ISG Provider Lens™

2021

Cybersecurity – Solutions & Services 2021

imagine your future®

ISG (Information Services Group) (NASDAQ: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 700 Kunden, darunter die 75 der 100 weltweit größten Unternehmen, unterstützt ISG Unternehmen, öffentliche Organisationen sowie Service- und Technologie-Anbieter dabei, Operational Excellence und schnelleres Wachstum zu erzielen. Der Fokus des Unternehmens liegt auf Services im Kontext der digitalen Transformation, inklusive Automatisierung, Cloud und Daten-Analytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzwerkbetrieb, Design von Technologie-Strategie und -Betrieb, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.300 Experten und ist in mehr als 20 Ländern tätig. Das globale Team von ISG ist bekannt für sein innovatives Denken, seine geschätzte Stimme im Markt, tiefgehende Branchen- und Technologie-Expertise sowie weltweit führende Marktforschungs- und Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren. Weitere Informationen unter www.isg-one.com.

Table of Contents

Definition

Unternehmen setzen zügig neue Technologien ein, um die digitale Transformation voranzutreiben, wettbewerbsfähig zu bleiben und den sich ständig ändernden Anforderungen der Endbenutzer gerecht werden zu können. Die zunehmende Verbreitung dieser Technologien sowie neue Tools, die für mehr Effizienz und Geschwindigkeit sorgen, haben zu einer erhöhten Gefährdung und einer wachsenden Angriffsfläche geführt. Ransomware, Advanced Persistent Threats und Phishing-Angriffe stellten sich 2020 als die schlimmsten Cyber-Bedrohungen heraus. Führende Unternehmen, darunter Experian, SolarWinds, Zoom, Magellan Health, Finastra und Marriott, sahen sich im letzten Jahr Cyberangriffen durch Hacking, bösartigen Code und Ransomware ausgesetzt.

Angreifer sind ständig dabei, neue, ausgeklügelte Möglichkeiten zu finden, um die Abwehrmechanismen zu durchbrechen, und so werden die Angriffe immer raffinierter, denn diese Angreifer verschaffen sich Zugang zu verschiedenen Punkten im IT-Ökosystem eines Unternehmens, z.B. Netzwerken in der Lieferkette, um so die Sicherheit zu durchbrechen. Im Jahr 2020 wurden etliche Cyberangriffe auf namhafte Unternehmen bekannt. Diese Attacken zielten auf geistiges Eigentum (IP), personenbezogene und vertrauliche Daten sowie Kundendaten von Unternehmen aus dem Gesundheitswesen, dem Gastgewerbe, der IT-Branche, dem Finanzsektor und anderen Branchen sowie auf Daten von Nationalstaaten. Dadurch wurde nicht nur der Betrieb gestört, sondern auch der Markenwert in Mitleidenschaft gezogen und die IT-Systeme und die finanzielle Gesundheit der angegriffenen Unternehmen beeinträchtigt.

Das globale Bedrohungsszenario wurde im Jahr 2020 durch die Corona-Krise weiter verschärft, denn im Zuge der Pandemie arbeiteten viele Menschen remote bzw. hauptsächlich von zu Hause aus. Dieses neue Arbeitsmodell führte zu einer verstärkten Nutzung von Collaboration-Tools und -Plattformen sowie öffentlichen Netzwerken; die User waren Angriffsvektoren wie Phishing und anderen bösartigen Bedrohungen von Hackern ausgesetzt. Angesichts dieser sich ständig verändernden Bedrohungslandschaft müssen Unternehmen einen detaillierten und umfassenden Ansatz für die Cybersicherheit verfolgen, um ihr Unternehmen zu schützen, und zwar mit einer Kombination aus Sicherheitsprodukten und -services aus Bereichen wie Identitäts- und Zugriffsmanagement (IAM), Datensicherheit und Managed Security Services (MSS), um so ein an ihre Bedürfnisse und Vorstellungen angepasstes robustes Security Framework aufzubauen.

Da die Art und Komplexität von Cybersecurity-Bedrohungen weiter zunimmt, sind Hacker ständig auf der Suche nach ungeschützten Quellen und IT-Infrastrukturen und nehmen diese ins Visier. Manche Bedrohungen wie Phishing, Spear Phishing und Ransomware machen sich die Unwissenheit und das Online-Verhalten der Menschen zunutze. Das erhöhte Maß an Online-Aktivitäten, insbesondere E-Commerce und Online-Transaktionen, hat für noch mehr Schwachstellen gesorgt und die Endanwender Cyberkriminellen ausgesetzt, die auf der Suche nach allen von ihnen hinterlassenen digitalen Spuren sind. Dies macht Anwender und IT-Endpunktsysteme mit schlechter Sicherheit und schwachen Abwehrmechanismen zur leichten Beute für Cyberangriffe.

Angesichts der schwerwiegenden Auswirkungen von Phishing- und Ransomware-Bedrohungen im Unternehmensumfeld wurden Services entwickelt, die solchen hochentwickelten Bedrohungen entgegenwirken. Diese Services und Lösungen gehen über die grundlegenden Perimeter- und konventionellen Sicherheitsmaßnahmen hinaus und bieten eine kontinuierliche Tiefenüberwachung, Inspektion und Schutz sowie einen strukturierten Ansatz zur Reaktion auf entsprechende Vorfälle. Neben der Notwendigkeit des Selbstschutzes haben Gesetze und Verordnungen wie die Datenschutz-Grundverordnung (DSGVO) in Europa Unternehmen dazu veranlasst, stärkere Schutzmaßnahmen zu implementieren, um Cyberangriffe abwehren zu können. Auch in anderen Ländern wie Brasilien und Australien gibt es ähnliche Gesetze, die Anwender vor Cyberbedrohungen und Angriffen schützen sollen.

Cybersicherheit wirkt sich stark auf Unternehmen und ihre Prozesse aus und hat sich zu einem wichtigen Bereich entwickelt. Allerdings ist es für IT-Verantwortliche oft schwierig, Security-Investitionen gegenüber der Geschäftsleitung – speziell gegenüber dem Finanzleiter, dem sie immer öfter unterstellt sind – zu verargumentieren. Im Gegensatz zu anderen IT-Projekten ist es nicht immer möglich, den Return on Investment (ROI) zu messen und nachzuweisen sowie bedrohungsbedingte Risiken zu quantifizieren. Daher sind die Sicherheitsmaßnahmen oft schwach und reichen nicht aus, um komplexe Bedrohungen zu bekämpfen. Andererseits führt die Verfügbarkeit geeigneter Technologie nicht immer zur Beseitigung von Schwachstellen; viele Sicherheitsvorfälle wie Trojaner- und Phishing-Angriffe werden durch die Unwissenheit der Endbenutzer verursacht. Ein zu geringes Sicherheitsbewusstsein der Endanwender kann

zu gezielten Angriffen wie Advanced Persistent Threats und Ransomware führen, die den guten Ruf der Marke beeinträchtigen und neben Betriebsausfällen auch Daten- und finanzielle Verluste verursachen. Zusätzlich zu einem zeitgemäßen ICT-Equipment spielen daher auch Beratung und Schulung für die Anwender (-Unternehmen) nach wie vor eine zentrale Rolle. Angesichts der zunehmenden Komplexität der Bedrohungen sind auch Überwachungs-, Erkennungs- und Reaktionsdienste verstärkt in den Fokus gerückt; sie sollen Unternehmen zusätzlich zu Perimeter-Schutz, signaturbasierten und weiteren Security Services Schutz bieten.

Die ISG Provider Lens™ Studie „Cybersecurity – Solutions & Services 2021" zielt darauf ab, ICT-Entscheider dabei zu unterstützen, ihr knappes Sicherheitsbudget anhand folgender Informationen optimal zu nutzen:

- transparente Darstellung der Stärken und Schwächen relevanter Anbieter
- differenzierte Positionierung der Anbieter nach Marktsegmenten
- Betrachtung verschiedener Märkte

Diese Studie bietet IT-Dienstleistern und Vendoren somit eine wesentliche Entscheidungsgrundlage für Positionierungs-, Beziehungs- und Go-to-Market-Überlegungen. ISG-Berater und Unternehmenskunden nutzen Informationen aus den ISG Provider Lens™ Reports auch zur Evaluierung ihrer derzeitigen sowie potenzieller neuer Anbieterbeziehungen.

Quadrantenbasierte Marktforschung

Diese ISG Provider Lens™-Quadrantenstudie umfasst sechs Quadranten zum Thema Cybersecurity, die in folgender Abbildung veranschaulicht werden.

Vereinfachte Darstellung

Quelle: ISG 2021

Identity & Access Management (IAM)

IAM-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die geforderte spezifische und sichere Verwaltung von Benutzeridentitäten und -geräten in Unternehmen. Dieser Quadrant umfasst auch Software-as-a-Service Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine IAM-Produkte (on-premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. Entsprechend der individuellen Unternehmensanforderungen können diese Lösungen auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in der Cloud (vom Kunden verwaltet), auf Basis eines as-a-Service-Modells oder in Form einer kombinierten Lösung.

IAM-Lösungen dienen der Erfassung, Aufzeichnung und Verwaltung von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets, einschließlich Privileged Access Management (PAM). Sie stellen sicher, dass die Zugriffsrechte entsprechend definierter Richtlinien gewährt werden. Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungen im Rahmen von Management Suites zunehmend in sichere Mechanismen, Frameworks und Automatisierung (z.B. der Risikobewertung) eingebunden, um Nutzer- und Attacken-Profiling in Echtzeit durchführen zu können. Von den Lösungsanbietern werden zudem weitere Features im Zusammenhang mit Social Media und mobilen Anwendern erwartet, um deren Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen.

Auswahlkriterien:

- Relevanz (Umsatz und Anzahl der Kunden) als IAM-Produktanbieter im jeweiligen Land
- IAM-Angebote sollten auf proprietärer Software und nicht auf Software von Drittanbietern beruhen.
- Die Lösung sollte entweder vor Ort, in der Cloud, als Identity as a Service (IDaaS), in einem verwalteten Modell (eines Drittanbieters) oder in einer Kombination davon eingesetzt werden können.
- Die Lösung sollte die Authentifizierung anhand von Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA), risiko- und kontextbasierten Modellen oder einer Kombination aus diesen Ansätzen unterstützen.
- Die Lösung sollte rollenbasierten Zugriff und Privileged Access Management (PAM) unterstützen.
- Der IAM-Anbieter sollte Zugriffsmanagement für eine oder mehrere Unternehmensanforderungen wie Cloud, Endpunkte, mobile Geräte, Anwendungsprogrammierschnittstellen (APIs) und Webanwendungen anbieten.
- Die Lösung sollte einen oder mehrere ältere und neuere IAM-Standards unterstützen, einschließlich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM.
- Zur Unterstützung durch einen sicheren Zugriff sollte das Portfolio eine oder mehrere der folgenden Möglichkeiten bieten: Directory-Lösungen, Dashboard- oder Self-Service-Management und Lifecycle Management (Migration, Synchronisierung und Replizierung).

Data Leakage/Loss Prevention (DLP) & Data Security

DLP-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine DLP-Produkte (on-premise oder cloudbasiert) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. DLP-Lösungen sind Angebote, die sensible Daten identifizieren und überwachen können, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste verhindern. Die Lösungen der Anbieter in diesem Markt bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf anderen Geräten.

Diese Lösungen sollten in der Lage sein, sensible Daten zu erkennen, Richtlinien durchzusetzen, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern. Sie gewinnen erheblich an Bedeutung, da es für Unternehmen schwieriger geworden ist, Datenbewegungen und -übertragungen zu kontrollieren. Die Zahl der Geräte, auch der mobilen, die zur Datenspeicherung genutzt werden, nimmt in Unternehmen zu. Sie sind meistens mit einer Internetverbindung ausgestattet und können Daten senden und empfangen, ohne diese über ein zentrales Internet-Gateway zu leiten. Die Geräte sind mit einer Vielzahl von Schnittstellen für den Datenaustausch ausgestattet, z.B. USB-Ports, Bluetooth, Wireless Local Area Network (WLAN) und Near-Field Communication (NFC). Datensicherheitslösungen schützen Daten vor unberechtigtem Zugriff, Offenlegung oder Diebstahl.

Auswahlkriterien:

- Relevanz (Umsatz und Anzahl der Kunden) als DLP-Produktanbieter im jeweiligen Land
- DLP-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
- Die Lösung sollte DLP über eine beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt unterstützen.
- Die Lösung sollte sensible Daten schützen, egal ob es sich dabei um strukturierte oder unstrukturierte Daten, Text- oder Binärdaten handelt.
- Die Lösung sollte mit grundlegendem Management-Support angeboten werden, einschließlich, aber nicht nur Reporting, Richtlinienkontrolle, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen.

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

Anbieter von fortgeschrittenen ETPDR-Produkten und -Lösungen offerieren eigenentwickelte, proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service-Angebote auf Basis von proprietärer Software. Reine Dienstleister die kein auf eigenentwickelter Software basierendes fortschrittliches ETPDR-Produkt (vor Ort oder in der Cloud) anbieten, werden hier nicht analysiert. Im Rahmen dieses Quadranten werden Anbiete bewertet, die Produkte für die kontinuierliche Überwachung und vollständige Transparenz aller Endpunkte bieten und hochentwickelte Bedrohungen analysieren, verhindern und darauf reagieren können.

Diese Lösungen gehen über einen reinen signaturbasierten Schutz hinaus und bieten Schutz vor Angriffen wie Ransomware, Advanced Persistent Threats (APTs) und Malware; zu diesem Zweck werden Vorfälle über alle Endpunkte hinweg untersucht. Die Lösung sollte in der Lage sein, den infizierten Endpunkt zu isolieren und die notwendigen Korrekturmaßnahmen/Reparaturen durchzuführen. Solche Lösungen bestehen aus einer Datenbank, in der die vom Netzwerk und den Endpunkten gesammelten Informationen aggregiert, analysiert und untersucht werden, und einem Agenten, der im Host-System residiert und die Überwachungs- und Reporting-Funktionen für die Vorfälle bereitstellt.

Auswahlkriterien:

- Relevanz (Umsatz und Anzahl der Kunden) als ETPDR-Produktanbieter im jeweiligen Land
- Fortschrittliches ETPDR-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
- Umfassende und vollständige Abdeckung und Visibilität aller Endpunkte im Netzwerk
- Nachweisliche effektive Abwehr von komplexen Bedrohungen wie Advanced Persistent Threats, Ransomware und Malware
- Nutzung und Analyse von Bedrohungsdaten sowie Echtzeit-Einblicke in Bedrohungen, die von den Endpunkten ausgehen

Managed Security Services (MSS)

Unter MSS fallen Betrieb und Management von IT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). Zu den typischen Dienstleistungen gehören Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests, Firewall-Betrieb, Anti-Virus-Betrieb, IAM-Betriebsservice, DLP-Betrieb und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Dieser Quadrant untersucht Dienstleister, die sich nicht ausschließlich auf proprietäre Produkte konzentrieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Lösung von Problemen.

Auswahlkriterien:

- Angebot von Sicherheitsdiensten wie Erkennung und Vorbeugung, Security Information & Event Management (SIEM) sowie Sicherheitsberatern und Audits, per Fernzugriff oder vor Ort beim Kunden
- Relevanz (Umsatz und Anzahl der Kunden) als MSS-Anbieter im jeweiligen Land
- Kein ausschließlicher Fokus auf proprietäre Produkte, sondern Management- und Betriebsleistungen für Best-of-Breed Security-Tools
- Vorhandene Akkreditierungen von Anbietern von Sicherheitstools
- SOCs sind idealerweise im Besitz und unter der Leitung des Anbieters und nicht überwiegend von Partnern.
- Zertifizierte Mitarbeiter, z.B. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Global Information Assurance Certification (GIAC) usw.

Technical Security Services (TSS)

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf ihre jeweiligen proprietären Produkte konzentrieren und Produkte oder Lösungen anderer Anbieter implementieren und integrieren können. TSS umfassen Integration, Wartung und Support von IT-Sicherheitsprodukten oder -lösungen. Sie adressieren alle Sicherheitsprodukte, einschließlich Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, Unified Threat Management (UTM) und andere.

Auswahlkriterien:

- Nachweisliche Erfahrung in der Implementierung von Sicherheitslösungen für Unternehmen im jeweiligen Land
- Kein ausschließlicher Fokus auf firmeneigene Produkte
- Autorisierung von Anbietern, deren Sicherheitslösungen zu vertreiben und zu unterstützen
- Zertifizierte Experten zur Unterstützung der jeweiligen Sicherheitstechnologien
- Potenzielle Mitgliedschaft (wünschenswert, aber nicht zwingend) in lokalen Sicherheitsverbänden und Zertifizierungsstellen

Strategic Security Services (SSS)

SSS umfassen in erster Linie die Beratung für IT-Sicherheit. Einige der in diesem Quadranten abgedeckten Services umfassen Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zur Architektur von Sicherheitslösungen sowie Aufklärung und Schulungen. Diese Services dienen der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition der Cybersicherheits-Strategie für Unternehmen. In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf eigene Produkte oder Lösungen konzentrieren. Die hier analysierten Services decken alle Sicherheitstechnologien ab.

Auswahlkriterien:

- Nachweis von Leistungen in SSS-Bereichen wie Evaluierung, Assessments, Anbieterauswahl, Architekturberatung und Risikoberatung
- Angebot von mindestens einem der oben genannten SSS im jeweiligen Land
- Die Durchführung von Sicherheitsberatungen unter Verwendung von Frameworks ist von Vorteil.
- Kein ausschließlicher Fokus auf proprietäre Produkte oder Lösungen

Quadranten nach Regionen

Im Rahmen der ISG Provider Lens™ Quadrantenstudie „Cybersecurity - Solutions & Services 2021“ werden die folgenden Regionen im Rahmen von fünf Quadranten analysiert:

Quadranten	USA	UK	Nordische Länder	Deutsch-land	Schweiz	Frankreich	Brasilien	Australien
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)	√	√	√	√	√	√	√	√

Zeitplan

Die Research-Phase umfasst die Befragung, Evaluierung, Analyse und Validierung und läuft von **März bis April 2021**. Die Ergebnisse werden den Medien im **Juli 2021** präsentiert.

Meilensteine	**Beginn**	**Ende**
Start	18. Februar 2021	
Umfrage-Phase	18. Februar 2021	15. März 2021
Sneak Preview	3. Mai 2021	
Pressemitteilung	21. Juni 2021	

Mit Klick auf den nachfolgenden Link können Sie die ISG Provider Lens™ 2021 Research-Agenda einsehen bzw. herunterladen: Jahresplan

Haftungsausschluss für die Produktion von Research-Unterlagen:

ISG erhebt Daten zum Zwecke der Recherche und Erstellung von Anbieterprofilen. Die Profile und die unterstützenden Daten werden von den ISG-Advisorn verwendet, um Empfehlungen auszusprechen und ihre Kunden über die Erfahrungen und Qualifikationen der von den Kunden identifizierten geeigneten Anbieter für Outsourcing-Leistungen zu informieren. Diese Daten werden im Rahmen des ISG FutureSource Prozesses und des Candidate Provider Qualification (CPQ) Prozesses erhoben. ISG behält sich vor, die erhobenen Daten in Bezug auf bestimmte Länder oder Regionen nur für die Weiterbildung der Advisors und deren Arbeit und nicht zur Erstellung von ISG Provider Lens™ Berichte, zu verwenden. Diese Entscheidungen werden auf der Grundlage der Qualität und der Vollständigkeit der direkt von den Anbietern erhaltenen Daten und der Verfügbarkeit von erfahrenen Analysten für die jeweiligen Länder oder Regionen getroffen. Die eingereichten Informationen können auch für einzelne Research-Projekte oder für Briefing Notes verwendet werden, die von den leitenden Analysten verfasst werden.

Teilliste der zu dieser Umfrage eingeladenen Unternehmen

Steht Ihr Unternehmen auf der Liste bzw. sind Sie der Meinung, dass Ihr Unternehmen als relevanter Anbieter hier nicht vertreten ist? Dann bitten wir Sie um Kontaktaufnahme, um Ihre aktive Teilnahme in der Research-Phase zu gewährleisten.

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

Kontaktpersonen für diese Studie

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

Benötigen Sie weitere Informationen?

Bei Fragen wenden Sie sich bitte per E-Mail an isglens@isg-one.com.