ISG Provider Lens™

2021

Cybersecurity – Solutions & Services 2021

imagine your future®

ISG (Information Services Group) (NASDAQ: III) é uma empresa global líder em consultoria e pesquisa de tecnologia. Uma parceira de negócios confiável para mais de 700 clientes, incluindo 75 das maiores 100 empresas do mundo, a ISG é comprometida em ajudar corporações, organizações do setor público e fornecedores de serviços e de tecnologia a alcançar a excelência operacional e crescimento mais rápido. A empresa se especializa em serviços de transformação digital, incluindo serviços de automação, análises de dados e nuvem; consultoria de fornecimento; governança gerenciada e de risco; serviços de fornecimento de rede; estratégia de tecnologia e design de operações; gerenciamento de mudança; inteligência de mercado, pesquisa e análise de tecnologia. Fundada em 2006, com base em Stamford, Conn., a ISG emprega mais de 1.300 profissionais, operando em mais de 20 países – uma equipe global conhecida por seu pensamento inovador, influência no mercado, expertise profunda em indústria e tecnologia, capacidades analíticas e de pesquisa de qualidade internacional com base nos dados de mercado mais abrangentes da indústria. Para mais informações, acesse www.isg-one.com.

Table of Contents

Definição

As empresas estão adotando rapidamente novas tecnologias para embarcar em jornadas de transformação digital para se manterem competitivas e alinhadas com as necessidades do usuário final que estão em constante evolução. A crescente adoção dessas tecnologias, junto com novas ferramentas para fornecer eficiência e velocidade, causou um aumento na exposição e uma superfície de ataque de ameaças cada vez maior. Ransomware, ameaças persistentes avançadas e ataques de phishing surgiram como algumas das principais ameaças cibernéticas de 2020. Experian, SolarWinds, Zoom, Magellan Health, Finastra e Marriott foram algumas das principais entidades que enfrentaram ataques cibernéticos de hackers, códigos maliciosos e ransomware no ano passado.

Os invasores estão sempre procurando maneiras novas e originais de violar os mecanismos de defesa. Isso causou um aumento na sofisticação desses invasores, à medida que eles acessam diferentes pontos em um ecossistema de TI corporativo, como redes da cadeia de suprimentos, para violar a segurança. O ano de 2020 foi testemunha de vários outros ataques cibernéticos de alto perfil. Os ataques visavam propriedade intelectual, informações de identificação pessoal (IIP), registros confidenciais e informações de clientes de empresas nos setores de saúde, hospitalidade, TI, finanças e outros, junto com dados pertencentes a estados-nações. Além de causar danos operacionais, esses ataques afetaram o valor da marca, os sistemas de TI e a saúde financeira das organizações que os enfrentaram.

O cenário de ameaça global foi ainda mais agravado em 2020 com a pandemia da COVID-19, que resultou em um grande número de profissionais trabalhando remotamente, principalmente em casa. Esse novo modelo de trabalho resultou em um maior uso de ferramentas e plataformas de colaboração e redes públicas e expôs os usuários a hackers por meio de vetores de ataque, como phishing e outras ameaças maliciosas. Com este cenário de ameaças em constante mudança, as empresas precisam adotar uma abordagem para a segurança cibernética que seja detalhada e inclusiva para proteger seus negócios, implementando uma combinação de produtos e serviços de segurança em áreas como gestão de identidade e acesso (IAM), segurança de dados e serviços gerenciados de segurança (MSS) para obter uma estrutura robusta e segura que seja adequada às suas necessidades e visão.

Conforme a natureza e a complexidade das ameaças à segurança cibernética continuam a aumentar, os hackers estão constantemente procurando e visando fontes e infraestruturas de TI vulneráveis. Algumas ameaças, como phishing, spear phishing e ransomware, tem como objetivo se beneficiar da ignorância das pessoas e de seu comportamento on-line. O aumento do nível de atividade on-line, liderado por e-commerce e transações on-line, ampliou a postura de vulnerabilidade e expôs os usuários finais aos cibercriminosos que estão procurando quaisquer vestígios digitais deixados para eles. Isso faz com que usuários e sistemas de endpoint de TI com baixa postura de segurança e mecanismos de defesa fracos sejam presas fáceis para ataques cibernéticos.

As sérias implicações enfrentadas pelas empresas causadas por ameaças de phishing e ransomware levaram ao surgimento de serviços para combater essas ameaças avançadas. Esses serviços e soluções vão além do perímetro básico e das medidas convencionais de segurança e oferecem monitoramento profundo, inspeção e proteção contínuos, juntamente com uma abordagem estruturada de resposta a incidentes. Além da necessidade de autoproteção, leis e regulamentos como o Regulamento Geral de Proteção de Dados (GDPR) na Europa levaram as empresas a implementar medidas de proteção mais fortes para combater ataques cibernéticos. Existem legislações semelhantes em outros países, como Brasil e Austrália, para proteger os usuários de ameaças e ataques cibernéticos.

A segurança cibernética tornou-se uma importante área de prática para as empresas devido ao seu impacto nos negócios e em seus processos. No entanto, os executivos de TI geralmente lutam para justificar os investimentos em segurança para as partes interessadas de negócios, especialmente o CFO. Ao contrário de outros projetos de TI, nem sempre é possível medir e demonstrar o retorno sobre o investimento (ROI), nem quantificar os riscos relacionados a ameaças. Portanto, as medidas de segurança costumam ser de baixo nível e não são suficientes para lidar com ameaças sofisticadas. Por outro lado, a disponibilidade de

tecnologia adequada nem sempre resulta na eliminação de vulnerabilidades: muitos incidentes de segurança, como cavalos de Tróia e ataques de phishing, são causados devido à ignorância dos usuários finais. Aspectos relacionados à conscientização entre os usuários finais podem resultar em ataques direcionados, como ameaças persistentes avançadas e ransomware, que afetam a reputação da marca e também causam perdas financeiras e de dados, além de interrupções operacionais. Portanto, consultoria e treinamento de usuários continuam a desempenhar um papel fundamental, juntamente com uma infraestrutura de TIC atualizada. A crescente complexidade das ameaças também levou a um maior enfoque nos serviços de monitoramento, detecção e resposta para proteger as empresas além do seu perímetro, proteção baseada em assinatura e outros serviços de segurança.

O estudo ISG Provider Lens™ Cibersegurança – Soluções e serviços 2021 visa apoiar os tomadores de decisão de TIC para fazerem o melhor uso de seus orçamentos de segurança restritos, oferecendo o seguinte:

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

Para provedores e fornecedores de TI, este estudo serve como uma importante base de tomada de decisão para posicionamento, relacionamentos principais e considerações de entrada no mercado. Consultores e clientes corporativos ISG também aproveitam as informações dos relatórios ISG Provider Lens™ enquanto avaliam seus relacionamentos com fornecedores atuais e novos contratos potenciais.

Pesquisa de quadrantes

Como parte do estudo de quadrantes do ISG Provider Lens™, este relatório inclui seis quadrantes sobre segurança cibernética ilustrados abaixo.

Simplified illustration

Soluções e serviços de cibersegurança		
Security Solutions		
Gerenciamento de identidade e acesso (IAM)	Prevenção contra vazamento/ perda de dados (DLP) e segurança de dados	Proteção, detecção e resposta avançada a ameaças de endpoint (ETPDR avançado)
Serviços de segurança		
Serviços técnicos de segurança	Serviços de segurança estratégica	Serviços gerenciados de segurança

Source: ISG 2021

Gerenciamento de identidade e acesso (IAM)

Os fornecedores e provedores de soluções de IAM são caracterizados por sua capacidade de oferecer software proprietário e serviços associados para atender à demanda exclusiva de gerenciamento seguro de identidades e dispositivos de usuários corporativos. Este quadrante também inclui software como serviço baseado em software proprietário. Provedores de serviços puros que não oferecem um produto IAM (local e/ou na nuvem) com base em software desenvolvido por conta própria 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 no modelo como serviço ou uma combinação dos dois.

As soluções de IAM têm como objetivo coletar, registrar e administrar identidades de usuários e direitos de acesso relacionados, assim como o acesso especializado a ativos críticos, incluindo gerenciamento de acesso privilegiado (PAM). Elas garantem que os direitos de acesso sejam concedidos com base em políticas definidas. Para lidar com os requisitos de aplicativos novos e existentes, as soluções de IAM estão cada vez mais integradas 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 recursos adicionais relacionados à mídia social e aos usuários móveis para atender às suas necessidades de segurança, que vão além da web tradicional e do gerenciamento de direitos relacionados ao contexto.

Critérios de elegibilidade:

- Relevância (receita e número de clientes) como fornecedor de produtos IAM no respectivo país.
- As ofertas de IAM devem ser baseadas em software proprietário e não em software de terceiros.
- A solução deve ser capaz de ser implantada em ou por meio de uma combinação de modelo local, na nuvem, identidade como serviço (IDaaS) e gerenciado (de terceiros).
- A solução deve ser capaz de ser compatível com autenticação feita em ou por uma combinação de login único (SSO), autenticação multifator (MFA), modelos baseados em risco e baseados em contexto.
- A solução deve ser capaz de ser compatível com acesso baseado em função e gerenciamento de acesso privilegiado.
- 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 aplicativos (APIs) e aplicativos da web.
- A solução deve ser capaz de oferecer compatibilidade com um ou mais padrões IAM herdados e mais recentes, incluindo, sem limitação: SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust e SCIM.
- Para oferecer compatibilidade por meio de acesso seguro, o portfólio deve oferecer um ou mais dos seguintes: soluções de diretório, painel ou gerenciamento de autoatendimento e gerenciamento de ciclo de vida (migração, sincronização e replicação).

Prevenção contra vazamento/perda de dados (DLP) e segurança de dados

Os fornecedores e provedores de soluções de DLP são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui software como serviço baseado em software proprietário. Provedores de serviços puros que não oferecem um produto DLP (local ou baseado na nuvem) com base em software desenvolvido por conta própria não estão incluídos aqui. As soluções 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 aplicativos em nuvem, endpoint, rede e outros dispositivos.

Essas soluções devem ser capazes de descobrir dados confidenciais, aplicar políticas, monitorar o tráfego e melhorar a conformidade dos dados. Elas estão ganhando uma importância considerável à medida que ficou mais difícil para as empresas controlar as movimentações e transferências de dados. O número de dispositivos, inclusive móveis, que são usados para armazenar dados está aumentando nas empresas. Quase sempre, esses dispositivos estão equipados com conexão à Internet e podem enviar e receber dados sem passar por um gateway central de Internet. Os dispositivos contam com várias interfaces, como portas USB, Bluetooth, rede local sem fio (WLAN) e comunicação de campo próximo (NFC), que permitem o compartilhamento de dados. As soluções de segurança de dados protegem os dados contra acesso não autorizado, divulgação ou roubo.

Critérios de elegibilidade:

- Relevância (receita e número de clientes) como fornecedor de produtos DLP no respectivo país.
- A oferta de DLP deve ser baseada em software proprietário e não em software de terceiros.
- A solução deve ser capaz de ser compatível com DLP em qualquer arquitetura, como nuvem, rede, armazenamento ou endpoint.
- A solução deve ser capaz de lidar com a proteção de dados confidenciais em dados estruturados ou não estruturados, texto ou dados binários.
- A solução deve ser oferecida com compatibilidade com gerenciamento básico, incluindo sem limitação: relatórios, controles de política, instalação e manutenção e funcionalidades avançadas de detecção de ameaças.

Proteção, detecção e resposta avançada a ameaças de endpoint (ETPDR avançado)

Os fornecedores e provedores de soluções de ETPDR avançado são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui software como serviço baseado em software proprietário. Provedores de serviços puros que não oferecem um produto ETPDR avançado (local ou baseado na nuvem) com base em software desenvolvido por conta própria não estão incluídos aqui. Este quadrante avalia os provedores que oferecem produtos que podem fornecer monitoramento contínuo e visibilidade total de todos os pontos de extremidade, e podem analisar, prevenir e responder a ameaças avançadas.

Essas soluções vão além da simples proteção baseada em assinatura e oferecem proteção contra adversários, como ransomware, ameaças persistentes avançadas (APTs) e malware, investigando os incidentes em todo o cenário de ponto de extremidade. A solução deve ser capaz de isolar o ponto de extremidade infectado e tomar a ação corretiva/remediação necessária. Tais soluções compreendem um banco de dados, em que as informações coletadas da rede e pontos de extremidade são agregadas, analisadas e investigadas, e um agente que reside no sistema host e oferece os recursos de monitoramento e relatório para os eventos.

Critérios de elegibilidade:

- Relevância (receita e número de clientes) como fornecedor avançado de produtos ETPDR no respectivo país.
- A oferta de ETPDR avançada deve ser baseada em software proprietário e não em software de terceiros.
- As soluções dos provedores devem fornecer cobertura abrangente e total e visibilidade de todos os terminais na rede.
- A solução deve demonstrar eficácia no bloqueio de ameaças sofisticadas, como ameaças persistentes avançadas, ransomware e malware.
- A solução deve aproveitar a inteligência de ameaças, analisar e oferecer percepções em tempo real sobre as ameaças que emanam dos pontos de extremidade.

Serviços Gerenciados de Segurança (MSS)

Os MSS compreendem as operações e gerenciamento de infraestruturas de segurança de TI para um ou vários clientes por um centro de operações de segurança (SOC). Os serviços típicos incluem monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, aconselhamento sobre medidas de prevenção, teste de penetração, operações de firewall, operações de antivírus, serviços de operação de IAM, operações de DLP e todos os outros serviços operacionais para fornecer proteção contínua em tempo real sem comprometer desempenho dos negócios. 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 serviço podem lidar com todo o ciclo de vida do incidente de segurança, desde a identificação até a resolução.

Critérios de elegibilidade:

- Capacidade de fornecer serviços de segurança como detecção e prevenção; segurança da informação e gerenciamento de eventos (SIEM); e consultor de segurança e suporte de auditoria, remotamente ou no local do cliente.
- Relevância (receita e número de clientes) como fornecedor de MSS no respectivo país.
- Não focado exclusivamente em produtos proprietários, mas pode gerenciar e operar as melhores ferramentas de segurança da categoria.
- Possui credenciamentos de fornecedores de ferramentas de segurança.
- Os SOCs de propriedade e gerenciados idealmente pelo provedor e não predominantemente por parceiros.
- Manter uma equipe certificada, por exemplo, em Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Global Information Assurance Certification (GIAC), etc.

Serviços Técnicos de Segurança (TSS)

Este quadrante examina os provedores de serviços que não têm um foco exclusivo em seus respectivos produtos proprietários e podem implementar e integrar produtos ou soluções de outros fornecedores. Os TSS cobrem integração, manutenção e suporte para produtos ou soluções de segurança de TI. Os TSS abordam todos os produtos de segurança, incluindo antivírus, nuvem e segurança de data center, IAM, DLP, segurança de rede, segurança de ponto de extremidade, gerenciamento unificado de ameaças (UTM) e outros.

Critérios de elegibilidade:

- Demonstrar experiência na implementação de soluções de segurança para empresas no respectivo país.
- Não focado exclusivamente em produtos proprietários.
- Autorizado por fornecedores para distribuir e oferecer suporte a soluções de segurança.
- Especialistas certificados para apoiar suas tecnologias de segurança.
- Capacidade de participar (desejável, não obrigatório) em associações de segurança locais e agências de certificação.

Serviços Estratégicos de Segurança (SSS)

Os SSS cobrem principalmente consultoria para segurança de TI. Alguns dos 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, postura de risco e definir a estratégia de segurança cibernética para empresas. Este quadrante examina os provedores de serviços que não têm um foco exclusivo em produtos ou soluções proprietários. Os serviços aqui analisados abrangem todas as tecnologias de segurança.

Critérios de elegibilidade:

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

Quadrantes por região

Como parte do Estudo de Quadrante Provider Lens™ do ISG, estamos apresentando a pesquisa de cinco quadrantes (mercado) a seguir sobre Cibersegurança - Soluções e Serviços de 2021 por região:

Quadrants	EUA	Reino Unido	Países nórdicos	Alemanha	Suíça	França	Brasil	Austrália
Gerenciamento de Identidade e Acesso (IAM)	√	√	√	√	√	√	√	√
Prevenção contra vazamento/perda de dados (DLP) e segurança de dados	√	√	√	√	√	√	√	√
Proteção, detecção e resposta avançada a ameaças de endpoint (ETPDR avançado)	√	√	√	√	√	√	√	√
Serviços Gerenciados de Segurança (MSS)	√	√	√	√	√	√	√	√
Serviços Técnicos de Segurança (TSS)	√	√	√	√	√	√	√	√
Serviços Estratégicos de Segurança (SSS)	√	√	√	√	√	√	√	√

Cronograma

A fase de pesquisa ocorre no período de **março** a **abril de 2021**, período em que ocorrerá a pesquisa, a avaliação, a análise e a validação. Os resultados serão apresentados à mídia em **julho de 2021**.

Marcos	Início	Término
Lançamento	18 de fevereiro de 2021	
Fase de pesquisa	18 de fevereiro de 2021	15 de março de 2021
Prévia	3 de maio de 2021	
Comunicado à imprensa	21 de junho de 2021	

Consulte o link abaixo para visualizar/baixar a agenda de pesquisa de 2021 do Provider Lens™: Plano Anual

Isenção de responsabilidade da produção de pesquisa:

O ISG coleta dados com o propósito de escrever pesquisas e criar perfis de provedor/fornecedor. Os 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 o trabalho de terceirização identificado pelos clientes. Esses dados são coletados como parte do processo do ISG FutureSource e do processo de Qualificação do Candidato a Provedor (Candidate Provider Qualification - CPQ). O ISG pode escolher apenas utilizar esses dados coletados pertencentes a determinados países ou regiões para a educação e os propósitos de seus conselheiros e não para produzir relatórios do Provider Lens™ do ISG. 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 pelos analistas líderes.

Lista parcial de empresas convidadas para a pesquisa

Você está na lista ou vê sua empresa como um provedor relevante que está faltando na lista? Então sinta-se à vontade para entrar em contato conosco para garantir a 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

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
Autor principal na Austrália

Frank Heuer
Autor principal na Alemanha e na Suiça

Benoit Scheuber
Autor principal da França

Monica K
Analista de Visão Geral Global

Gowtham Kumar
Autor principal nos EUA

Srinivasan P N
Analista de Visão Geral Global

Paulo Brito
Autor principal no Brasil

Gerente de Projeto

Kartik Subramaniam
Autor principal no Reino Unido e países nórdicos

Dhananjay Vasudeo Koli
Gerente de Projeto Global

Você precisa de informações adicionais?

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