ISG Provider Lens™

2021

Cybersecurity – Solutions & Services 2021

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 700 clients, including 75 of the top 100 enterprises in the world, 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; technology 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 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

Definition

Enterprises are swiftly adopting new technologies to embark on digital transformation journeys to stay competitive and align with ever-evolving end-user needs. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has led to an increase in exposure and a growing threat attack surface. Ransomware, advanced persistent threats, and phishing attacks emerged as some of the leading cyberthreats in 2020. Experian, SolarWinds, Zoom, Magellan Health, Finastra and Marriott were some of the leading entities that faced cyberattacks from hacking, malicious code, and ransomware over the last year.

Attackers are always looking for new and Ingenious ways to breach the defense mechanisms. This has led to an increase in their sophistication, as these attackers access different points in an enterprise IT ecosystem such as supply chain networks to breach security. The year 2020 witnessed several other high-profile cyberattacks. The attacks targeted the intellectual property, personal identifiable information (PII) and confidential records, and client information of enterprises across the healthcare, hospitality, IT, finance, and other industries, along with data belonging to nation states. Apart from causing operational damage, these attacks impacted brand value, IT systems and the financial health of the targeted organizations.

The global threat scenario was further exacerbated in 2020 with the COVID-19 pandemic, which resulted in a large number of professionals working remotely, mainly from home. This new work model resulted in an increased use of collaboration tools and platforms and public networks and exposed users to hackers through attack vectors such as phishing and other malicious threats. With this 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 security and managed security services (MSS) to achieve a robust secure framework that is suited to their needs and vision.

As the nature and complexity of cybersecurity threats continue to increase, hackers are constantly searching and targeting vulnerable sources and IT infrastructures. Some threats such as phishing, spear phishing and ransomware aim to benefit from the ignorance of people and their online behavior. The increased level of online activity, led by e-commerce and online transactions, has broadened the vulnerability stance and exposed end users to cybercriminals who are looking for any digital traces left behind for them. This makes users and IT endpoint systems with low security posture and weak defense mechanisms easy prey to cyberattacks.

The serious implications faced by enterprises from phishing and ransomware threats have led to the emergence of services to counter such advanced threats. These services and solutions extend beyond basic perimeter and conventional security measures and offer continuous deep monitoring, inspection, and protection, along with a structured incident response approach. In addition to the need for self-protection, laws, and regulations such as the General Data Protection Regulation (GDPR) in Europe have led businesses to implement stronger safeguard measures to counter cyberattacks. Similar legislation exists in other countries such as Brazil and Australia to safeguard users from cyberthreats and attacks.

Cybersecurity has become an important practice area for enterprises due to its impact on businesses and their processes. However, IT executives often struggle to justify security investments to business stakeholders, particularly the CFO. Unlike other IT projects, it is not always possible to measure and demonstrate the return on investment (ROI) as well as quantify threat-related risks. Therefore, security measures are often at a low level and are not sufficient to address sophisticated threats. On the other hand, the availability of suitable technology does not always result in the elimination of vulnerabilities; many security incidents such as Trojan and phishing attacks are caused due to the ignorance of end users. Awareness related aspects among end users may result in targeted attacks such as advanced persistent threats and ransomware, which impact brand reputation as well as cause data and financial losses, in addition to operational outages. Therefore, consulting and user training continue to play a key role, together with up-to-date ICT infrastructure. The rising complexity in threats has also led to an increased focus on monitoring, detection, and response services to safeguard the enterprises beyond perimeter; signature-based protection; and other security services.

Definition (cont.)

The ISG Provider Lens™ Cybersecurity - Solutions & Services 2021 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 weaknesses 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 considerations. ISG advisors and enterprise clients also leverage the information from ISG Provider Lens™ reports while evaluating their current vendor relationships and potential new engagements.

Quadrants Research

As part of the ISG Provider Lens™ quadrant study, this report includes six quadrants on cybersecurity illustrated below.

Simplified illustration

Source: ISG 2021

Identity and Access Management (IAM)

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services to meet unique demand 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 self-developed software are not included here. Depending on the organizational requirements, these solutions could be deployed in several ways such as on-premises or on cloud (managed by customer) or 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 features related to social media and mobile users to address their security needs 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 respective country.
- IAM offerings should be based on proprietary software and not on 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 a 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), risk-based and context-based models.
- The solution should be capable of supporting role-based access and privileged access management.
- 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 self-developed 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 should be able to discover sensitive data, enforce policies, monitor traffic, and improve data compliance. They are gaining considerable importance as it has become more 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 respective country.
- The DLP offering should be based on proprietary software and not on 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 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 (on-premises or cloud-based) based on self-developed 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 adversaries 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 infected endpoint and take the necessary corrective action/remediation. Such solutions comprise a database, wherein the information collected from network and endpoints is aggregated, analyzed, and investigated, and an agent that resides in the host system and 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 respective country.
- The advanced ETPDR offering should be based on proprietary software and not on third-party software.
- The providers' solutions should provide comprehensive and total coverage and visibility of all 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 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. These service providers 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); and security advisor and auditing support, remotely or at the client site.
- Relevance (revenue and number of customers) as an MSS provider in the respective country.
- Not exclusively focused on proprietary products but can manage and operate the best-of-breed security tools.
- Possess accreditations from vendors of 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), Global Information Assurance Certification (GIAC), etc.

Technical Security Services (TSS)

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. TSS covers integration, maintenance and support for IT 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 respective country.
- Not exclusively focused on proprietary products.
- Authorized by vendors to distribute and support 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 respective country.
- 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.	U.K.	Nordics	Germany	Switzer-land	France	Brazil	Australia
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 **March and April 2021**, during which survey, evaluation, analysis, and validation will take place. The results will be presented to the media in **July 2021**.

Milestones	Beginning	End
Launch	February 18, 2021	
Survey phase	February 18, 2021	March 15, 2021
Sneak previews	May 3, 2021	
Press release	June 21, 2021	

Please refer to the link below to view/download the Provider Lens™ 2021 research agenda: Annual Plan

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.

Partial list of companies being invited for the survey

Are you on 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

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

Boldon James

Booz Allen Hamilton

Brainloop

Bricata

Bridewell Consulting

Broadcom

BT Group

CANCOM

Capgemini

Carbon Black

Censornet

Centrify

CenturyLink

CGI

Check Point

Chronicle Security

CI Security

Cigniti

Cipher

Cisco Systems

Citrix Systems

Claranet

Clavister

Clearswift

Cloud Range

CloudCodes

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

CyberCX

Cyber Security Services

CyberArk

Cybercom Group

Cybereason

CyberSecOp Consulting

Cygilant

Cylance

CymbiQ

Cynet

Cypher

Darktrace

Datadog

deepwatch

Dell RSA

Deloitte

Deutsche Telekom

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

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

Rapid7

Raytheon

Red Canary

Redscan

RiskIQ

Rook Security

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

T-Systems

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

Craig Baty
Lead Author Australia

Frank Heuer
Lead Author Germany and Switzerland

Benoit Scheuber
Lead Author France

Monica K
Global Overview Analyst

Gowtham Kumar
Lead Author U.S.

Srinivasan P N
Global Overview Analyst

Paulo Brito
Lead Author Brazil

Project Manager

Kartik Subramaniam
Lead Author U.K. and Nordics

Dhananjay Vasudeo Koli
Global Project Manager

Do you need any further information?

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