ISG Provider Lens™

2021

Cybersecurity – Solutions & Services 2021

imagine your future®

ISG (Information Services Group) (NASDAQ : III) est une société de recherche et de conseil technologique de premier plan au niveau mondial. Partenaire commercial de confiance de plus de 700 clients, dont 75 des 100 premières entreprises mondiales, ISG s'engage à aider les entreprises, les organisations du secteur public et privé, et les fournisseurs de services et de technologies à atteindre l'excellence opérationnelle et une croissance plus rapide. La société est spécialisée dans les services de transformation numérique, notamment l'automatisation, le cloud et l'analyse des données, le conseil en matière d'approvisionnement, les services de gestion de la gouvernance et des risques, les services d'opérateur réseau, la conception de stratégies et d'opérations, la gestion du changement, la veille commerciale et la recherche et l'analyse technologiques. Fondée en 2006 et basée à Stamford, dans le Connecticut, ISG emploie plus de 1 300 professionnels du numérique opérant dans plus de 20 pays - une équipe mondiale connue pour sa pensée novatrice, son influence sur le marché, sa profonde expertise industrielle et technologique, et ses capacités de recherche et d'analyse de classe mondiale basées sur les les données les plus complètes sur les marchés.

Table of Contents

Définition

Les entreprises adoptent rapidement de nouvelles technologies pour se lancer dans des parcours de transformation numérique afin de rester compétitives et s'aligner sur les besoins en constante évolution des utilisateurs finaux. L'adoption croissante de ces technologies, ainsi que de nouveaux outils permettant de gagner en efficacité et en rapidité, a conduit à une augmentation de l'exposition et à une menace grandissante de la surface d'attaque. Les ransomwares, les menaces avancées persistantes et les attaques par hameçonnage sont devenus les principales cybermenaces en 2020. Experian, SolarWinds, Zoom, Magellan Health, Finastra et Marriott étaient parmi les principales entités qui ont été confrontées à des cyberattaques de piratage, de code malveillant et de ransomware au cours de l'année dernière.

Les attaquants sont toujours à la recherche de moyens nouveaux et authentiques pour briser les mécanismes de défense. Cela a conduit à une augmentation du degré de leur sophistication, car ces attaquants accèdent à différents points de l'écosystème informatique d'une entreprise, tels que les réseaux de la chaîne d'approvisionnement, pour violer la sécurité. L'année 2020 a été témoin de plusieurs autres cyberattaques de grande envergure. Les attaques visaient la propriété intellectuelle, les informations personnelles identifiables (PII) et les dossiers confidentiels, ainsi que les informations clients d'entreprises des secteurs de la santé, de l'hôtellerie, de l'informatique, de la finance et d'autres, ainsi que des données appartenant à des États-nations. En plus de causer des dommages opérationnels, ces attaques ont eu un impact sur la valeur de la marque, les systèmes informatiques et la santé financière des organisations ciblées.

Le scénario de menace mondiale a été encore exacerbé en 2020 avec la pandémie COVID-19, qui a conduit un grand nombre de professionnels à travailler à distance, principalement à domicile. Ce nouveau modèle de travail a entraîné une utilisation accrue des outils, des plates-formes de collaboration ainsi que des réseaux publics en exposant les utilisateurs aux pirates informatiques via des vecteurs d'attaque tels que l'hameçonnage et d'autres menaces malveillantes. Avec l'évolution constante du monde des menaces informatiques, les entreprises doivent adopter une approche détaillée et globale de la cybersécurité afin de protéger leurs activités en mettant en œuvre une combinaison de produits et de services de sécurité dans des domaines tels que la gestion des identités et des accès (IAM), la sécurité des données et les services de sécurité gérés (MSS), de manière à obtenir un cadre de sécurité solide qui soit adapté à leurs besoins et à leur vision.

Alors que la nature et la complexité des menaces de cybersécurité continuent d'augmenter, les pirates informatiques recherchent et ciblent constamment les sources vulnérables et les infrastructures informatiques. Certaines menaces telles que l'hameçonnage, l'harponnage et les ransomwares visent à tirer parti de l'ignorance des gens et de leur comportement en ligne. L'augmentation du niveau d'activité en ligne, menée par le commerce électronique et les transactions en ligne, a élargi la position de vulnérabilité et exposé les utilisateurs finaux aux cybercriminels qui recherchent toute trace numérique laissée derrière eux. Les utilisateurs et les systèmes de points finaux informatiques ayant une faible posture de sécurité et des mécanismes de défense faibles sont donc des proies faciles pour les cyberattaques.

Les graves implications auxquelles sont confrontées les entreprises en raison des menaces liées à l'hameçonnage et aux logiciels de ransomware ont conduit au développement de services destinés à contrer ces menaces avancées. Ces services et solutions s'étendent au-delà du périmètre de base et des mesures de sécurité conventionnelles et offrent une surveillance, une inspection et une protection continues en profondeur, ainsi qu'une approche structurée de réponse aux incidents. Outre le besoin d'autoprotection, les lois et réglementations telles que le règlement général sur la protection des données (RGPD) en Europe ont conduit les entreprises à mettre en œuvre des mesures de sauvegarde plus strictes pour contrer les cyberattaques. Une législation similaire existe dans d'autres pays tels que le Brésil et l'Australie pour protéger les utilisateurs contre les cybermenaces et les attaques.

La cybersécurité est devenue un domaine de pratique important pour les entreprises en raison de son impact tant sur les sociétés que sur leurs processus. Cependant, les responsables informatiques ont souvent du mal à justifier les investissements de sécurité auprès des parties prenantes de l'entreprise, en particulier le directeur financier. Contrairement à d'autres projets informatiques, il n'est pas toujours possible de mesurer et de démontrer le retour sur investissement (ROI) ainsi que de quantifier les risques liés aux menaces. Par conséquent, les mesures de sécurité sont souvent à un faible niveau et ne sont pas suffisantes pour faire face aux menaces sophistiquées. D'un autre côté, la disponibilité d'une technologie appropriée n'entraîne pas toujours l'élimination des vulnérabilités ; de nombreux incidents de sécurité tels que les chevaux de Troie et les attaques d'hameçonnage sont dus à l'ignorance des utilisateurs finaux. Les aspects liés à la notoriété

parmi les utilisateurs finaux peuvent entraîner des attaques ciblées telles que des menaces persistantes avancées et des ransomwares, qui ont un impact sur la réputation de la marque et entraînent des pertes de données et financières, en plus des pannes opérationnelles. Par conséquent, les conseils et la formation des utilisateurs continuent de jouer un rôle clé, de même que l'infrastructure TIC moderne. La complexité croissante des menaces a également conduit à mettre davantage l'accent sur les services de surveillance, de détection et d'intervention pour protéger les entreprises au-delà du périmètre, de même que sur la protection basée en fonction des signatures et sur d'autres services de sécurité.

L'étude ISG Provider Lens™ Cybersecurity - Solutions & Services 2021 vise à aider les décideurs TIC à utiliser au mieux leurs budgets de sécurité serrés en proposant ce qui suit :

- Transparence sur les forces et les faiblesses des prestataires concernés.
- Un positionnement différencié des prestataires par segments de marché.
- Une perspective sur les marchés locaux.

Pour les vendeurs et les fournisseurs informatiques, cette étude constitue une base décisionnelle importante pour le positionnement, les relations clés et les considérations de mise sur le marché. Les conseillers ISG et les entreprises clientes exploitent également les informations des rapports ISG Provider Lens™ tout en évaluant leurs relations avec les fournisseurs actuels et les nouveaux engagements potentiels.

Recherche Quadrant

Dans le cadre de l'étude des quadrants ISG Provider Lens™, ce rapport comprend six quadrants sur la cybersécurité illustrés ci-dessous.

Illustration simplifiée

Solutions et services de cybersécurité		
Solutions de sécurité		
Gestion des identités et des accès (IAM)	Prévention des fuites/pertes de données (DLP) et sécurité des données	Protection, détection et réponse avancées des menaces pour les points finaux (ETPDR avancée)
Services de sécurité		
Services de sécurité technique	Services de sécurité stratégique	Services de sécurité gérés

Source : ISG 2021

Gestion des identités et des accès (IAM)

Les fournisseurs IAM et les fournisseurs de solutions se caractérisent par leur capacité à offrir des logiciels propriétaires et des services associés pour répondre à une demande unique de gestion sécurisée des identités et des appareils des utilisateurs d'entreprise. Ce quadrant comprend également le logiciel en tant que service basé sur un logiciel propriétaire. Les fournisseurs de services purs qui n'offrent pas de produit IAM (sur site et/ou cloud) basé sur des logiciels développés par eux-mêmes ne sont pas inclus ici. En fonction des exigences organisationnelles, ces solutions peuvent être déployées de plusieurs manières telles que sur site ou sur le cloud (géré par le client) ou en tant que modèle, service ou une combinaison de ceux-ci.

Les solutions IAM visent à collecter, enregistrer et administrer les identités des utilisateurs et les droits d'accès associés, ainsi que l'accès spécialisé aux actifs critiques, y compris la gestion des accès privilégiés (PAM). Ils garantissent que les droits d'accès sont accordés en fonction de politiques définies. Pour gérer les exigences des applications existantes et nouvelles, les solutions IAM sont de plus en plus intégrées avec des mécanismes, des cadres et une automatisation sécurisés (par exemple, des analyses de risques) dans leurs suites de gestion afin de fournir des fonctionnalités de profilage des utilisateurs et des attaques en temps réel. Les fournisseurs de solutions doivent également fournir des fonctionnalités supplémentaires liées aux réseaux sociaux et aux utilisateurs mobiles pour répondre à leurs besoins en termes de sécurité, qui vont au-delà de la gestion traditionnelle des droits liés au Web et au contexte.

Critères d'éligibilité :

- La pertinence (recettes et nombre de clients) en tant que fournisseur de produits IAM dans le pays concerné.
- Les offres IAM doivent être basées sur des logiciels propriétaires et non sur des logiciels tiers.
- La solution doit pouvoir être déployée dans l'un ou l'autre ou par une combinaison des modèles suivants : sur site, dans le cloud ou sous forme d'identité en tant que service (IDaaS) et géré (par un tiers).
- La solution doit être capable de prendre en charge l'authentification soit par une combinaison de modèles d'authentification unique (SSO), d'authentification multi-factorielle (MFA), basés sur les risques et sur le contexte.
- La solution doit être capable de prendre en charge l'accès basé sur les rôles et la gestion des accès privilégiés.
- Le fournisseur IAM doit être en mesure de fournir une gestion des accès pour un ou plusieurs besoins de l'entreprise tels que le cloud, les points finaux, les appareils mobiles, les interfaces de programmation d'applications (API) et les applications Web.
- La solution doit être capable de prendre en charge une ou plusieurs normes IAM héritées et plus récentes, y compris, mais sans s'y limiter, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust et SCIM.
- Pour prendre en charge un accès sécurisé, le portefeuille doit offrir un ou plusieurs des éléments suivants : des solutions d'annuaire, un tableau de bord ou une gestion en libre-service et une gestion du cycle de vie (migration, synchronisation et réplication).

Prévention des fuites/pertes de données (DLP) et sécurité des données

Les vendeurs et fournisseurs de solutions DLP se caractérisent par leur capacité à proposer des logiciels propriétaires et des services associés. Ce quadrant comprend également le logiciel en tant que service basé sur un logiciel propriétaire. Les simples prestataires de services qui ne proposent aucun produit DLP (sur site ou dans le cloud) basé sur un logiciel développé par eux-mêmes ne sont pas inclus ici. Les solutions DLP sont des offres qui peuvent identifier et surveiller les données sensibles, fournir un accès uniquement aux utilisateurs autorisés et empêcher les fuites de données. Les solutions des fournisseurs sur le marché se caractérisent par une combinaison de produits capables de fournir une visibilité et un contrôle sur les données sensibles résidant dans les applications cloud, les points finaux, le réseau et d'autres appareils.

Ces solutions doivent être capables de découvrir des données sensibles, d'appliquer des politiques, de surveiller le trafic et d'améliorer la conformité des données. Ils prennent une importance considérable car il est devenu plus difficile pour les entreprises de contrôler les mouvements et les transferts de données. Le nombre d'appareils, notamment mobiles, utilisés pour stocker des données augmente dans les entreprises. Ceux-ci sont pour la plupart équipés d'une connexion Internet et peuvent envoyer et recevoir des données sans les faire passer par une passerelle Internet centrale. Les appareils sont fournis avec une multitude d'interfaces, telles que des ports USB, Bluetooth, un réseau local sans fil (WLAN) et une technologie NFC (« Near Field Communication »), qui permettent le partage de données. Les solutions de sécurité des données protègent les données contre l'accès, la divulgation ou le vol non autorisés.

Critères d'éligilibité :

- La pertinence (recettes et nombre de clients) en tant que fournisseur de produits DLP dans le pays concerné.
- L'offre DLP doit être basée sur un logiciel propriétaire et non sur un logiciel tiers.
- La solution doit être capable de prendre en charge DLP sur n'importe quelle architecture telle que le cloud, le réseau, le stockage ou les point finaux.
- La solution doit être capable de gérer la protection des données sensibles sur des données structurées ou non structurées, du texte ou des données binaires.
- La solution doit être proposée avec un support de gestion de base, y compris, mais sans s'y limiter, les rapports, les contrôles de politique, l'installation et la maintenance, et des fonctionnalités avancées de détection des menaces.

Protection, détection et réponse avancées des menaces pour les points finaux (ETPDR avancée)

Les vendeurs et fournisseurs de solutions ETPDR avancés se caractérisent par leur capacité à offrir des logiciels propriétaires et des services associés. Ce quadrant comprend également le logiciel en tant que service basé sur un logiciel propriétaire. Les simples fournisseurs de services qui ne proposent aucun produit ETPDR avancé (sur site ou dans le cloud) basé sur un logiciel développé par eux-mêmes ne sont pas inclus ici. Ce quadrant évalue les fournisseurs offrant des produits capables de fournir une surveillance continue et une visibilité totale de tous les points finaux, ainsi qu'une analyse, une prévention et une réponse aux menaces avancées.

Les solutions vont au-delà de la simple protection basée sur les signatures et offrent une protection contre les adversaires tels que les rançongiciels, les menaces persistantes avancées (APT) et les logiciels malveillants en enquêtant sur les incidents sur l'ensemble des terminaux. La solution doit permettre d'isoler le point terminal infecté et de prendre les mesures correctives nécessaires. Ces solutions comprennent une base de données, dans laquelle les informations collectées à partir du réseau et des points finaux sont agrégées, analysées et étudiées, et un agent qui réside dans le système hôte et offre les capacités de surveillance et de rapport des événements.

Critères d'éligibilité :

- La pertinence (recettes et nombre de clients) en tant que fournisseur de produits ETPDR avancés dans le pays concerné.
- L'offre ETPDR avancée doit être basée sur un logiciel propriétaire et non sur un logiciel tiers.
- Il convient donc aux fournisseurs de veiller à ce que les solutions assurent une couverture et une visibilité complètes et totales de tous les points terminaux du réseau.
- La solution proposée doit faire preuve d'efficacité pour bloquer les menaces sophistiquées telles que les menaces persistantes avancées, les logiciels contre rançon et les logiciels malveillants.
- La solution doit tirer parti des renseignements sur les menaces, les analyser et offrir un aperçu en temps réel des menaces émanant des différents points d'accès.

Services de sécurité gérés (MSS)

Les MSS consistent en l'exploitation et la gestion des infrastructures de sécurité informatique pour un ou plusieurs clients par un centre d'opérations de sécurité (SOC). Les services typiques comprennent la surveillance de la sécurité, l'analyse du comportement, la détection des accès non autorisés, les conseils sur les mesures de prévention, les tests de pénétration, les opérations de pare-feu, les opérations anti-virus, les services d'exploitation IAM, les opérations DLP et tous les autres services d'exploitation visant à fournir une protection continue en temps réel sans compromettre les performances de l'entreprise. Ce quadrant examine les fournisseurs de services qui ne sont pas exclusivement axés sur les produits propriétaires mais qui peuvent gérer et exploiter les meilleurs outils de sécurité. Ces fournisseurs de services sont capables de gérer l'ensemble du cycle de vie des incidents de sécurité, depuis leur identification jusqu'à leur résolution.

Critères d'éligibilité :

- Capacité à fournir des services de sécurité tels que la détection et la prévention, la gestion des informations et des événements de sécurité (SIEM), le conseil en sécurité et le soutien aux audits, à distance ou sur le site du client.
- La pertinence (recettes et nombre de clients) en tant que fournisseur de MSS dans le pays concerné.
- Pas exclusivement axés sur les produits propriétaires mais capables de gérer et exploiter les outils de sécurité ultra-performants.
- Posséder des accréditations de fournisseurs d'outils de sécurité.
- Les SOC sont idéalement détenus et gérés par le fournisseur et non pas principalement par des partenaires.
- Maintenir un personnel certifié, par exemple, en tant que professionnel Certified Information Systems Security Professional (CISSP), responsable Certified Information Security Manager (CISM), Global Information Assurance Certification (GIAC), etc.

Services de sécurité technique (TSS)

Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur leurs produits propriétaires respectifs et qui peuvent mettre en œuvre et intégrer les produits ou solutions d'autres fournisseurs. Les TSS englobent l'intégration, la maintenance et le soutien des produits ou solutions de sécurité informatique. Les TSS couvrent tous les produits de sécurité, y compris les anti-virus, la sécurité des nuages et des centres de données, l'IAM, le DLP, la sécurité des réseaux, la sécurité des points d'extrémité, la gestion unifiée des menaces (UTM) et autres.

Critères d'éligibilité :

- Faire preuve d'expérience dans la mise en œuvre de solutions de sécurité pour les entreprises dans le pays concerné.
- Pas exclusivement axés sur les produits propriétaires.
- Autorisé par les fournisseurs à distribuer et à soutenir les solutions de sécurité.
- Avoir recours à des experts certifiés afin de soutenir ses technologies de sécurité.
- Capacité à participer (souhaitable, non obligatoire) aux associations locales de sécurité et aux organismes de certification.

Services de sécurité stratégique (SSS)

Le SSS couvre principalement le conseil en matière de sécurité informatique. Quelques-uns des services proposés dans ce quadrant sont notamment les audits de sécurité, les services de conseil en matière de conformité et de risques, les évaluations de sécurité, le conseil en architecture de solutions de sécurité, ainsi que la sensibilisation et la formation. Ces services sont utilisés pour évaluer la maturité de la sécurité, la posture de risque, et définir la stratégie de cybersécurité des entreprises. Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur leurs produits ou solutions propriétaires. Les services analysés ici couvrent toutes les technologies de sécurité.

Critères d'éligibilité :

- Les fournisseurs de services doivent faire preuve de compétences dans les domaines du SSS tels que l'évaluation, l'appréciation, la sélection des fournisseurs, le conseil en architecture et le conseil en matière de risques.
- Les prestataires de services doivent offrir au moins un des SSS susmentionnés dans le pays concerné.
- L'exécution de services de conseil en matière de sécurité à l'aide de cadres constituera un atout.
- Pas exclusivement axés sur les produits ou solutions propriétaires.

Quadrant par région

Dans le cadre de l'étude des quadrants ISG Provider Lens™, nous introduisons les cinq quadrants (marché) suivants de l'étude sur la cybersécurité, Solutions et Services 2021 par région:

Quadrants	États-Unis	Royaume - Uni	Pays nordiques	Allemagne	Suisse	France	Brésil	Australie
Gestion des identités et des accès (IAM)	√	√	√	√	√	√	√	√
Prévention des fuites/ pertes de données (DLP) et sécurité des données	√	√	√	√	√	√	√	√
Protection, détection et réponse avancées des menaces pour les points finaux (ETPDR avancée)	√	√	√	√	√	√	√	√
Services de sécurité gérés (MSS)	√	√	√	√	√	√	√	√
Services de sécurité technique (TSS)	√	√	√	√	√	√	√	√
Services de sécurité stratégique (SSS)	√	√	√	√	√	√	√	√

Calendrier

La phase de recherche se situe entre **mars** et **avril 2021**, au cours de laquelle l'enquête, l'évaluation, l'analyse et la validation auront lieu. Les résultats seront présentés aux médias en **juillet 2021**.

Étapes	Début	Fin
Lancement	18 février 2021	
Phase d'étude	18 février 2021	15 mars 2021
Aperçu préliminaire	3 mai 2021	
Communiqué de presse	21 june 2021	

Veuillez vous référer au lien ci-dessous pour visualiser/télécharger le programme de recherche du fournisseur Lens™ 2021. Plan annuel

Avis de non-responsabilité concernant les résultats de la recherche :

L'ISG collecte des données dans le but de rédiger des recherches et de créer des profils de fournisseurs/prestataires. Les profils et les données justificatives sont utilisés par les conseillers du GSI pour faire des recommandations et informer leurs clients de l'expérience et des qualifications de tout fournisseur/prestataire applicable pour les travaux d'externalisation identifiés par les clients. Ces données sont collectées dans le cadre du processus FutureSource de l'ISG et du processus de qualification des candidats fournisseurs (CPQ). ISG peut choisir de n'utiliser ces données collectées concernant certains pays ou régions que pour l'éducation et les besoins de ses conseillers et de ne pas produire les rapports du fournisseur d'ISG Lens™. Ces décisions seront prises en fonction du niveau et de l'exhaustivité des informations reçues directement des fournisseurs/prestataires et de la disponibilité d'analystes expérimentés pour ces pays ou régions. Les informations soumises peuvent également être utilisées pour des projets de recherche individuels ou pour des notes d'information qui seront rédigées par les analystes principaux.

Liste partielle des entreprises invitées à participer à cette étude

Faites-vous partie de la liste ou considérez-vous votre entreprise comme un fournisseur pertinent qui ne figure pas dans la liste? Alors n'hésitez pas à nous contacter pour assurer votre participation active à la phase de recherche.

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 pour l'étude

Craig Baty
Auteur principal Australie

Frank Heuer
Auteur principal, Allemagne et Suisse

Benoit Scheuber
Auteur principal France

Monica K
Analyste d'aperçu global

Gowtham Kumar
Auteur principal États-Unis

Srinivasan P N
Analyste d'aperçu global

Paulo Brito
Auteur principal Brésil

Chef de projet

Kartik Subramaniam
Auteur principal Royaume-Uni et Pays nordiques

Dhananjay Vasudeo Koli
Chef de projet global

Avez-vous besoin d'informations supplémentaires ?

En cas de questions, veuillez nous contacter à l'adresse isglens@isg-one.com.