ISG Provider Lens™

2022

Cybersecurity – Solutions & Services 2022 - U.S. Public Sector

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

Public Sector entities in the U.S., including state and municipal governments, public utilities, safety, educational institutes and non-governmental organizations (NGOs) increasingly face cyber threats as they adapt to different ways of working in the post-pandemic business environments.

ISG's analysis of 2022 market data indicates an ever widening range of concerns among U.S. Public Sector CIOs and CISOs that include the following:

- Threat from external hacking organizations, including foreign governments and the general hacking community
- Expanding threat horizons from increasing remote work environments
- Reducing ability and time to respond to cyber threats
- Inadequately trained or careless employees in an organization
- Threats from ransomware, malware and phishing attacks
- Inadequate data collection and monitoring
- Budget constraints and resource limits

Dealing with these concerns becomes more challenging due to the nature of public sector work and IT in the U.S. Organizations often have complex legacy infrastructures, systems and data types that vary based on organizational and functional requirements. Multiple entities inside and outside public agencies require access to current and historical, public and private data. Meanwhile, organizations are struggling to implement, extend and support the still-emerging digital remote work reality, which, in turn, can vary by worker role; organizational function; and local, state and federal regulations.

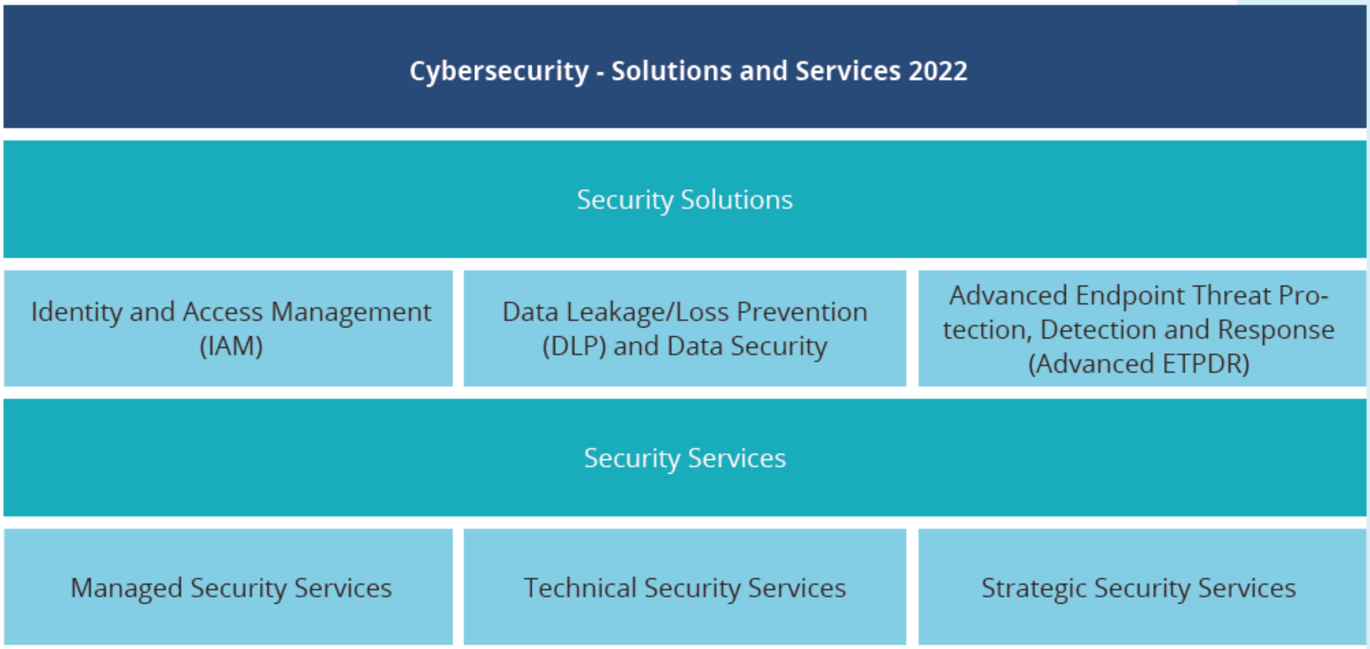
This ISG Provider Lens™ U.S. Public Sector Cybersecurity Solutions & Services 2022 study supports government and non-government IT decision-makers in their evaluation of providers, services and solutions by offering the following:

- Segmentation and assessment of solutions and services by critical offering type
- Transparency on the strengths and weaknesses of relevant providers
- Differentiated positioning of providers by market segments

For IT services providers and solution vendors, this study serves as an important decision-making basis for positioning key relationships and go-to-market considerations. ISG advisors, enterprises, and public sector clients are able to leverage the information from ISG Provider Lens™ reports, while evaluating their current vendor relationships and potential engagements.

Quadrants Research

This study assesses cybersecurity providers and offerings 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

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 and device identities. This quadrant also includes Software as a Service, based on proprietary software. Pure service providers that do not offer an IAM product based on proprietary software are not included here. Depending on unique organizational requirements, these solutions could be deployed in several ways — on-premises, in the cloud (managed by the customer), as an As-a-Service model or a combination thereof.

IAM solutions are aimed at collecting, recording and administering 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 that align with governance and compliance requirements. To handle existing and new application requirements, IAM solutions are increasingly embedded with security mechanisms, frameworks and automation (for example, risk analyses) within their management suites to provide real-time attack profiling functionalities. Solution providers are also expected to provide additional features that address the security needs of mobile users and a variety of enterprise and edge devices that go beyond traditional web and context-related rights management.

Eligibility criteria

- Relevance (revenue and number of customers) as an IAM product vendor in the U.S.
- IAM offerings should be based on proprietary software and not on a third-party software.
- The solution should be capable of being deployed in either, or by a combination of, on-premises, cloud, Identity as a Service (IDaaS) and managed (third-party) model.
- The solution should be capable of supporting authentication either, or by a combination of, single-sign on (SSO), multifactor authentication (MFA), passwordless authentication, and 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, endpoints, 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, FIDO2, WebAuthn, WS-Federation, WS-Trust and SCIM.
- The solution should be capable of supporting identity lifecycle management for provisioning and managing credentials such as passwords, keys, public key infrastructure (PKI) certificates and biometric information (fingerprint, facial recognition or iris scan).
- To support secure access, the portfolio should offer one or more of the following: directory solutions, dashboard or self-service management, and identity 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, based on proprietary software are not included here. DLP solutions are offerings that can identify and monitor sensitive data, provide access to 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, endpoints, networks and other devices.

These solutions should be able to identify sensitive data, enforce policies, monitor traffic and improve data compliance. They are gaining considerable importance because it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile, that are 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. The devices are supplied with a multitude of interfaces, such as USB ports, Bluetooth, wireless local area network (WLAN) and near-field communication (NFC), which enable data sharing. Data security solutions protect data from unauthorized access, disclosure or theft.

Eligibility criteria

- Relevance (revenue and number of customers) as a DLP product vendor in the U.S.
- 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.

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 based on proprietary software are not included here. This quadrant evaluates providers offering products that can provide continuous monitoring and total visibility of all endpoints, and can analyze, prevent and respond to advanced threats.

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

Eligibility criteria

- Relevance (revenue and number of customers) as an advanced ETPDR product vendor in the U.S.
- The advanced ETPDR offering should be based on proprietary software and not on a third-party software.
- The providers’ solutions should provide comprehensive and total coverage and visibility of IT and OT endpoints in the network.
- The solution should demonstrate effectiveness in blocking sophisticated threats such as advanced persistent threats, ransomware and malware.
- The solution should leverage threat intelligence, analyze and offer real-time insights on threats emanating across endpoints.

Managed Security Services (MSS)

MSS comprises the operations and management of IT security infrastructures for one or several customers by a security operations center (SOC). Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, IAM operation services, DLP operations, and all other operating services to provide ongoing, real-time protection without compromising on business performance. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate the best-of-breed security tools. They can handle the entire security incident lifecycle, starting from identification to resolution.

Eligibility criteria

- Ability to provide security services such as detection and prevention; security information and event management (SIEM); security advisor and auditing support, remotely, or at the client site.
- Relevance (revenue and number of customers) as an MSS provider in the U.S.
- Not exclusively focused on proprietary products but can manage and operate the best-of-breed security tools.
- Possess accreditations from vendors of both IT and OT security tools.
- SOCs ideally owned and managed by the provider and not predominantly by partners.
- Maintain 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)

This quadrant examines service providers that do not focus exclusively on their respective proprietary products and can implement and integrate other vendor products or solutions. TSS covers integration, maintenance and support for IT and OT security products or solutions. TSS addresses all security products, including anti-virus, cloud, and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM) and others.

Eligibility criteria

- Demonstrate experience in implementing security solutions for companies in the U.S.
- Not exclusively focused on proprietary products.
- Authorized by vendors to distribute and support IT and OT security solutions.
- Certified experts to support its security technologies.
- Ability to participate (desirable, not mandatory) in local security associations and certification agencies.

Strategic Security Services (SSS)

SSS primarily covers consulting for IT security. Some of the services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity, risk posture, and define cybersecurity strategy for enterprises. This quadrant examines service providers that do not have an exclusive focus on proprietary products or solutions. The services analyzed here cover all security technologies.

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 U.S.
- Execution of security consulting services using frameworks will be an advantage.
- No exclusive focus on proprietary products or solutions.

Quadrants by Region

Quadrants	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 refer to this link below to view/download the ISG Provider Lens™ 2022 research agenda.

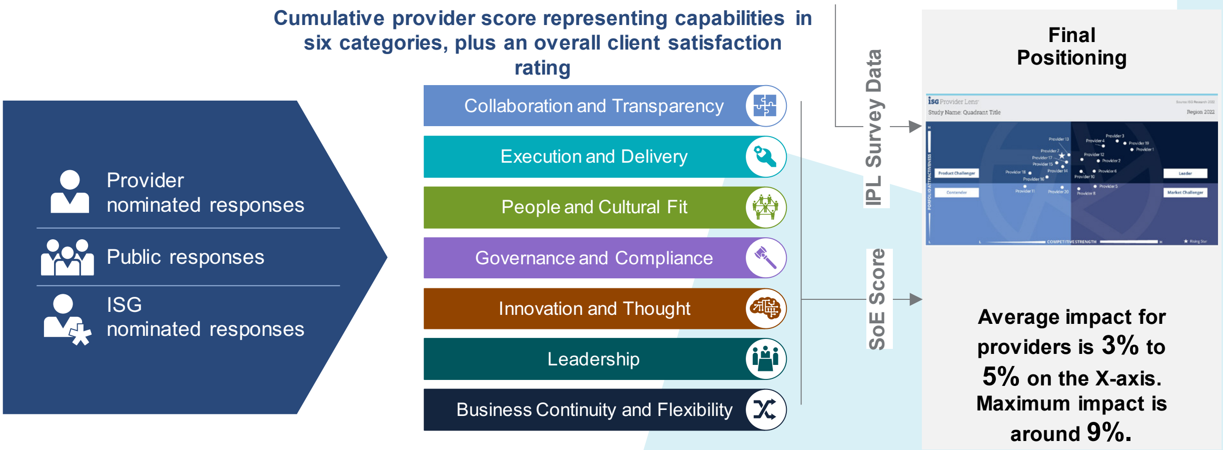
Access to Online Portal

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 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.



Cumulative provider score representing capabilities in six categories, plus an overall client satisfaction rating

Provider nominated responses

Public responses

ISG nominated responses

Collaboration and Transparency

Execution and Delivery

People and Cultural Fit

Governance and Compliance

Innovation and Thought

Leadership

Business Continuity and Flexibility

IPL Survey Data

SoE Score

Final Positioning

Average impact for providers is 3% to 5% on the X-axis. Maximum impact is around 9%.

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.

List of companies to be invited for the survey

Are you on the list, or do you see your company as relevant provider that is missing from 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

Armis

Ascentor

AT&T

Atomicorp

Atos

Attivo Networks

Auth0

Authy

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

Claroty

Clavister

Clearswift

Cloud Range

CloudCodes

List of companies to be invited for the survey

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

Cloudflare

CloudPassage

Cocus

Code42

Cognizant

ColorTokens

Column Information Security

Combitech

Comodo

Compasso UOL

Compugraf

Computacenter

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

Dell RSA

Deloitte

Deutsche Telekom

DeviceLock

Digicert

Digital Guardian

DriveLock

Dubex

Duo Security, Inc (part of Cisco)

DXC

Econet

ECSC

Efecte

Elastic

Embratel

EmpowerID

Enfogroup

Entrust

Ergon

Ericsson

eSentire Inc.

ESET

E-Trust

Evidian

Exabeam

Expel, Inc.

ExtraHop

EY

fasthelp

Fidelis

FireEye

Fischer Identity

Forcepoint

List of companies to be invited for the survey

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

Forescout Technologies
Forgerock
Fortinet
Framework Security
F-Secure
Fujitsu
GBS
Giesecke + Devrient
Google Cloud Platform
Google DLP
GlobalSign
GuidePoint Security
HCL
Heimdal Security
Herjavec Group
Hexaware
Hexagon
HID Global
Hitachi
Huawei
HyTrust
IBLISS
IBM
ID North

Idaptive
Imperva
InfoGuard
Infosys
Ingalls Information Security
Innofactor
Insta
Intercede
Intrinsec
Inuit
IronDefense
ISH Tecnologia
ISPIN
It4us
itWatch
Juniper Networks
Kasada
Keyfactor
KPMG
Kudelski
Lacework
Logicalis
LogicMonitor
LogRhythm

Lookout
LTI
Malwarebytes
ManagedMethods
ManageEngine
Masergy
Matrix42
McAfee
Micro Focus
Microland
Microsoft
Microsoft Azure
Microsoft Defender
Mnemonic
MobileIron
MonoSign
Morphisec
Mphasis
Napatech
NCC group
NEC (Arcon)
NetNordic Group
Netsecurity AS
Netskope

List of companies to be invited for the survey

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

Nettitude

NEVIS

Nextios

Nexus

Nixu Corporation

NokNok Labs

Nozomi Networks

NTT

Okta

Omada

One Identity

OneLogin

Onevinn

Open Systems

Open Text

Opswat

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

Rapid7

Raytheon

Red Canary

Redscan

RiskIQ

Rook Security

SailPoint

Salesforce

Salt Security

SAP

Saviynt

Schneider Electric

SecureAuth

SecureTrust

Secureworks

Sectigo

Securonix

senhasegura

SentinelOne

Sentor

Service IT

Simeio

SIX Group

Software AG

SoftwareONE

SolarWinds

Sonda

SonicWall

Sophos

Sopra Steria

Spirion

SSH Communications Security

List of companies to be invited for the survey

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

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

T-Systems

Ubisecure

Unisys

United Security Providers

Utimaco

Varonis

Vectra

Verizon

Vmware

Watchcom Security Group

Watchguard

Webroot

Wipro

XenonStack

Yubico

Zacco

Zensar

ZeroFOX

Zscaler

Contacts for this study

Keao Caindec

Lead Analyst, U.S. Public Sector

Gowtham Kumar

Lead Analyst, U.S.

Monica K

Research Analyst

Ridam Bhattacharjee

Project Manager

Do you need any further information?

If you have any questions, please contact us at isglens@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 contact us at isglens@isg-one.com.