ISG Provider Lens™

Cybersecurity – Services and Solutions

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

BROCHURE | **JANUARY 2025** | **AUSTRALIA, BRAZIL, FRANCE, GERMANY, SWITZERLAND, U.K., U.S., U.S. PUBLIC SECTOR AND GLOBAL**

Table of Contents

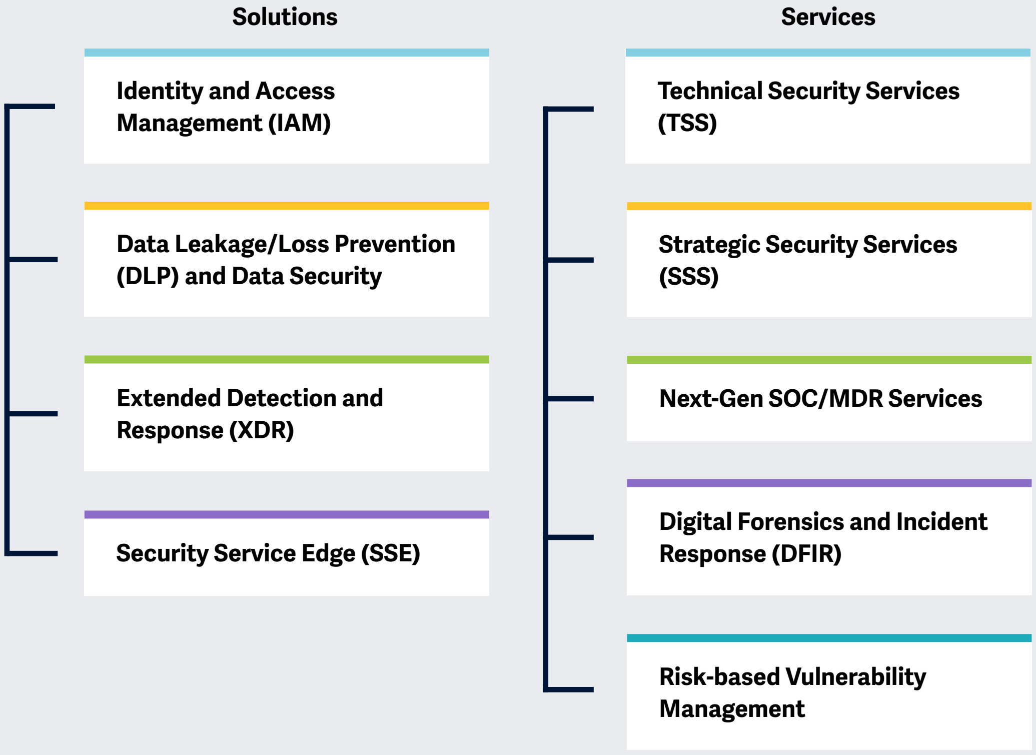
Cybersecurity in the Age of AI and Upcoming Disruptive Technology

In the era of rapid technological advancements and AI integration into daily operations, the cybersecurity landscape has become increasingly complex and multifaceted. Regulatory requirements such as the Network and Information Security (NIS) 2 Directive in the European Union are elevating the demand for robust cybersecurity measures, compelling organizations to reassess their security frameworks amidst emerging threats. Simultaneously, the commoditization of hacking tools has significantly reduced entry barriers for malicious actors, resulting in a surge of cybercriminal activities and a corresponding escalation of risks.

The proliferation of technology has expanded the attack surface, posing critical challenges for organizations as they navigate between operational technology (OT) and IT. The scarcity of skilled cybersecurity personnel has amplified this complexity, spurring accelerated demand for managed security services as companies seek external expertise to fortify their defenses.

Continued AI development presents risks and opportunities in the cybersecurity space. Security service providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats and understanding the transformative impact of new technologies such as quantum computing. In response to these challenges, businesses are increasingly investing in solutions such as identity and access management (IAM), data loss prevention (DLP), extended detection and response (XDR), and security service edge (SSE), combining advanced tools and human expertise with behavioral and contextual intelligence to enhance their security posture.

Key focus areas for Cybersecurity – Services and Solutions 2025.



Solutions

- Identity and Access Management (IAM)
- Data Leakage/Loss Prevention (DLP) and Data Security
- Extended Detection and Response (XDR)
- Security Service Edge (SSE)

Services

- Technical Security Services (TSS)
- Strategic Security Services (SSS)
- Next-Gen SOC/MDR Services
- Digital Forensics and Incident Response (DFIR)
- Risk-based Vulnerability Management

Simplified Illustration Source: ISG 2025

The ISG Provider Lens™ Cybersecurity – Services and Solutions study 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 Australia, Brazil, France, Germany, Switzerland, the U.K., the U.S. and the U.S. Public Sector.
- IAM, SSE and XDR topics will be analyzed for the global market.
- To consider country-specific characteristics in this global study, XDR's analysis would be extended to Brazil, DLP would be analyzed exclusively for Germany, a focus on DFIR will be undertaken for France and Risk-based Vulnerability Management will be assessed for France and 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 in this quadrant are distinguished by their proprietary software, including SaaS, and services for managing enterprise user identities. It excludes pure service providers that do not offer an IAM product, either on-premises or cloud-based, developed with proprietary software. Depending on organizational needs, these solutions can be deployed on-premises, in customer-managed clouds, as as-a-service models or a combination of these options.

IAM solutions focus on managing user identities and access rights, including specialized access through privileged access management (PAM) governed by defined policies. IAM suites integrate secure mechanisms, frameworks and automation for real-time user and attack profiling to meet evolving application needs. Providers are also expected to include social media and mobile access functionalities, addressing security needs beyond traditional web rights management. This quadrant also encompasses machine identity management.

Eligibility Criteria

1. Offer solutions that can be **deployed on-premises,** in the **cloud,** as **identity-as-a-service** (IDaaS) or through a managed third-party model
2. Deliver 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** to address multiple enterprise needs such as **cloud, endpoint, mobile devices, APIs and web applications**
5. Propose 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 SCIMOffer a portfolio with one or more of the following solutions — **directory, dashboard or self-service management** and lifecycle management (migration, sync and replication) — to support secure access

Definition

DLP solution providers assessed in this quadrant are distinguished by their proprietary software, including SaaS, and associated services. It excludes pure service providers that do not offer a DLP product, either on-premises or cloud-based, developed with proprietary software. DLP solutions can identify and monitor sensitive data and provide access to authorized users. They include a mix of products offering visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

DLP solutions help companies face challenges in controlling data movements, with over one-third of data violations originating internally. The proliferation of mobile and other devices for data storage elevates these concerns, as they can exchange data without central gateways. Data security solutions protect against unauthorized access and theft by prioritizing, classifying and monitoring data at rest and in transit, enabling organizations to enhance data security.

Eligibility Criteria

1. Offer DLP solutions based on **proprietary software** and not third-party software
2. Demonstrate the capability to support DLP **across any architecture, such as the cloud, network, storage or endpoint**
3. Showcase the ability to **protect sensitive data**, whether **structured or unstructured**, in text or binary formats
4. Provide solutions with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
5. Offer solutions capable of **identifying sensitive data, enforcing policies**, monitoring traffic and improving data compliance

Definition

XDR solution providers assessed in this quadrant are distinguished by their platforms that integrate, correlate and contextualize data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-based technology integrating multiple security solutions and using analytics to improve detection accuracy. It consolidates security products to enhance visibility and threat context across enterprise workspaces, networks and workloads.

XDR solutions use telemetry and contextual data for detection and response, integrating multiple products into a unified interface. They feature high automation and prioritize alerts based on severity to determine the needed tailored responses. 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 and address integration challenges. They help security operations teams manage 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 that 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 and IDPS), **network detection and response**, identity management, email security, mobile threat detection, cloud workload protection and deception identification
4. Provide solutions with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solutions capable of **blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware
6. Provide solutions using **threat intelligence** and **real-time insights on threats** emanating across endpoints
7. Deliver solutions with **automated response features**

Definition

SSE solution providers assessed in 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. Providers offer SSE solutions as an integrated security service through globally positioned points of presence 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 DLP, browser isolation and next-generation firewall (NGFW) to secure access to cloud and on-premises applications.

Providers 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 will be covered in the ISG Provider Lens™ Network – Software Defined Services and Solutions 2025 study.

Eligibility Criteria

1. Provide SSE as an **integrated solution** with **ZTNA, CASB, SWG and FWaaS** components
2. Offer solutions **predominantly based on proprietary** software; these solutions may **partially rely on partner solutions** while avoiding **complete dependency on third-party** software
3. Maintain **globally located points of presence** to deliver solutions
4. Deliver **SSE functionalities to cloud and on-premises** environments (including hybrid environments)
5. Undertake **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 **availability of solutions globally**

Technical Security Services (TSS)

Definition

TSS providers assessed in this quadrant cover integration, maintenance and support for IT and OT security products or solutions. TSS encompasses a wide range of security products, including cloud and data center security, IAM, DLP, network security, endpoint security, OT security, SASE and others.

These providers offer playbooks and roadmaps to enhance security using best-of-breed tools, improving posture and reducing threats. Their portfolios support complete or individual security architecture transformations, alongside product or solution identification, assessment, design and implementation. They invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio.

This quadrant also includes classic managed security services provided without a security operations center. It examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other solution vendors and service providers.

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Obtain **authorization from 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
4. **Do not focus exclusively** on **proprietary products** or solutions
5. Present **case studies** that demonstrate successful design, deployment and management of cybersecurity solutions for companies within the target country

Definition

SSS providers assessed in this quadrant offer IT and OT security consulting. Services include security audits, assessments, and awareness and training. These providers also help assess security maturity and define cybersecurity strategies to meet enterprise-specific requirements.

Providers employ experienced security consultants to plan and manage end-to-end security programs for enterprises. Considering the rising demand from SMBs and talent shortages, SSS providers offer on-demand experts via virtual CISO services. They create business continuity roadmaps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to improve cyber literacy and response among enterprise board members and employees.

They also provide guidance on selecting security technologies and suppliers, reviewing organizational structures for cybersecurity, evaluating security processes and practices, and improving them in alignment with the risks faced. This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Display competence in the application of good practices and market security frameworks such as ISO 27000, NIST and CIS
3. **Offer at least one of the above** strategic security services in the respective countries assessed for this study
4. Provide **security consulting services using frameworks such as NIST and ISO**
5. **Do not focus exclusively** on **proprietary products** or solutions

Definition

Providers assessed in this quadrant offer services related to the continuous monitoring of IT and OT infrastructures 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 and remediation.

Next-Gen SOC providers are in demand to strengthen enterprises' security posture and improve the effectiveness of security programs. They blend traditional managed security services with innovation to deliver integrated cyber defense and managed detection and response (MDR) services. These providers also invest in threat detection and hunting, threat intelligence, modeling and forensics, incident management and advanced technologies, such as automation, big data, AI and ML, to offer a holistic approach to proactive threat mitigation and advanced security.

Eligibility Criteria

1. Offer standard services, including **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, either remotely or at clients' site
3. MDR-specific capabilities, including **advanced threat intelligence** and **behavior-based and human-led threat hunting,** delivering **offensive and defensive** security capabilities with a **unified view** for reporting and metrics
4. Possess **accreditations** from security tools vendors
5. **Manage own SOCs**
6. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
7. Offer a variety of tiered pricing models

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 offer proven DFIR techniques and methodologies and can 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 led to the adoption of DFIR services. DFIR is essential to identify data loss following a security breach and establish effective threat responses through playbooks. Service providers demonstrate expertise in digital forensics, including triage, timeline and log analysis, malware examination and artifact analysis. Providers also have experience in litigation support for claims and audits and proficiency in tools such as SIEM, SOAR, endpoint detection and response (EDR) and XDR.

Eligibility Criteria

1. Employ a **dedicated incident response team** (CERT or CSIRT) of experts with relevant certifications such as GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE) and CISSP, showcasing their expertise and commitment to maintaining industry standards
2. Possess experience and expertise in **handling various** SIEM, SOAR, EDR and XDR solutions
3. Offer DFIR services that **identify the root cause** of a **breach** and evaluate its short- and long-term impact
4. Possess **capabilities** in malware analysis, ransomware decryption and data recovery
5. Demonstrate **partnership** with product vendors and managed security service providers to enhance threat intelligence, dark web monitoring and SOC capabilities and mitigate advanced, persistent and sophisticated threats

Definition

Risk-based vulnerability management service providers assessed in this quadrant are distinguished by their advanced technical skills and ability to undertake continual updates on known vulnerabilities and sophisticated methods bypassing established defenses through practices such as penetration testing. Generative AI (GenAI) tools have empowered cybercriminals to identify and exploit vulnerabilities in technology assets, particularly the ones exposed to the internet. This trend, coupled with an increase in ransomware incidents, underscores the need for continuous vulnerability management rather than the approach of sporadic assessments.

Considering the rapid frequency of updates to internet-facing services, implementing continuous vulnerability detection has become essential to an effective risk-based cybersecurity strategy. Providers must now offer targeted solutions that transcend traditional practices, recognizing that a risk-based framework is vital to effectively manage vulnerabilities and minimize the impact in today's fast-evolving threat landscape.

Eligibility Criteria

1. Encompass specialized in-house teams capable of **rigorously assessing vulnerabilities and indicating solutions** to remove flaws and gradually reduce 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 web applications, mobile devices, internal networks, cloud, APIs, IoT and other exposed assets
3. Use methods such as **dynamic application security testing (DAST), static application security testing (SAST) and penetration testing** of specific objectives using manual and/or automated tools for service delivery
4. Use and evidence **recognized industry standards** such as SOC 2, ISO27001, NIST 800-53, PCI-DSS and HIPPA when indicating security flaws
5. Offer **retesting, specialized support and mechanisms** for monitoring corrective actions, updating the risk and severity matrix (exposure to remaining vectors) as required
6. Employ a **technical expert team** (Ethical Hackings) with certifications such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), CompTIA Penetration Testing (CompTIA PenTest+) and GIAC Penetration Tester (GPEN)

Quadrants by Region

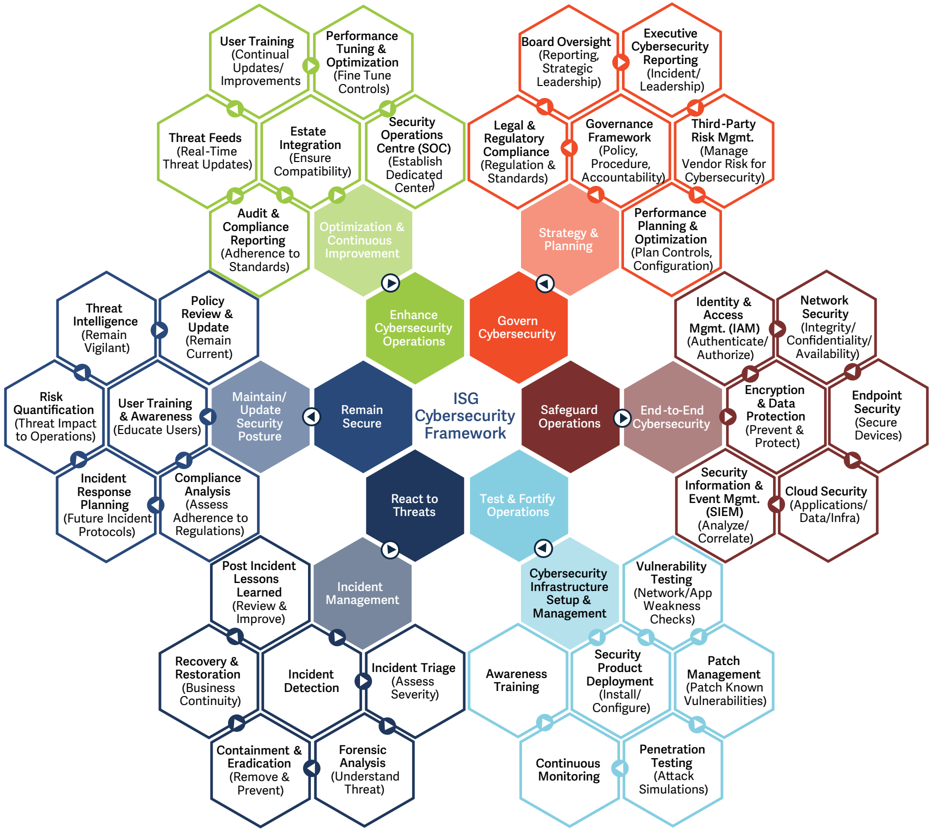
As a part of this ISG Provider Lens™ quadrant study, we are introducing the following nine quadrants on Cybersecurity – Services and Solutions 2025:

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)	✓	✓	✓	✓	✓	✓	✓	✓	
Next-Gen SOC/MDR Services	✓	✓	✓	✓	✓	✓	✓	✓	
Digital Forensics and Incident Response (DFIR)					✓				
Risk-based Vulnerability Management					✓	✓			

ISG's Cybersecurity Framework

Key characteristics of the proprietary framework:

- Encapsulates what enterprises are doing across the Cybersecurity market and helps connect them to digital solutions
- Represents the entire value chain of supply and demand within the market
- Inner tiles represent themes of enterprise objectives
- Outer tiles represent initiatives
- Behind each outer tile is a specific set of capabilities, with unique market leading providers and solutions


User Training (Continual Updates/ Improvements)
Performance Tuning & Optimization (Fine Tune Controls)
Board Oversight (Reporting, Strategic Leadership)
Executive Cybersecurity Reporting (Incident/ Leadership)
Threat Feeds (Real-Time Threat Updates)
Estate Integration (Ensure Compatibility)
Security Operations Centre (SOC) (Establish Dedicated Center)
Legal & Regulatory Compliance (Regulation & Standards)
Governance Framework (Policy, Procedure, Accountability)
Third-Party Risk Mgmt. (Manage Vendor Risk for Cybersecurity)
Audit & Compliance Reporting (Adherence to Standards)
Optimization & Continuous Improvement
Strategy & Planning
Performance Planning & Optimization (Plan Controls, Configuration)
Threat Intelligence (Remain Vigilant)
Policy Review & Update (Remain Current)
Enhance Cybersecurity Operations
Govern Cybersecurity
Identity & Access Mgmt. (IAM) (Authenticate/ Authorize)
Network Security (Integrity/ Confidentiality/ Availability)
Risk Quantification (Threat Impact to Operations)
User Training & Awareness (Educate Users)
Maintain/ Update Security Posture
Remain Secure
ISG Cybersecurity Framework
Safeguard Operations
End-to-End Cybersecurity
Encryption & Data Protection (Prevent & Protect)
Endpoint Security (Secure Devices)
Incident Response Planning (Future Incident Protocols)
Compliance Analysis (Assess Adherence to Regulations)
React to Threats
Test & Fortify Operations
Security Information & Event Mgmt. (SIEM) (Analyze/ Correlate)
Cloud Security (Applications/ Data/Infra)
Post Incident Lessons Learned (Review & Improve)
Incident Management
Cybersecurity Infrastructure Setup & Management
Vulnerability Testing (Network/App Weakness Checks)
Recovery & Restoration (Business Continuity)
Incident Detection
Incident Triage (Assess Severity)
Awareness Training
Security Product Deployment (Install/ Configure)
Patch Management (Patch Known Vulnerabilities)
Containment & Eradication (Remove & Prevent)
Forensic Analysis (Understand Threat)
Continuous Monitoring
Penetration Testing (Attack Simulations)

The research phase falls in the period between January and February 2025, during which survey, evaluation, analysis and validation will take place. The results will be presented to the media in July 2025.

Milestones	Beginning	End
Survey Launch	January 7, 2025	
Survey Phase	January 7, 2025	February 7, 2025
Sneak Preview	May 2025	June 2025
Press Release & Publication	July 2025	

Collecting client testimonials via the Star of Excellence Program requires early client referrals (no official reference needed) because CX scores have a direct influence on the provider's position in the IPL quadrant and the awards.

Please refer to the link to view/download the ISG Provider Lens™ 2025 research agenda.

Access to Online Portal

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

Buyers Guide

ISG Software Research, formerly "Ventana Research," offers market insights by evaluating technology providers and products through its Buyers Guides. The findings are drawn from the research-based analysis of product and customer experience categories, ranking and rating software providers and products to help facilitate informed decision-making and selection processes for technology.

In the course of the Cybersecurity – Services and Solutions IPL launch, we want to take advantage of the opportunity to draw your attention to related research and insights that ISG Research will publish in 2025. For more information, refer to the Buyers Guide research schedule.

Research Production Disclaimer:

ISG collects data for the purposes of conducting 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.

Client Feedback Nominations

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:
star@cx.isg-one.com

ISG Star of Excellence

The ISG Provider Lens 2025 – Cybersecurity – Services and Solutions research study analyzes the relevant software vendors/service providers in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Analysts:
Frank Heuer, Gowtham Kumar, Bhuvaneshwari Mohan, Benoit Scheuber, Dr. Maxime Martelli, Andrew Milroy and João Mauro

Research Analysts:
Monica K, Sandya Kattimani, Rafael Rigotti and Bhuvaneshwari Mohan

Project Manager:
Shreemadhu Rai B

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 study will include data from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. ISG recognizes the time lapse and possible market developments between research and publishing, in terms of mergers and acquisitions, and acknowledges that those changes will not reflect in the reports for this study.

All revenue references are in U.S. dollars ($US) unless noted.

Contacts For This Study

Study Sponsor

Heiko Henkes

Director and Principal Analyst

Frank Heuer

Lead Analyst - Germany, Switzerland

Gowtham Kumar

Lead Analyst - U.S., U.S. Public Sector, Global

Bhuvaneshwari Mohan

Lead Analyst- U.K., U.S. Public Sector, Global

Benoit Scheuber

Lead Analyst - France

Dr. Maxime Martelli

Lead Analyst - Global

Andrew Milroy

Lead Analyst - Australia

João Mauro

Lead Analyst - Brazil

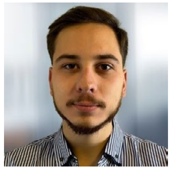
Monica K

Research Analyst

Contacts For This Study

Sandya
Kattimani

Research Analyst



Rafael
Rigotti

Research Analyst

Rajesh
Chillappagari

Data Analyst

Laxmi
Sahebrao

Data Analyst

Shreemadhu
Rai B

Project Manager

ISG Provider Lens Advisors Involvement Program

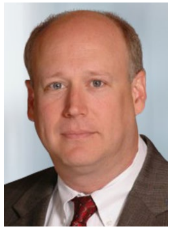
ISG Provider Lens offers market assessments incorporating practitioner insights, reflecting regional focus and independent research. ISG ensures advisor involvement in each study to cover the appropriate market details aligned to the respective service lines/technology trends, service provider presence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

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

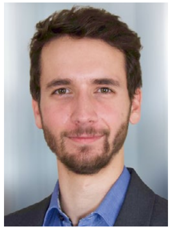


Doug Saylors

Partner, Co-lead ISG Cybersecurity

David Gordon

Principal Consultant Cybersecurity



Anas Barmo

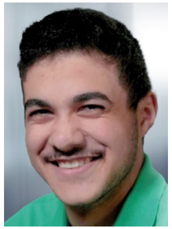
Senior Consultant Cybersecurity

Brendan Prater

Consulting Manager Cybersecurity

Advisory Team

ISG Advisors to this study



Marco
Ezzy

Consultant
Cybersecurity

Tim
Merscheid

Consulting Manager
Cybersecurity

Christophe
de Boisset

Consulting Manager
Cybersecurity

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

Absolute Software*
AC3*
Accenture*
ACESI Group
Acronis*
Actar (Peers Group)
ActioNet*
Adarma*
ADIT Group
Advens*
Agility Networks*
Airbus Protect*
AISI
Akamai*
Algosecure

Alice&Bob.Company*
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
AntemetA
Apixit
Appdome
Apura Cyber Intelligence S/A
Arcon
Asper*
AT&T Cybersecurity*
Atos*
Avatier*

Aveniq*
Avertium*
Axians*
Axur
Azion
BAYOOSOFT*
BDO
Bechtle*
Berghem*
Beta Systems*
BeyondTrust*
BIP
Bitdefender*
BlackBerry*
Blaze Information Security*

BluePex*
BlueVoyant*
Brainloop*
Bravo GRC
Bridewell
Broadcom
BT*
CANCOM*
Capgemini*
Cato Networks*
CDW*
Century Data
CGI*
ChapsVision CyberGov
Check Point Software*

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

Cipher*
Cirion*
Cisco*
Citrix
Claranet*
Clavis*
ClearSale
Cloud Target
Cloudflare*
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Consulteer InCyber

Controlware*
CoSoSys (Netwrix)*
Critical Start*
Cross Identity*
CrowdStrike*
CTM*
CyberArk*
CyberCX*
Cybereason*
CyberProof*
Cyberprotect
CyberSecOp*
Cybersolutions
Cyderes*
Darktrace

Data#3*
Datacom*
DATAGROUP*
dataRain
Delfia
Delinea
Deloitte*
Deutsche Telekom
Devensys
Devoteam*
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust
Edge UOL*

Embratel
EmpowerID*
Ensono
Entrust*
Ergon Informatik*
Ericom Software*
e-Safer
ESET*
E-TRUST*
Eviden*
EY*
FastHelp*
Fidelis Cybersecurity*
FireEye
Fischer Identity*

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

- Forcepoint*
- ForgeRock (Ping Identity)
- Formind*
- Fortinet*
- Fortra*
- Framatome Cybersecurity
- Fujitsu*
- FusionAuth*
- Future Segurança da Informação
- GBS*
- GC Security*
- Genetec
- Getronics*
- Gigamon
- Globant*
- glueckkanja*
- GoCache*
- Google*
- GTT*
- HackerOne
- HackerSec*
- Hakai Offensive Security*
- Happiest Minds*
- HCLTech*
- Headmind Partners*
- HiSolutions*
- HPE Aruba Networking
- HSC Brasil
- HubOne (SysDream)*
- Huge Networks*
- IBLISS Digital Security*
- IBM*
- iboss*
- iC Consult*
- Ilex IAM Platform*
- Imperva
- Imprivata*
- IMS Networks
- IN Groupe*
- indevis*
- InfoGuard*
- Infosys*
- Integrity360*
- Interop
- Intrinsec*
- ISH Tecnologia*
- ISPIN*
- IT.eam*
- It4us
- Italtel*
- ITC Secure*
- I-Tracing
- Itrust (Free Pro)*
- ITS Group*
- itWatch*
- Kaspersky*
- KnowBe4
- KPMG*
- Kroll*
- Kryptus*

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

Kudelski Security*
Kyndryl*
Lastpass*
Leidos*
Lexfo*
Logical IT
Logicalis*
Lookout*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Mandiant
Materna Radar*

Matrix42*
McAfee
Metsys*
Micro Focus
Microland*
Microsoft*
Modulo Security Solutions
Mphasis*
MTF*
NAVA*
NBS System
NCC Group*
NEC*
Neosoft
NetSecurity

Netskope*
Network Secure
Neverhack*
Nevis*
Nextios
Nok Nok Labs*
Nomios*
Novared
Noventiq
Npo Sistemas
NRI ANZ*
NTSEC
NTT DATA*
NTT Ltd.
NXO*

NYBBLE
OEDIV
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Optiv*
Oracle*
Orange Cyberdefense*
OST Tecnologia
P1 SECURITY
Palo Alto Networks*
pco*
Peers

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

Performanta*
Perimeter 81*
Persistent Systems*
Ping Identity*
Presidio*
Pride Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PurpleSec*
PwC*
Quorum Cyber*
Rackspace Technology*
Radware

Rapid7*
RCZ
Red river
Redbelt
Redscan*
Reply
RSA Security*
Safeway
Safeweb
SailPoint*
SAP*
Saviynt*
SCC*
Scunna*
SCUTUM

SEC4U
SecureAuth*
Secureway
Secureworks*
Securiti
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sekuro*
senhasegura*
SenseOn*
SentinelOne*
Seqrite
Sequretek
Service IT*

Servix
Seti
SFR*
Shearwater Group*
Sigma
Sigma Telecom
Skyhigh Security*
SLK Software*
SNS Security
Softcat*
SolarWinds*
Solor
SONDA*
Sophos*
Sopra Steria*

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

Spie ICS*
Splunk
Squad*
Stefanini*
suresecure*
Swisscom*
Symantec
Synetis*
Syntax*
Sysinterga
Systancia*
Talion*
Tanium
Tata Communications*
TCS*

TDec Network Group*
Tech Mahindra*
TEHTRIS*
Telefonica Tech*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
TIVIT*
Trellix*
Trend Micro*

Trustwave*
T-Systems*
UMB*
Under Protection
Unisys*
United Security Providers*
ValueLabs*
Varonis*
Vectra*
Venturus
Verizon Business*
Versa Networks*
Vigilant
VMware Carbon Black
Vortex Security*

Vortex TI
WALLIX*
WatchGuard
Wavestone*
Wipro*
Xmco
YSSY*
Zensar Technologies*
Zscaler*

About Our Company & Research

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 AI and 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 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, 2025

BROCHURE: CYBERSECURITY – SERVICES AND SOLUTIONS