ISG Provider Lens®

Cybersecurity — Services and Solutions

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

BROCHURE | JANUARY 2026 | AUSTRALIA, BRAZIL, FRANCE, GERMANY, SWITZERLAND, U.K., U.S. AND U.S. PUBLIC SECTOR

Table of Contents

Introduction

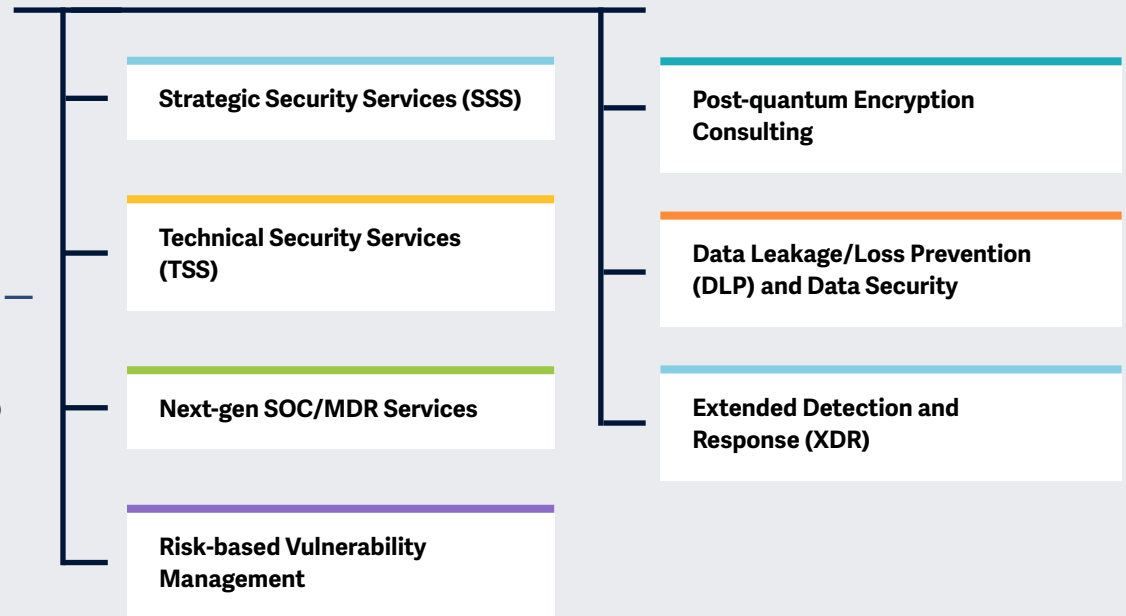
In 2026, the cybersecurity landscape is expected to witness an increase in threat sophistication, expanding regulatory demands and a rapid shift toward intelligence-driven defense models. Enterprises across industries are under pressure to secure their increasingly distributed architectures, protect sensitive data across hybrid environments and respond to the surge in AI-enabled attacks. Meanwhile, boards and regulators seek demonstrable cyber resilience and verifiable control effectiveness, paving the way for security programs as part of digital transformation agendas.

In this light, the market is reorganizing itself into clearly defined capability domains. While technical security services (TSS) ensure configuration integrity, secure implementations and continuous hardening, strategic security services (SSS) are gaining importance as executives prioritize cybersecurity with governance, risk and architectural alignment.

Next-generation SOCs and managed detection and response (MDR) services are also gaining traction, driven by the demand for 24/7 threat monitoring, AI-supported analysis and outcome-based response models. Additionally, risk-based vulnerability management reinforces preventive security by prioritizing exposures using business context and attack path insights. Finally, post-quantum encryption consulting enters the market scope as organizations begin preparing cryptographic inventories and transition strategies to safeguard long-term data confidentiality.

This IPL study covers the mentioned capability domains, among others, and offers a comprehensive view how providers differentiate in an environment defined by speed, intelligence and resilience.

Key focus areas for Cybersecurity – Services and Solutions 2026



Simplified Illustration Source: ISG 2026

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.
- Differentiated positioning of providers by segments on their competitive strengths and portfolio attractiveness.
- Focus on different markets, including Australia, Brazil, France, Germany, Switzerland, U.K., U.S. and U.S. public sector.
- Country-specific characteristics: Post-quantum Encryption Consulting in Germany and the U.S., XDR and risk-based vulnerability management analysis in Brazil and DLP analysis in Germany.

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 the information from these reports to evaluate their current vendor relationships and potential engagements.

Definition

This quadrant evaluates service providers that deliver consulting-led cybersecurity services focusing on strategy, governance, risk management and organizational transformation for IT and OT environments. These providers assess security maturity, quantify risks, define target operating models and develop cybersecurity strategies, policies and roadmaps aligned with business objectives and regulatory requirements. Their offerings include audits, assessments, security awareness programs, business continuity planning, tabletop exercises and advisory on technology selection.

These providers also employ experienced consultants who guide enterprises through program design, governance improvements and capability development, including virtual Chief Information Security Officer (vCISO) models for ongoing or on-demand strategic leadership. Unlike TSS, which emphasize hands-on integration and engineering, SSS providers focus on advisory outcomes rather than operational monitoring or proprietary product execution.

Eligibility Criteria

1. Provide **vendor-agnostic security consulting** covering maturity assessments, strategy development, policy design, governance models and roadmap creation
2. Demonstrate capabilities in **strategic domains** such as risk quantification, regulatory readiness, vendor selection, business continuity planning and broader cyber risk advisory
3. **Apply recognized frameworks** and comply with standards (such as ISO 27000, NIST CSF, CIS Controls) when guiding enterprise programs
4. **Deliver at least one of the above** strategic security service within the target region through **qualified and certified** consultants
5. Present **documented evidence of engagements** that improved clients' security posture, governance structures, compliance readiness or risk-based decision-making
6. Provide **structured consulting methodologies**, templates or playbooks for assessments, strategic planning or organizational transformation
7. Operate as **consulting-led service providers** rather than product vendors, while allowing proprietary frameworks or tools that support advisory delivery
8. **Do not** focus exclusively on proprietary products

Definition

This quadrant evaluates service providers that design, integrate, implement and modernize IT and OT security technologies across multi-vendor environments. Their services include deploying and configuring security controls for identity and access management, cloud and data centers, SASE/SSE, endpoints, networks, OT and industrial control systems (ICS), and related domains. Providers use reference architectures, automation frameworks and proprietary accelerators to deliver engineering-led transformations that streamline implementation and enhance control effectiveness.

They maintain strong partnerships with security vendors, hold specialized certifications and support lifecycle tasks such as hardening, tuning, patching and device management. Unlike SSS, which focus on advisory and governance, TSS providers emphasize hands-on technical execution. They do not offer SOC-based monitoring or MDR operations but may provide traditional managed security services.

Eligibility Criteria

1. Demonstrate experience in **designing, integrating and implementing** IT and/or OT security technologies, supported by multi-vendor certifications and OEM partnerships
2. Deploy **accelerators, proprietary toolsets or reference architectures** that enhance implementation quality, interoperability and time-to-value
3. Employ **certified engineers and architects** adept at configuring, customizing and optimizing security solutions across cloud, networks, endpoints and OT environments
4. Show a **structured, methodology-driven approach** for evaluating, selecting and integrating security technologies that align with client requirements, risk profiles and architectural constraints
5. Deliver **lifecycle engineering services** such as configuration management, policy tuning, patching, control hardening and technology modernization
6. Present documented **case studies** demonstrating successful security technology deployments or transformations within the target region
7. Operate as **service-led integrators** rather than standalone ISVs, permitting proprietary accelerators or internally developed tools that support service delivery
8. **Do not** focus exclusively on proprietary products

Definition

This quadrant evaluates service providers that deliver continuous monitoring and MDR services through SOCs. Their offerings span the entire incident lifecycle, including detection, triage, investigation, containment and coordinated remediation. Providers integrate and operate modern security technologies, apply threat intelligence and advanced analytics, and deliver human-led and automated threat hunting to strengthen enterprise resilience. Next-gen SOC/MDR services combine managed security operations with innovative AI-driven analytics, autonomous triage and security orchestration, automation and response (SOAR)-based orchestration to reduce response times and improve threat visibility across IT and OT environments. They support co-managed models and do not focus on strategic advisory or technology implementation, which fall within the scope of SSS and TSS, respectively.

Eligibility Criteria

1. Deliver 24/7 **monitoring, detection and response** services through **owned SOCs**, covering IT and/or OT environments
2. Provide **MDR-specific capabilities**, including behavioral analytics, large language model (LLM)-aware threat intelligence integration, human-led and automated threat hunting, and advanced detection engineering
3. **Operate and manage** Security Information and Event Management (SIEM), SOAR, endpoint detection and response (EDR), network detection and response (NDR) and other relevant security technologies, supported by OEM accreditations
4. Demonstrate a structured **incident response approach** covering triage, investigation, containment, remediation coordination and post-incident improvement
5. Use **AI-driven** analytics, autonomous triage agents and SOAR workflows to accelerate detection and reduce mean time to respond (MTTR)
6. Offer **co-managed service** models with enterprise teams, enabling shared visibility, analyst collaboration and joint response processes
7. Present **reference cases** showing measurable improvements in detection coverage, response efficiency or operational resilience within the target region
8. **Do not** focus exclusively on proprietary products, but manage and operate best-of-breed security tools

Definition

This quadrant evaluates service providers that deliver continuous, risk-based vulnerability management services across IT, cloud, application and digital infrastructure environments. These providers identify, assess and prioritize vulnerabilities based on exploitability, exposure and business impact rather than severity scores alone. Their services combine automated discovery, penetration testing, application security testing and contextual risk analysis to address rapidly evolving attack techniques, including those accelerated by GenAI, and increased ransomware activity.

Risk-based vulnerability management facilitates continuous visibility into internet-facing and internal assets, enables prioritization of remediation aligned to real attack paths and business criticality, and helps enterprises reduce exposure in fast-changing technology landscapes through ongoing observability, assessment, retesting and risk recalibration.

Eligibility Criteria

1. Deliver **continuous vulnerability assessment services** that prioritize findings based on exploitability, exposure and business impact and not merely static severity metrics
2. Provide **testing services** across web and mobile applications, APIs, internal networks, cloud environments (containers, Kubernetes/K8S and Docker), ATMs, URAs, IoT and other exposed assets
3. Apply **recognized testing methods** such as penetration testing, dynamic application security testing (DAST), static application security testing (SAST), interactive application security testing (IAST) and related techniques combining automated tooling and manual expert validation
4. Align **vulnerability findings and reporting** with relevant standards and frameworks such as ISO 27001, NIST SP 800-53, PCI DSS, SOC 2 and applicable regulatory or industry-specific requirements
5. Offer **retesting, remediation tracking and continuous risk reassessment** to reflect changes in exposure, threat intelligence and mitigation progress
6. Employ **security professionals** such as ethical hackers (CEHs), offensive security certified professionals (OSCPs) and information systems security professionals (CISSPs), and experts holding CompTIA PenTest+ or GIAC certifications, to support consistent service quality

Post-quantum Encryption Consulting

Definition

This quadrant evaluates consulting-led service providers that assist enterprises in preparing for and executing the cryptographic transition required to mitigate risks associated with quantum computing. These providers assess cryptographic dependencies across the IT, OT, IoT and digital supply chain environments, including inventory management, identification of quantum-vulnerable algorithms and exposure to *harvest now, decrypt later* threats. They develop risk-based post-quantum cryptography (PQC) strategies, design migration and hybrid cryptographic roadmaps, and advise on the adoption of emerging post-quantum standards aligned with the National Institute of Standards and Technology (NIST), Federal Office for Information Security (BSI) and other regulatory bodies. PQC consulting addresses the impacts on key management, identity systems, communications, applications and infrastructure architectures, enabling organizations to plan for compliant, scalable and future-resilient cryptographic transformations.

Eligibility Criteria

1. Deliver **cryptographic and quantum risk assessments**, including inventorying cryptographic assets, algorithms and key usage across IT, OT, IoT, cloud, network and application environments
2. Demonstrate **consulting capabilities in PQC strategy development**, including phased migration roadmaps, hybrid cryptography planning and dependency analysis
3. Provide advisory services aligned with **emerging standards and guidance** such as NIST PQC, BSI TR-02102, European Telecommunications Standards Institute (ETSI) and relevant ISO/IEC mandates
4. Assess the **impacts on key management**, public key infrastructure (PKI), identity and access systems, secure communications and application architectures
5. Present evidence of **PQC-related client engagements**, pilots, simulations or PoCs addressing quantum-led risk reduction
6. Offer vendor-neutral advisory services while demonstrating knowledge of relevant technology ecosystems and cryptographic implementations
7. **Support compliance** with government mandates and meet the objectives of sector-specific or national cryptographic transition initiatives

Data Leakage/Loss Prevention (DLP) and Data Security

Definition

This quadrant evaluates independent software vendors (ISVs) that develop proprietary DLP and data security solutions delivered as on-premises software, cloud platforms or SaaS. These products enable the discovery, classification and monitoring of sensitive data across endpoints, networks, cloud services and storage systems and apply policy-based controls to prevent unauthorized access or exfiltration. Modern DLP technologies increasingly integrate device hardening, application control and behavioral analytics to prevent data misuse at the endpoints and enforce policies even in offline or unmanaged environments.

They provide centralized governance, reporting and compliance support to protect structured and unstructured data throughout its lifecycle. In a distributed IT landscape with heightened risks of insider and data flow breaches, these solutions form the core safeguard for protecting critical information assets and ensuring consistent data handling practices.

Eligibility Criteria

1. Provide a **proprietary DLP or data security product** (no embedded third-party DLP engines)
2. **Support core architectures** such as endpoint, network, cloud and storage environments
3. **Detect, classify and protect** structured and unstructured data at rest and in transit
4. Offer **centralized management functions**, including policy controls, reporting and configuration
5. **Enable** data discovery, real-time monitoring and policy-based enforcement actions
6. **Demonstrate** enterprise-scale deployments and documented customer adoption

Definition

This quadrant evaluates ISVs that develop proprietary XDR platforms integrating telemetry, analytics and response capabilities across endpoints, networks, identities, cloud workloads and applications. These solutions correlate and contextualize data from multiple security controls to enhance detection accuracy, reduce alert fatigue and strengthen operational efficiency. Modern XDR platforms unify threat visibility in a single interface, apply behavioral and ML analytics, and automate response actions based on severity and business context.

They operate as cloud-based or hybrid architectures with a defined front-end sensor layer and a back-end analytics and orchestration engine. As enterprises seek to consolidate tooling and improve detection maturity, XDR serves as a strategic foundation for coordinated, intelligence-driven defense.

Eligibility Criteria

1. Provide a **proprietary XDR platform** (no reliance on third-party XDR engines)
2. Include a **defined XDR front end** (multi-sensor integration) and XDR back end (analytics, correlation and orchestration)
3. **Integrate at least three** native or tightly coupled sensors, e.g., EDR/endpoint protection platform (EPP), NDR, identity, email, mobile or cloud workload protection
4. Deliver **unified visibility** across endpoints, networks and cloud environments
5. Demonstrate the **ability to detect and block sophisticated threats** such as advanced persistent threats (APTs), ransomware and advanced malware
6. **Use threat intelligence**, behavioral analytics and real-time telemetry correlations
7. Provide **automated or semi-automated** response actions with measurable impact

Quadrants by Regions

As a part of this ISG Provider Lens® quadrant study, we are introducing the following seven quadrants on Cybersecurity — Services and Solutions 2026

Quadrant	Australia	Brazil	France	Germany	Switzerland	U.K.	U.S.	U.S. Public Sector
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	Large & Mid	Large & Mid	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	Large & Mid	Large & Mid	✓
Next-gen SOC/MDR Services	✓	Large & Mid	✓	Overall & Mid	Overall, Large & Mid	Large & Mid	Large & Mid	✓
Risk-based Vulnerability Management		✓						
Post-quantum Encryption Consulting				✓			✓	
Data Leakage/Loss Prevention (DLP) and Data Security				✓				
Extended Detection and Response (XDR)		✓						

Schedule

The research phase falls in the period between January and June 2026, during which survey, evaluation, analysis and validation will take place. The results will be presented to the media in July 2026.

Milestones	Beginning	End
Survey Launch	January 7, 2026	
Survey Phase	January 7, 2026	February 13, 2026
Webinar Call	January 12, 2026	
Sneak Preview	May 2026	June 2026
Press Release & Publication	July 2026	

Please refer to the **ISG Provider Lens® 2026 research** agenda to view and download the list of other studies conducted by ISG Provider Lens®.

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!

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 2026. For more information, refer to the Buyers Guide research schedule.

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 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

Methodology & Team

The ISG Provider Lens® 2026 – 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, Bhuvaneshwari Mohan, Yash Jethani, Benoit Scheuber, Andrew Milroy and João Mauro

Research Analyst:
Monica K and Rafael Rigotti

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 and Switzerland

Bhuvaneshwari Mohan

Lead Analyst – U.K., U.S. Public Sector

Yash Jethani

Lead Analyst – U.S.

Benoit Scheuber

Lead Analyst – France

Andrew Milroy

Lead Analyst – Australia

João Mauro

Lead Analyst – Brazil

Monica K

Research Analyst

Rafael Rigotti

Research Analyst

Rajesh Chillappagari

Data analyst

Laxmi Sahebrao Kadve

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 consultant 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, Lead ISG Cybersecurity

David Gordon

Director Cybersecurity

Jason Stading

Director Cybersecurity

Brendan Prater

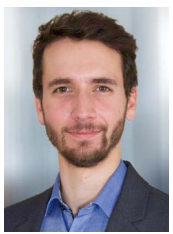
Principal Consultant Cybersecurity

Christophe deBoisset

Consulting Manager

Marco Ezzy

Consultant Cybersecurity



Anas Barmo

Consulting Manager

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

8com
Absolute Software*
AC3*
Accenture*
Acronis*
Actar (Peers Group)
ActioNet*
Addvalue
Advania
Advens*
Agility Networks*
Airbus Protect*
Aizoon*
Akamai Technologies
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
Appdome
Apura Cyber Intelligence S/A
Arcon
Arctic Wolf Networks, Inc.
Asper*
Atos*
Aveniq*
Avertium*
Avivatec
Axians*
Axur
Azion
BDO
Bechtle/Apixit*
Berghem
BeyondTrust
BIP
Bitdefender
Blaze Information Security
Bluepex*
BlueVoyant*
Brainloop*
Bravo GRC
Brennan IT*
Bricon
Bridewell*
Broadcom*
BT*
CANCOM*
Capgemini*
Capita*
CDW*
Century Data
CGI*
Check Point Software*
CI&T*
Cipher*
Cirion Technologies*
Cisco*
Citrix
Claranet*

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

Claro empresas
Clavis*
ClearSale
Cloud Target*
CloudFlare
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Controlware*
CoSoSys (Netwrix)*
C-Risk
Critical Start*
Crowdstrike*
CTM*
CyberArk
CyberProof*
CyberSecOp*
Cyderes*
Cyera
Cynet Security Ltd.
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Data-Sec
deepwatch, Inc.
Defcon1
Delfia
Delinea
Deloitte*
Deutsche Telekom*
Devoteam*
Dfense
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust*
Edge UOL*
e-Safer
ESET
E-TRUST
Expel, Inc
EY*
FastHelp
Fidelis Cybersecurity*
FireEye
Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Fujitsu*
Future Segurança da Informação

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

GBS*
GC Security
Genetec
Genpact
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec
Hakai Offensive Security
Happiest Minds*
HCLTech*
Headmind Partners*
Hillstone Networks
HiSolutions*
Holiseum*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iC Consult*
ID Quantique
Imperva
inCloud Tecnologia
indevis*
Inetum*
InfoGuard*
Infosys*
Innova Solutions*
Insight*
Inspira*
Integrity360*
Interactive*
Interop
Intrinsec*
IPTRUST*
ISH Tecnologia*
iSPIN*
iT.eam*
It4us
Italtel*
ITC Secure*
I-tracing
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*
L8 Group
Leidos*
Level blue (Trustwave)*
Littlefish
Logical IT
Logicalis*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Materna*
Matrix42*
McAfee
McKinsey
Metsys*
Micro Focus
Microland*
Microsoft*
Mimecast*
MindPoint Group LLC
Minsait (Indra)
Modulo Security Solutions*
Mphasis*
MTF*
NAVA*
NCC Group*
NEC
NetBr
Netconn
Netfive
NetSecurity
Netskope*
NetSurion
Network Secure
Network Security Professionals, Inc.
Neverhack*
Nextios
Niji*
Nomios*
Nova8
Novacoast
Novared
Noventiq
Npo Sistemas
NRI*
NTSEC
NTT DATA*
Nv7
NXO*
Okta
One Identity
Ontinue (Open Systems)*
OpenText*
Oplium
Optiv*
Optus*
Opus Tech

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

Oracle
Orange Cyberdefense*
ORBIT*
Ornisec*
OST Tecnologia
Palo Alto Networks*
pco*
Peers
Performanta*
Persistent Systems*
Post-Quantum
PQShield
Presidio*
PRIDE Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PurpleSec*
PwC*
qbeyond
Qrypt
Quantum Xchange
QuintessenceLabs
Quorum Cyber*
QuSecure
Rackspace Technology*
Radware
Rapid7
RCZ
Redbelt
ReliaQuest
Reply
Riedel Networks
Rpost
RSA Security
Safe Inc
Safeweb
SailPoint
Samsung
Scaltel
SCC*
Scunna*
SEC4U
Secureway
Secureworks*
Securiti
Security First
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sempre IT
Senhasegura
Sequretek*
Service IT*
Servix
Seti
SFR*
Sigma Telecom
Skaylink

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

Skyhigh Security*
SLK Software*
Smarttech247*
SNS Security*
Softcat PLC*
Solo Iron*
Solo Networking
Solor
Sonda*
Sophos*
Sopra Steria*
Splunk
Squad*
Stefanini*
Strati
suresecure*
SVA*
Swisscom*
Symantec
Synetis*
Syntax*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
Telefonica*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
Tidalcyber
TIVIT*
Trellix*
Trend Micro*
Trigent
T-Systems*
UMB*
Under Protection*
Unisys*
United Security Providers*
Varonis*
Vectra*
Venturus
Verizon Business*
Vigilant
VIVO
VMware Carbon Black
Vodafone
Vortex Security*
Vortex TI
Vultus*
WatchGuard
Wavestone*
Wipro*

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

Wizard Group

WWT*

Xantaro*

XYPRO Technology Corp.

You IT

Zensar Technologies*

Zscaler*

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 (Nasdaq: III) is a global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth.

The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.

For more information, visit isg-one.com.

ISG Provider Lens®

JANUARY, 2026

BROCHURE: CYBERSECURITY — SERVICES AND SOLUTIONS