ISG Provider Lens™

2022

Cybersecurity – Solutions and Services 2022

imagine your future®

O ISG (Information Services Group) (NASDAQ: III) é uma empresa líder mundial em pesquisa e consultoria tecnológica. Um parceiro comercial confiável para mais de 800 clientes, incluindo 75 das 100 maiores empresas do mundo, o ISG está comprometido em ajudar corporações, organizações do setor público e provedores de serviços e tecnologia a alcançar excelência operacional e crescimento mais rápido. A empresa é especializada em serviços de transformação digital, incluindo automação, analytics de nuvens e dados; consultoria em sourcing; governança gerenciada e serviços de risco; serviços de operadoras de rede; estratégia tecnológica e projeto de operações; gerenciamento de mudanças; inteligência de mercado e pesquisa e análise de tecnologia. Fundado em 2006, e sediado em Stamford, Connecticut, o ISG emprega mais de 1.300 profissionais operando em mais de 20 países - uma equipe global conhecida por seu pensamento inovador, influência de mercado, profunda experiência na indústria e tecnologia, e capacidade de pesquisa e análise de classe mundial com base nos dados de mercado mais abrangentes da indústria. Para mais informações visite www.isg-one.com.

Table of Contents

Introdução

As empresas estão adotando tecnologias emergentes para embarcar em sua jornada de transformação digital para se manterem competitivas e se alinharem às necessidades em constante evolução dos usuários finais. Isso foi ainda mais exacerbado com a pandemia da COVID-19, acelerando a adoção corporativa de trabalho remoto, aplicações em nuvem e outras tecnologias digitais para sobreviver e prosperar. A crescente adoção dessas tecnologias, juntamente com novas ferramentas para fornecer eficiência e velocidade, levou a um aumento na superfície de ataque de ameaças. Ransomware, ameaças persistentes avançadas e ataques de phishing surgiram como algumas das principais ameaças cibernéticas em 2022. À medida que a natureza e a complexidade dos ataques cibernéticos continuam a aumentar, a segurança cibernética tornou-se uma prioridade não apenas para empresas, mas também para agências governamentais para proteger suas economias, indústrias e cidadãos.

Com o cenário de ameaças em constante mudança, as empresas precisam adotar uma abordagem detalhada e inclusiva de segurança cibernética para proteger seus negócios, implementando uma combinação de produtos e serviços de segurança em áreas como gerenciamento de identidade e acesso (IAM), prevenção de vazamento/perda de dados (DLP) e serviços gerenciados de segurança (MSS) para obter uma estrutura robusta e segura para reduzir a exposição ao risco.

Além da necessidade de autoproteção, regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) na Europa e outras conformidades regionais obrigaram as empresas a implementar medidas de proteção robustas para combater ataques cibernéticos. Legislação semelhante existe em outros países, como Brasil e Austrália, para proteger os usuários de ameaças cibernéticas.

Embora a segurança cibernética tenha se tornado uma área de prática importante para os CISOs corporativos, os executivos de TI muitas vezes lutam para justificar os investimentos em segurança, pois nem sempre é possível medir e demonstrar o ROI, bem como quantificar os riscos relacionados a ameaças. A sofisticação das tecnologias disponíveis, as dificuldades em identificar e corrigir vulnerabilidades e a falta de conscientização entre os usuários finais continuam a incomodar as empresas e seus executivos.

Por outro lado, a implantação de ferramentas de segurança adequadas não implica que uma empresa seja imune a vulnerabilidades; o fator humano continua sendo o elo mais fraco no muro de segurança, que é continuamente explorado por invasores por meio de ameaças cibernéticas, como cavalos de Troia e ataques de phishing. A falta de conscientização entre os usuários finais pode resultar em ataques direcionados, como ameaças persistentes avançadas (APTs) e ransomware, afetando a reputação da marca, causando perdas financeiras e de dados e precipitando interrupções operacionais. Portanto, treinamento de usuários, a avaliação de risco e os serviços de consultoria continuarão a desempenhar um papel fundamental para manter a infraestrutura de tecnologia da informação e comunicação (TIC) da empresa segura.

O estudo ISG Provider Lens™ Cybersecurity – Solutions and Services 2022 visa apoiar os tomadores de decisão de TIC a fazer o melhor uso de seus orçamentos limitados de segurança, oferecendo o seguinte:

- Transparência quanto aos pontos fortes e de atenção dos fornecedores relevantes.
- Um posicionamento diferenciado dos fornecedores por segmentos de mercado.
- Uma perspectiva sobre os mercados locais.

Para provedores e fornecedores de TI, este estudo serve como uma importante base de tomada de decisão para posicionamento, relacionamentos-chave e considerações de entrada no mercado (GTM). Os consultores do ISG e os clientes corporativos utilizam as informações dos relatórios ISG Provider Lens™ enquanto identificam e avaliam seus relacionamentos atuais com fornecedores e outros possíveis compromissos.

Pesquisa de Quadrantes

Como parte do estudo de quadrantes ISG Provider Lens™, este relatório inclui seis quadrantes sobre segurança cibernética, conforme ilustrado abaixo:

Ilustração simplificada

Cybersecurity Solutions & Services		
Soluções de Segurança		
Identity & Access Management (IAM)	Data Leakage/Loss Prevention (DLP) & Data Security	Advanced Endpoint Threat Protection, Detection & Response (Advanced ETPDR)
Serviços de Segurança		
Technical Security Services	Strategic Security Services	Managed Security Services

Fonte: ISG 2022

Soluções de Segurança

O escopo das soluções a seguir abrange apenas fornecedores de software e soluções que oferecem software de segurança com um modelo de licenciamento e como uma solução sob demanda como serviço. Prestadores de serviços com soluções equivalentes que agregam valor como parte de um projeto maior, mas não oferecem modelos de licenciamento não serão considerados para os quadrantes da solução.

Identity & Access Management (IAM)

Os fornecedores de IAM e provedores de soluções são caracterizados por sua capacidade de oferecer software proprietário e serviços associados para gerenciar com segurança identidades e dispositivos de usuários corporativos. Este quadrante também inclui Software como Serviço baseado em software proprietário. Os provedores de serviços puros que não oferecem um produto de IAM (no local e/ou na nuvem) baseado em software proprietário não estão incluídos aqui. Dependendo dos requisitos organizacionais, essas soluções podem ser implantadas de várias maneiras, como no local ou na nuvem (gerenciado pelo cliente) ou como um modelo As-a-Service ou uma combinação deles.

As soluções de IAM visam coletar, registrar e administrar identidades de usuários e direitos de acesso relacionados, bem como acesso especializado a ativos críticos, incluindo gerenciamento de acesso privilegiado (PAM). Eles garantem que os direitos de acesso sejam concedidos com base em políticas definidas. Para lidar com os requisitos de aplicações novas e existentes, as soluções de IAM são cada vez mais incorporadas a mecanismos, estruturas e automação seguros (por exemplo, análises de risco) em seus conjuntos de gerenciamento para fornecer funcionalidades de perfil de ataque e usuário em tempo real. Os provedores de soluções também devem fornecer funcionalidades adicionais relacionadas à mídia social e ao uso de dispositivo móvel para atender às suas necessidades específicas de segurança que vão além do gerenciamento tradicional de direitos relacionados à Web e ao contexto. O gerenciamento de identidade de máquina também está incluído aqui.

Critérios de elegibilidade:

- A solução deve ser capaz de ser implantada em combinação com local, nuvem, identidade como serviço (IDaaS) e um modelo gerenciado de terceiros.
- A solução deve ser capaz de dar suporte à autenticação por uma combinação de logon único (SSO), autenticação multifator (MFA), modelos baseados em risco e baseados em contexto.
- A solução deve ser capaz de dar suporte a acesso baseado em função e PAM.
- O fornecedor de IAM deve ser capaz de fornecer gerenciamento de acesso para uma ou mais necessidades corporativas, como nuvem, endpoint, dispositivos móveis, interfaces de programação de aplicações (APIs) e aplicações da web.
- A solução deve ser capaz de oferecer suporte a um ou mais padrões de IAM legados e mais recentes, incluindo, mas não se limitando a SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust e SCIM.
- Para oferecer suporte por meio de acesso seguro, o portfólio deve oferecer um ou mais dos seguintes: soluções de diretório, painel ou gerenciamento de autoatendimento e gerenciamento do ciclo de vida (migração, sincronização e replicação).

Data Leakage/Loss Prevention (DLP) & Data Security

Os fornecedores de DLP e os provedores de soluções são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui software como serviço, baseado em software proprietário. Os provedores de serviços puros que não oferecem um produto de DLP (no local ou baseado em nuvem) com base em software proprietário não estão incluídos aqui. As soluções de DLP são ofertas que podem identificar e monitorar dados confidenciais, fornecer acesso apenas para usuários autorizados e evitar vazamento de dados. As soluções de fornecedores no mercado são caracterizadas por uma combinação de produtos capazes de fornecer visibilidade e controle sobre dados confidenciais que residem em aplicações em nuvem, endpoint, rede e outros dispositivos.

Essas soluções estão ganhando importância considerável à medida que se torna cada vez mais difícil para as empresas controlar as movimentações e transferências de dados. O número de dispositivos, incluindo dispositivos móveis, que estão sendo usados para armazenar dados está aumentando nas empresas. Estes são, na sua maioria, equipados com uma ligação à Internet e podem enviar e receber dados sem os passar por um gateway central de Internet. As soluções de segurança de dados protegem os dados contra acesso não autorizado, divulgação ou roubo.

Critérios de elegibilidade:

- A oferta de DLP deve ser baseada em software proprietário e não em software de terceiros.
- A solução deve ser capaz de dar suporte à DLP em qualquer arquitetura, como nuvem, rede, armazenamento ou endpoint.
- A solução deve ser capaz de lidar com proteção de dados confidenciais em dados estruturados ou não estruturados, texto ou dados binários.
- A solução deve ser oferecida com um suporte básico de gerenciamento, incluindo, mas não limitando a, relatórios, controles de política, instalação e manutenção e funcionalidades avançadas de detecção de ameaças.
- A solução deve ser capaz de identificar dados confidenciais, aplicar políticas, monitorar o tráfego e melhorar a conformidade dos dados.

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

Os fornecedores de ETPDR avançado e os provedores de soluções são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui software como serviço, baseado em software proprietário. Os provedores de serviços puros que não oferecem um produto de ETPDR avançado (no local ou baseado em nuvem) baseado em software proprietário não estão incluídos aqui. Este quadrante avalia os provedores que oferecem produtos que podem fornecer monitoramento contínuo e visibilidade completa de todos os endpoints, além de analisar, prevenir e responder a ameaças avançadas. As soluções de segurança de endpoint que integram o Secure Access Service Edge (SASE) também estão incluídas aqui. Em nossa análise, a segurança de endpoint também inclui a proteção correspondente de soluções de tecnologia operacional (OT).

Essas soluções vão além da proteção simples e baseada em assinatura e abrangem a proteção contra riscos como ransomware, ameaças persistentes avançadas (APTs) e malware, investigando os incidentes em todo o cenário de endpoints. A solução deve ser capaz de isolar o endpoint comprometido e tomar as medidas corretivas ou remediações necessárias. Tais soluções compreendem um banco de dados, onde as informações coletadas de uma rede e endpoints são agregadas, analisadas e investigadas, e o agente que reside no sistema host oferece os recursos de monitoramento e relatório dos eventos.

Critérios de elegibilidade:

- A solução deve oferecer cobertura e visibilidade abrangentes e totais de todos os endpoints em uma rede.
- A solução deve demonstrar eficácia no bloqueio de ameaças sofisticadas, como ameaças persistentes avançadas, ransomware e malware.
- A solução deve utilizar a inteligência de ameaças, analisar e oferecer insights em tempo real sobre ameaças que emanam de endpoints.
- A solução deve incluir recursos de resposta automatizada que incluem, mas não se limitam a exclusão de arquivos maliciosos, sandboxing, encerramento de processos suspeitos, isolamento de endpoint infectado e bloqueio de contas suspeitas.

Serviços de Segurança

O escopo dos serviços a seguir abrange apenas provedores que oferecem serviços de segurança com uma equipe de especialistas dedicada e certificada. Os fornecedores de produtos e soluções com ofertas equivalentes que agregam valor apenas com sua solução como parte dos serviços de suporte não serão considerados para os quadrantes de serviços.

Managed Security Services (MSS)

O quadrante MSS compreende as operações e o gerenciamento de infraestruturas de segurança de TI e TO para um ou vários clientes por um centro de operações de segurança (SOC). Este quadrante examina os provedores de serviços que não se concentram exclusivamente em produtos proprietários, mas podem gerenciar e operar as melhores ferramentas de segurança. Esses provedores de serviços podem lidar com todo o ciclo de vida do incidente de segurança, desde a identificação até a resolução.

Critérios de elegibilidade:

- Os serviços típicos devem incluir monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, consultoria sobre medidas de prevenção, testes de penetração, operações de firewall, operações de antivírus, serviços de operação de gerenciamento de identidade e acesso (IAM), operações de prevenção de perda/vazamento de dados (DLP) e todos outros serviços operacionais para fornecer proteção contínua e em tempo real, sem comprometer o desempenho dos negócios. Em particular, o Secure Access Service Edge (SASE) também está incluído.
- Capacidade de fornecer serviços de segurança, como detecção e prevenção; informações de segurança e gerenciamento de eventos (SIEM); e consultoria de segurança e suporte de auditoria, remotamente ou no local do cliente.
- Possuir credenciamentos de fornecedores de ferramentas de segurança.
- SOCs idealmente de propriedade e gerenciados pelo provedor e não predominantemente por parceiros.
- Manter equipe certificada, por exemplo, em Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) e Global Information Assurance Certification (GIAC).

Technical Security Services (TSS)

O quadrante TSS abrange integração, manutenção e suporte para produtos ou soluções de segurança de TI e de tecnologia operacional (TO). Os serviços de DevSecOps também estão incluídos aqui. O quadrante TSS aborda todos os produtos de segurança, incluindo antivírus, nuvem e segurança de data center, IAM, DLP, segurança de rede, segurança de endpoint, gerenciamento unificado de ameaças (UTM), segurança de TO, SASE e outros. Este quadrante examina os provedores de serviços que não têm foco exclusivo em seus respectivos produtos proprietários e podem implementar e integrar produtos ou soluções de outros fornecedores.

Critérios de elegibilidade:

- Demonstrar experiência na implementação de soluções de segurança cibernética para empresas no respectivo país.
- Estar autorizado por fornecedores de tecnologia de segurança (hardware e software) para distribuir e dar suporte a soluções de segurança.
- Os provedores devem empregar especialistas certificados (credenciados por fornecedores, associações e organizações , agências governamentais) capazes de oferecer suporte a tecnologias de segurança.

Strategic Security Services (SSS)

O quadrante SSS cobre principalmente a consultoria para segurança de TI e TO. Os serviços cobertos neste quadrante incluem auditorias de segurança, serviços de consultoria de conformidade e risco, avaliações de segurança, consultoria de arquitetura de solução de segurança e conscientização e treinamento. Esses serviços são usados para avaliar a maturidade da segurança e a postura de risco e definir a estratégia de segurança cibernética para empresas (adaptada a requisitos específicos). Este quadrante examina os provedores de serviços que não se concentram exclusivamente em produtos ou soluções proprietárias. Os serviços aqui analisados abrangem todas as tecnologias de segurança, especialmente segurança de TO e SASE.

Critérios de elegibilidade:

- Os provedores de serviços devem demonstrar habilidades em áreas de SSS, como avaliação, testes, seleção de fornecedores, consultoria de arquitetura e consultoria de risco.
- Os provedores de serviços devem oferecer pelo menos um dos SSS acima no respectivo país.
- A execução de serviços de consultoria de segurança utilizando frameworks será uma vantagem.
- Não ter foco exclusivo em produtos ou soluções proprietárias.

Quadrantes por Região

Como parte do estudo de quadrantes ISG Provider Lens™, estamos apresentando a pesquisa (de mercado) com os seguintes seis quadrantes sobre segurança cibernética - Solutions and Services 2022 por região:

Quadrante	EUA	Reino Unido	Nórdicos	Ale-manha	Suíça	França	Brasil	Austrália	Singapu-ra e Malásia	Setor público america-no
Identity & Access Management (IAM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Leakage/ Loss Prevention (DLP) & Data Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced Endpoint Threat Protection, Detection & Response (Advanced ETPDR)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Managed Security Services (MSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Cronograma

A fase de pesquisa situa-se no período entre **fevereiro e março de 2022**, durante o qual ocorrerá o levantamento, avaliação, análise e validação. Os resultados serão apresentados à mídia em **julho de 2022**.

Fases	Início	Encerramento
Lançamento	16 de fevereiro de 2022	
Fase de pesquisa	16 de fevereiro de 2022	14 de março de 2022
Prévia	abril de 2022	
Comunicado de imprensa	julho de 2022	

Consulte o link para visualizar/baixar a agenda de pesquisa ISG Provider Lens™ 2022:

Acesso ao Portal Online

Você pode visualizar/baixar o questionário here usando as credenciais que você já criou ou consultar as instruções fornecidas no e-mail de convite para gerar uma nova senha. Aguardamos sua participação!

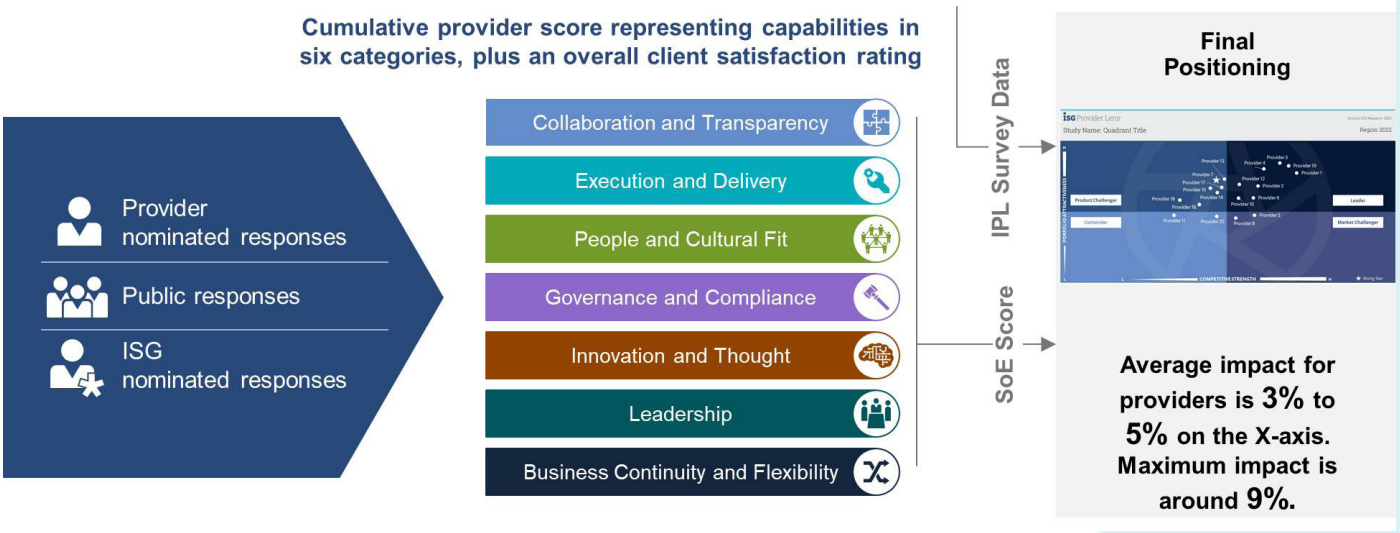
Isenção de responsabilidade da produção de pesquisa:

O ISG coleta dados com o propósito de escrever pesquisas e criar perfis de provedor/fornecedor. Perfis e dados de suporte são usados por consultores do ISG para fazer recomendações e informar seus clientes sobre a experiência e as qualificações de qualquer provedor/fornecedor aplicável para terceirizar o trabalho identificado pelos clientes. Esses dados são coletados como parte do processo ISG FutureSource e do processo Candidate Provider Qualification (CPQ). O ISG pode escolher usar apenas os dados coletados relativos a determinados países ou regiões para a educação e os propósitos de seus conselheiros e não produzir relatórios ISG Provider Lens™. Essas decisões serão tomadas com base no nível e integridade das informações recebidas diretamente de provedores/fornecedores e na disponibilidade de analistas experientes para esses países ou regiões. As informações enviadas também podem ser usadas para projetos de pesquisa individuais ou para notas informativas que serão escritas por analistas líderes.

ISG Star of Excellence™ – Chamada para nomeações

O Star of Excellence é um reconhecimento independente da excelente prestação de serviços com base no conceito de "Voz do Cliente". O programa foi desenvolvido pelo ISG para coletar feedback dos clientes sobre o sucesso dos provedores de serviços em demonstrar os mais altos padrões de excelência no atendimento ao cliente e foco no cliente.

A pesquisa global é sobre serviços associados a estudos de IPL. Todos os analistas do ISG receberão continuamente informações sobre a experiência do cliente de todos os provedores de serviços relevantes. Esta informação é acrescentada ao feedback existente em primeira mão do consultor que o IPL utiliza no contexto de sua abordagem de consultoria liderada por profissionais.



Os provedores são convidados a nominate seus clientes para participar. Uma vez que a nomeação tenha sido submetida, o ISG envia uma confirmação por correio para ambos os lados. É evidente que o ISG anonimiza todos os dados do cliente e não os compartilha com terceiros.

É nossa visão que o Star of Excellence seja reconhecido como o principal reconhecimento da indústria pela excelência no atendimento ao cliente e sirva como referência para medir os sentimentos do cliente.

Para garantir que seus clientes selecionados completem o feedback para seu compromisso indicado, use a seção de indicação de clientes no website da Star of Excellence.

Criamos um e-mail onde você pode direcionar qualquer dúvida ou fazer comentários. Este e-mail será verificado diariamente, aguarde até 24 horas para ter uma resposta. Aqui está o endereço de e-mail: Star@isg-one.com

Lista parcial de empresas a serem convidadas para a pesquisa

Você está na lista ou vê sua empresa como um fornecedor relevante que esteja faltando na lista? Então sinta-se à vontade para entrar em contato conosco para garantir sua participação ativa na fase de pesquisa.

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
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
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

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

Contatos para este estudo

Frank Heuer
Analista Líder - Alemanha, Suíça

Gowtham Kumar
Analista Líder, EUA

Arun Kumar Singh
Analista Líder – Reino Unido, Países Nórdicos

Benoit Scheuber
Analista Líder, França

Dr. Maxime Martelli
Analista Co-líder, França

Craig Baty
Analista Líder, Austrália

Sergio Rezende
Analista Líder, Brasil

Keao Caindec
Analista Líder, EUA, Setor Público

Monica K
Analista de Pesquisa

Ridam Bhattacharjee
Gerente de Projeto

Descrição do programa ISG Provider Lens QCRT

O ISG Provider Lens™ oferece avaliações de mercado incorporando insights de profissionais, refletindo o foco regional e conduzindo pesquisas independentes. O ISG garante o envolvimento do consultor em cada estudo para cobrir os detalhes de mercado apropriados alinhados às respectivas linhas de serviço/tendências de tecnologia, presença do provedor de serviços e contexto empresarial. Em cada região, o ISG tem líderes de opinião especializados e consultores respeitados que conhecem os portfólios e ofertas dos fornecedores, bem como os requisitos empresariais e as tendências do mercado. Em média, três consultores participam como parte da Equipe de Revisão de Qualidade e Consistência (QCRT) de cada estudo, que garante que cada estudo reflita a experiência dos consultores do ISG no campo, o que complementa a pesquisa primária e secundária que os analistas realizam. Os orientadores participam de cada estudo como parte do grupo QCRT e contribuem em diferentes níveis, dependendo de sua disponibilidade e experiência.

Os conselheiros QCRT:

- Ajudam a definir e a validar quadrantes e questionários,
- Aconselham sobre a inclusão de prestadores de serviços, participam de chamadas de briefing,
- Compartilham suas perspectivas sobre as classificações dos provedores de serviços e revisam os rascunhos dos relatórios.

O programa ISG Provider Lens QCRT ajuda a completar o processo de pesquisa, apoiando estudos abrangentes focados em pesquisa.

Equipe de Revisão de Qualidade e Consistência para este estudo

Doug Saylors
Co-líder, ISG Cibersegurança

Roger Albrecht
Co-líder, ISG Cibersegurança

Anand Balasubramanium
Consultor Sênior

Você precisa de mais alguma informação?

Se você tiver alguma dúvida, não hesite em nos contatar em isglens@isg-one.com.