ISG Provider Lens™

2022

Cybersecurity – Solutions and Services 2022

imagine your future®

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

Table of Contents

Introduction

Enterprises are adopting emerging technologies to embark on their digital transformation journey to stay competitive and align with ever-evolving end-user needs. This was further exacerbated with the COVID-19 pandemic accelerating enterprise adoption of remote work, cloud applications and other digital technologies to survive and thrive. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has led to an increase in threat attack surface. Ransomware, advanced persistent threats and phishing attacks have emerged as some of the leading cyber threats in 2022. As the nature and complexity of cyberattacks continue to increase, cybersecurity has become a priority not just for enterprises, but for government agencies as well to protect their economies, industries and citizens.

With the ever-changing threat landscape, enterprises need to take a detailed and inclusive approach to cybersecurity to safeguard their businesses by implementing a mix of security products and services across areas such as identity and access management (IAM), data leakage/loss prevention (DLP) and managed security services (MSS) to achieve a robust, secure framework to reduce risk exposure.

In addition to the need for self-protection, regulations such as the General Data Protection Regulation (GDPR) in Europe, and other regional compliances, have compelled businesses to implement robust safeguard measures to counter cyberattacks. Similar legislation exists in other countries such as Brazil and Australia to safeguard users from cyberthreats.

Although, cybersecurity has become an important practice area for enterprise CISOs, IT executives often struggle to justify security investments, as it is not always possible to measure and demonstrate the ROI as well as quantify threat-related risks. The sophistication of available technologies, difficulties in identifying and fixing vulnerabilities and the lack of awareness among end users continue to taunt enterprises and its executives.

On the other hand, deploying adequate security tools does not imply that an enterprise will be immune to vulnerabilities; the human factor continues to remain the weakest link in the security wall, which is continuously exploited by attackers through cyber threats such as Trojan and phishing attacks. A lack of awareness among end users may result in targeted attacks such as advanced persistent threats (APTs) and ransomware, impacting brand reputation, causing data and financial loss and precipitating operational outages. Therefore, user training, risk assessment and advisory services will continue to play a key role in keeping enterprise information and communications technology (ICT) infrastructure secure.

The ISG Provider Lens™ Cybersecurity – Solutions and Services 2022 study aims to support ICT decision makers in making the best use of their tight security budgets by offering the following:

- Transparency on the strengths and cautions of relevant providers.
- A differentiated positioning of providers by market segments.
- A perspective on local markets.

For IT providers and vendors, this study serves as an important decision-making basis for positioning, key relationships and go-to-market (GTM) considerations. ISG advisors and enterprise clients leverage the information from ISG Provider Lens™ reports while identifying and evaluating their current vendor relationships and potential engagements.

Quadrant Research

As part of the ISG Provider Lens™ quadrant study, this report includes six quadrants on Cybersecurity as illustrated below:

Cybersecurity - Solutions and Services 2022		
Security Solutions		
Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)
Security Services		
Managed Security Services	Technical Security Services	Strategic Security Services

Source: ISG 2022

Security Solutions

The scope of the following solutions only covers software and solution vendors that offer security software with a licensing model and as an on-demand as-a-service solution. Service providers with equivalent solutions that add value as a part of a larger project, but do not offer licensing models will not be considered for the solution quadrants.

Identity and Access Management (IAM)

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

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

Eligibility criteria:

- The solution should be capable of being deployed in combination with on-premises, cloud, identity as a service (IDaaS) and a managed third-party model.
- The solution should be capable of supporting authentication by a combination of single-sign on (SSO), multifactor authentication (MFA), risk-based and context-based models.
- The solution should be capable of supporting role-based access and PAM.
- The IAM vendor should be able to provide access management for one or more enterprise needs such as cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.
- The solution should be capable of supporting one or more legacy and newer IAM standards, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM.
- To support through secure access, the portfolio should offer one or more of the following: directory solutions, dashboard or self-service management and lifecycle management (migration, sync and replication).

Data Leakage/Loss Prevention (DLP) and Data Security

DLP vendors and solution providers are characterized by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. **Pure service providers that do not offer a DLP product (on-premises or cloud-based) based on proprietary software are not included here.** DLP solutions are offerings that can identify and monitor sensitive data, provide access for only authorized users and prevent data leakage. Vendor solutions in the market are characterized by a mix of products capable of providing visibility and control over sensitive data residing in cloud applications, endpoint, network and other devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile devices, that are being used to store data is increasing in companies. These are mostly equipped with an Internet connection and can send and receive data without passing it through a central Internet gateway. Data security solutions protect data from unauthorized access, disclosure or theft.

Eligibility criteria:

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

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

Advanced ETPDR vendors and solution providers are characterized by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. **Pure service providers that do not offer an advanced ETPDR product (on-premises or cloud-based) based on proprietary software are not included here.** This quadrant evaluates providers offering products that can provide continuous monitoring and complete visibility of all endpoints, and can analyze, prevent and respond to advanced threats. Endpoint security solutions that integrate Secure Access Service Edge (SASE) are also included here. In our consideration, endpoint security also includes the corresponding protection of operational technology (OT) solutions.

These solutions go beyond plain, signature-based protection and encompass protection from risks such as ransomware, advanced persistent threats (APTs) and malware by investigating the incidents across the complete endpoint landscape. The solution should be able to isolate the compromised endpoint and take the necessary corrective action or remediation. Such solutions comprise a database, wherein the information collected from a network and endpoints is aggregated, analyzed and investigated, and the agent that resides in the host system offers the monitoring and reporting capabilities for the events.

Eligibility criteria:

- The solution provides comprehensive and total coverage and visibility of all endpoints in a network.
- The solution demonstrates effectiveness in blocking sophisticated threats such as advanced persistent threats, ransomware and malware.
- The solution leverages threat intelligence, analyzes and offers real-time insights on threats emanating across endpoints.
- The solution should include automated response features that include, but are not limited to, deleting malicious files, sandboxing, ending suspicious processes, isolating infected endpoint and blocking suspicious accounts.

Security Services

The scope of the following services only cover providers that offer security services with a dedicated and certified team of experts. Product and solution vendors with equivalent offerings that add value only with their solution as a part of support services, will not be considered for the services quadrants.

Managed Security Services (MSS)

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

Eligibility criteria:

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

Technical Security Services (TSS)

TSS covers integration, maintenance and support for both IT and operational technology (OT) security products or solutions. DevSecOps services are also included here. TSS addresses all security products, including anti-virus, cloud, and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, SASE and others. **This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.**

Eligibility criteria:

- Demonstrate experience in implementing cyber security solutions for companies in the respective country.
- Authorized by security technology vendors (hardware and software) to distribute and support security solutions.
- Providers should employ certified experts (vendor-sponsored, association- and organization-led credentials, government agencies) capable of supporting security technologies.

Strategic Security Services (SSS)

SSS primarily covers consulting for IT and OT security. Services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting and awareness and training. These services are used to assess security maturity and risk posture, and define cybersecurity strategy for enterprises (tailored to specific requirements). **This quadrant examines service providers that are not exclusively focus on proprietary products or solutions.** The services analyzed here cover all security technologies, especially OT security and SASE.

Eligibility criteria:

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

Quadrants by Region

As part of the ISG Provider Lens™ Quadrant Study, we are introducing the following six quadrants (market) research on Cybersecurity - Solutions & Services 2022 by region:

Quadrants	U.S.	U.K	Nordics	Germany	Switzerland	France	Brazil	Australia	Singa-pore & Malaysi	U.S. Public sector
Identity and Access Management (IAM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Leakage/Loss Prevention (DLP) and Data Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed Security Services (MSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Schedule

The research phase falls in the period between **February and March 2022** during which survey, evaluation, analysis and validation will take place. The results will be presented to the media in **July 2022.**

Milestones	Beginning	End
Launch	February 16, 2022	
Survey Phase	February 16, 2022	March 14, 2022
Sneak Preview	April 2022	
Press release	July 2022	

Please click this link to view/download the ISG Provider Lens™ 2022 research agenda.

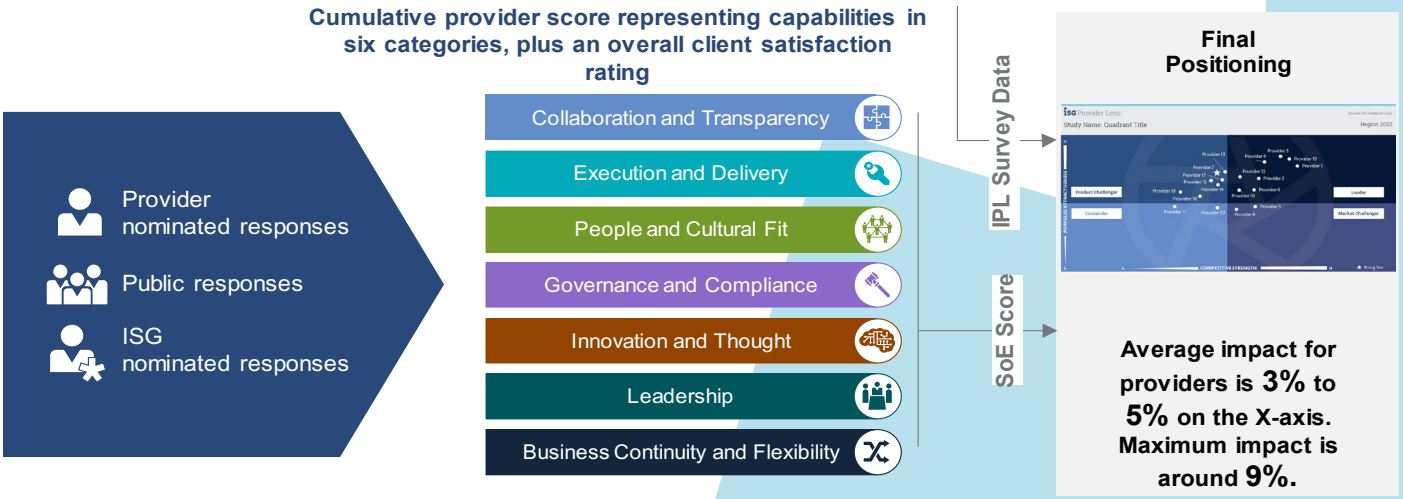
Access to Online Portal

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!

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 program, designed by ISG, collects client feedback about a service provider's 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. 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@isg-one.com

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 work identified by the 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 to produce ISG Provider Lens™ reports. These decisions will be made based on the level and completeness of 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.

Partial list of companies being invited for the survey

Are you in the list or do you see your company as a relevant provider that is missing in the list? Then feel free to contact us to ensure your active participation in the research phase.

2Secure
Absolute Software
Accenture
Actifio
Acuity Risk Management
ADT Cybersecurity (Datashield)
Advanced
Advenica
Agility Networks Tecnologia
Akamai
Alert Logic
AlgoSec
All for One
Amazon Web Services
Aqua Security Software
Arcserve
Arctic Wolf
Ascentor
AT&T
Atomicorp
Atos
Attivo Networks
Auth0
Avatier
Avectris
Axians
Axis Security
BAE Systems
Barracuda Networks
BDO Norway
Bechtle
BehavioSec
Beijaflore
Beta Systems
BetterCloud
BeyondTrust
BigID
Bitdefender
Bitglass
Bittium
BlueSteel Cybersecurity
BlueVoyant
BluVector
BoldonJames
Booz Allen Hamilton
Brainloop
Bricata
Bridewell Consulting
Broadcom
BT
CANCOM
Capgemini
Carbon Black
Censornet
Centrify
CenturyLink
CGI
Check Point
Chronicle Security
CI Security
Cigniti
Cipher
Cisco
Citrix
Claranet
Clavister
Clearswift
Cloud Range
CloudCodes
Cloudflare
CloudPassage
Cocus
Code42
Cognizant
ColorTokens
Column Information Security
Combitech
Comodo
Compasso UOL
Compugraf
Computacenter

Partial list of companies being invited for the survey

Are you in the list or do you see your company as a relevant provider that is missing in the list? Then feel free to contact us to ensure your active participation in the research phase.

Confluera
Contrast Security
Controlware
Core
Coromatic
CorpFlex
CoSoSys
Crowdstrike
Cryptomathic
CSIS Security Group
CTR Secure Services
Cyber 1
Cyber CX
Cyber Security Services
Cyber Swiss
CyberArk
Cybercom Group
Cybereason
CyberSecOp Consulting
Cygilant
Cylance
CymbiQ
Cynet
Cypher
Darktrace
Datadog
deepwatch
Deloitte
Deutsche Telekom Security
DeviceLock
Digital Guardian
DriveLock
Dubex
Duo Security, Inc (part of Cisco)
DXC
Econet
ECSC
Efecte
Elastic
Embratel
EmpowerID
Enfogroup
Ergon
Ericsson
eSentire Inc.
ESET
E-Trust
Evidian
Exabeam
Expel, Inc.
ExtraHop
EY
fasthelp
Fidelis
FireEye
Fischer Identity
Forcepoint
Forescout Technologies
Forgerock
Fortinet
Framework Security
F-Secure
Fujitsu
GBS
Giesecke + Devrient
Google DLP
GuidePoint Security
HCL
Heimdal Security
Herjavec Group
Hexaware
HID Global
Hitachi
Huawei
HyTrust
IBLISS
IBM
ID North
Idaptive
Imperva
InfoGuard

Partial list of companies being invited for the survey

Are you in the list or do you see your company as a relevant provider that is missing in the list? Then feel free to contact us to ensure your active participation in the research phase.

Infosys
Ingalls Information Security
Innofactor
Insta
Intercede
Intrinsec
Inuit
IronDefense
ISH Tecnologia
ISPIN
It4us
itWatch
Juniper Networks
Kasada
Kaspersky
KPMG
Kudelski
Lacework
Logicalis
LogicMonitor
LogRhythm
Lookout
LTI
Malwarebytes
ManagedMethods
ManageEngine
Masergy
Matrix42
McAfee
Micro Focus
Microland
Microsoft
Mnemonic
MobileIron
MonoSign
Morphisec
Mphasis
Napatech
Nazomi Networks
NCC group
NEC (Arcon)
NetNordic Group
Netsecurity AS
Netskope
Nettitude
NEVIS
Nextios
Nexus
Nixu Corporation
NTT
Okta
Omada
One Identity
OneLogin
Onevinn
Open Systems
Open Text
Optimal IdM
Optiv Security
Oracle
Orange Cyberdefense
Orca Security
Outpost24
Paladion
Palo Alto Networks
Panda Security
Perimeter 81
Persistent
Ping Identity
Pointsharp
PrimeKey
Privitar
Proficio Carlsbad
Proofid
ProofPoint
Protiviti/ICTS
PwC
QinetiQ
Qualys
Radiant Logic
Radware

Partial list of companies being invited for the survey

Are you in the list or do you see your company as a relevant provider that is missing in the list? Then feel free to contact us to ensure your active participation in the research phase.

Rapid7
Raytheon
Red Canary
Redscan
RiskIQ
Rook Security
RSA
SailPoint
Salesforce
Salt Security
SAP
Saviynt
Schneider Electric
SecureAuth
SecureTrust
Secureworks
Securonix
senhasegura
SentinelOne
Sentor
Service IT
Simeio
SIX Group
Software AG
SoftwareONE
SolarWinds
Sonda
SonicWall
Sophos
Sopra Steria
Spirion
SSH Communications Security
Stefanini
StratoKey
Sumo Logic
Swisscom
Synopsys
Synoptek
Sysdig
Tanium
TBG Security
TCS
TDec Network
Tech Mahindra
Telefonica Cibersecurity Tecnologia SA
Telia Cygate
Telos
Tempest Security Intelligence
Tesserent
Thales/Gemalto
Thirdspace
Threat Stack
ThreatConnect
Thycotic
ti8m
TietoEvry
Titus
TIVIT
Trend Micro
TrueSec
Trustwave
Ubisecure
Unisys
United Security Providers
Varonis
Vectra
Verizon
VMware
Watchcom Security Group
Watchguard
Webroot
Wipro
XenonStack
Yubico
Zacco
Zensar
ZeroFOX
Zscaler

Contacts for this study

Frank Heuer
Lead Analyst - Germany, Switzerland

Benoit Scheuber
Lead Analyst, France

Gowtham Kumar
Lead Analyst, U.S.

Dr. Maxime Martelli
Co-Lead Analyst, France

Arun Kumar Singh
Lead Analyst - U.K., Nordics

Keao Caindec
Lead Analyst, U.S. Public Sector

Craig Baty
Lead Analyst, Australia

Monica K
Research Analyst

Sergio Rezende
Lead Analyst, Brazil

Ridam Bhattacharjee
Project Manager

Do you need any further information?

If you have any questions, please do not hesitate to contact us at ISG.ProviderLens@isg-one.com.

ISG Provider Lens QCRT Program Description

ISG Provider Lens offers market assessments incorporating practitioner insights, reflecting regional focus and independent research. ISG ensures advisor involvement in each study to cover the appropriate market details aligned to the respective service lines/technology trends, service provider presence and enterprise context. In each region, ISG has expert thought leaders and respected advisors who know the provider portfolios and offerings as well as enterprise requirements and market trends. On average, three advisors participate as part of each study's quality and consistency review team (QCRT). The QCRT ensures each study reflects ISG advisors' experience in the field, which complements the primary and secondary research the analysts conduct. ISG advisors participate in each study as part of the QCRT group and contribute at different levels depending on their availability and expertise.

The QCRT advisors:

- help define and validate quadrants and questionnaires,
- advise on service providers inclusion, participate in briefing calls,
- give their perspectives on service provider ratings and review report drafts.

The ISG Provider Lens QCRT program helps round out the research process, supporting comprehensive research-focused studies.

Quality & Consistency Review Team for this study

Doug Saylors
Co-lead, ISG Cybersecurity

Roger Albrecht
Co-lead, ISG Cybersecurity

Anand Balasubramanium
Senior Consultant

Do you need any further information?

If you have any questions, please do not hesitate to contact us at ISG.ProviderLens@isg-one.com.