposed to the internet. In addition, there has been a proliferation of incidents involving ransomware, with recurring cases, highlighting the need for continuous perimeter protection, no longer limited to one-off annual or six-monthly assessments.

Considering the current frequency of updates to services exposed to the Internet by companies, the insertion of continuous vulnerability detection services (pre- and post-entry into production) has become fundamental to the cyber security strategy and, together with the other trends, makes up the challenge and mission of the suppliers in this quadrant.

The scenario is that of a fast-paced race against orchestrated threats with increasing methodological and technical sophistication and high destructive power. Suppliers in this quadrant must therefore offer suitable antidotes in addition to the traditional approach, which is now recognized as insufficient for mitigating risks and impacts.

Eligibility Criteria

1. Have specialized in-house teams capable of **rigorously assessing vulnerabilities and indicating solutions** for removing flaws and/or gradually reducing their severity, based on concrete evidence of attack vectors
2. Offer services that include **black box, grey box and white box approaches**, capable of assessing, for example, web applications, mobile devices, internal networks, cloud, APIs, IoT and other exposed assets
3. Use methods such as **DAST, SAST and Pentesting** of specific objectives using manual and/or automated tools for service delivery
4. **Recognized industry standards** such as SOC 2, ISO27001, NIST 800-53, PCI-DSS and HIPPA must be used and evidenced when indicating security flaws
5. Offer **retesting, specialized support and mechanisms** for monitoring corrective actions, dynamically reflected in the updating of the risk and severity matrix (exposure to remaining vectors)

Quadrants by Region

As part of this ISG Provider Lens™ quadrant study, we are introducing the following Nine quadrants on Cybersecurity - Solutions and Services 2024:

Quadrant	U.S.	U.K.	Germany	Switzerland	France	Brazil	Australia	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 (TSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services – SOC (MSS-SOC)	✓	✓	✓	✓	✓	✓	✓	✓	
Digital Forensics and Incident Response (DFIR)	✓				✓				
Vulnerability Assessment and Penetration Testing (VAPT)						✓			

Schedule

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

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

Please refer to the link to view/download the ISG Provider Lens™ 2024 research agenda.

Access to Online Portal:

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

Research Production Disclaimer:

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

ISG Star of Excellence™ – Call for nominations

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

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

Gowtham Kumar

Lead Analyst – U.S.

Bhuvaneshwari Mohan

Lead Analyst – U.K.

Benoit Scheuber

Lead Analyst – France

Dr. Maxime Martelli

Lead Analyst – France

Craig Baty

Lead Analyst – Australia

Christian Horst Alves Reis

Lead Analyst – Brazil

Phil Hassey

Lead Analyst – U.S. Public sector

Monica K

Research Analyst

Contacts For This Study

Bhuvaneshwari Mohan

Research Analyst

Sandya Kattimani

Research Analyst

Bruno Nakazone

Research Analyst

Shreemadhu Rai B

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 and the 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.

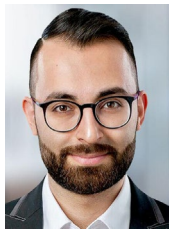
The QCRT advisors:

- 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

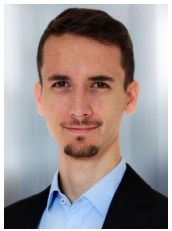
Doug Saylors

Partner, Co-lead ISG Cybersecurity



Reza Memarian

Principal Consultant Cybersecurity



Anas Barmo

Senior Consultant Cybersecurity

Joyce Harkness

Director Cybersecurity

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*
Alice&Bob.Company*
Aruba*
Atos*
Avatier*
AWS*
BAYOONET*
Brainloop*
Broadcom*
Cato Networks*
Check Point*
Cipher*
Cisco*
CoSoSys*
Cross Identity*
CrowdStrike*
CyberArk*
Cybereason*
Cynet*
Darktrace*
DriveLock*
Elastic Security
EmpowerID*
Ergon*
Ericom Software*
eSentire*
ESET*
E-TRUST*
Fidelis Cybersecurity*
Fischer Identity*
Forcepoint*
ForgeRock*
Fortinet*
Fortra
FusionAuth*
GBS*
GoCache*
Google*
HarfangLab*
Hashicorp*
HCLTech*
Heimdal Security*
Huge Networks*
IBM*
iboss*
Imprivata*
IN Groupe*
Infinite Networks*
itWatch*
Kasada*
Kaspersky*
LastPass*
Logpoint*

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

Lookout*
ManageEngine*
Mandiant*
Matrix42*
Microland*
Microsoft*
Netskope*
NetWitness*
Nevis*
Nok Nok Labs*
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Oracle*
Orange Cyberdefense*
Palo Alto Networks*
Perimeter 81*
Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
SecureAuth*
Secureworks*
senhasegura*
SenseOn*
SentinelOne*
SilverSky*
Skyhigh Security*
Solarwinds*
Sophos*
Systancia*
TEHTRIS*
Tenfold
Thales*
Trellix*
Trend Micro*
Unisys*
United Security Providers*
Varonis*
Versa Networks*
VMware*
Wallix*
WatchGuard*
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*
ActioNet*
Adarma*
Advens*
Agility*
Airbus CyberSecurity*
All for One Group*
ASG*
AT&T Cybersecurity*
Atos*
Aveniq*
Avertium*
Axians*
Bechtle*
Beta Systems*
BeyondTrust*
Bitdefender*
BlackBerry*
BluePex*
BlueVoyant*
BT*
CANCOM*
Capgemini*
CGI*
Cipher*
Cirion*
Cisco*
Claranet*
Cloudflare*
Comline
Compugraf*
Computacenter*
Conscia*
Controlware*
Critical Start*
CTM*
CyberSecOp*
Cyderes*
Data#3*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
ECSC*
Edge UOL*
EY*
FastHelp*
Getronics*
glueckkanja-gab*
HackerSec*
Happiest Minds*
HCLTech*
HiSolutions*
IBLISS*
IBM*

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

iC Consult*
indevis*
InfoGuard*
Infosys*
Integrity360*
Intrinsec*
ISH*
ISPIN*
IT.eam*
Italtel*
ITC Secure*
I-Tracing
Itrust*
Khipu Networks*
KPMG*
Kudelski Security*
Kyndryl*
Leidos*
Logicalis*
LTIMindtree*
Lumen*
Macquarie Telecom Group*
Materna*
Microland*
Mphasis*
NCC Group*
NEC*
Nettitude*
Nextios*
Nomios*
NTT DATA*
NTT Ltd.*
NXO*
Obrela Security*
Open Systems*
Optiv*
Orange Cyberdefense*
Performanta*
Persistent Systems*
Presidio*
Proficio*
PurpleSec*
PwC*
Quorum Cyber*
Rackspace Technology*
Redbelt*
SCC*
Secureworks*
SecurityHQ*
Sekuro*
Service IT*
SFR*
Shearwater Group*
SilverSky*
SLK Software*
Softcat*

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

SONDA*
Sopra Steria*
Stefanini*
suresecure*
SVA System Vertrieb Alexander
Swisscom*
Syntax*
Talion*
Tata Communications*
TCS*
TDEC*
Tech Mahindra*
Telstra*
Tempest*
terreActive*
Tesserent*
Thales*
TIVIT*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
ValueLabs*
Vectra*
Verizon Business*
Wavestone*
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 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.

ISG Provider Lens™

JANUARY, 2024

BROCHURE: CYBERSECURITY – SOLUTIONS AND SERVICES