ISG Provider Lens™

2022

Cybersecurity – Solutions and Services 2022

imagine your future®

ISG (Information Services Group) (Nasdaq: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 800 Kunden, darunter über 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, Strategie- und -Betriebs-Design, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.300 mit der Digitalisierung vertraute 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

Einleitung

Unternehmen setzen neue Technologien ein, um die digitale Transformation voranzutreiben, wettbewerbsfähig zu bleiben und den sich ständig ändernden Anforderungen der Endbenutzer gerecht werden zu können. Diese Entwicklung wurde durch die COVID-19-Pandemie noch beschleunigt, denn dadurch wurde verstärkt auf Telearbeit, Cloud-Anwendungen und andere digitale Technologien gesetzt, um wirtschaftlich überleben und wachsen zu können. Die zunehmende Verbreitung dieser Technologien sowie neue Tools, die für mehr Effizienz und Geschwindigkeit sorgen, haben zu einer immer größeren Angriffsfläche geführt. Ransomware, Advanced Persistent Threats und Phishing-Angriffe stellten sich 2022 als die schlimmsten Cyber-Bedrohungen heraus. Angesichts der immer vielfältigeren und komplexen Cyberangriffe ist die Cybersicherheit nicht nur für Unternehmen, sondern auch für Regierungsbehörden zu einer Priorität geworden, um den Schutz der Wirtschaft, Industrie und Bürger zu gewährleisten.

Im Zuge dieser sich ständig verändernden Bedrohungslandschaft muss ein detaillierter und umfassender Ansatz für die Cybersicherheit zum Schutz des Unternehmens verfolgt werden, und zwar mit einer Kombination aus Sicherheitsprodukten und -services aus Bereichen wie Identity & Access Management (IAM), Data Leakage/Loss Prevention (DLP) sowie Datensicherheit und Managed Security Services (MSS), um so ein robustes, sicheres Framework aufzubauen und potenzielle Risiken zu mindern.

Neben dem erforderlichen Selbstschutz haben Verordnungen wie die Datenschutz-Grundverordnung (DSGVO) in Europa und weitere regionale Compliance-Vorgaben Unternehmen dazu gezwungen, robuste Schutzmaßnahmen zu implementieren, um Cyberangriffe abwehren zu können. Auch in anderen Ländern wie Brasilien und Australien gibt es ähnliche Gesetze, die Anwender vor Cyberbedrohungen schützen sollen.

Cybersicherheit ist für CISOs in Unternehmen zu einem wichtigen Tätigkeitsbereich geworden; dennoch haben IT-Führungskräfte oft Schwierigkeiten, Sicherheitsinvestitionen zu verargumentieren, da es nicht immer möglich ist, den ROI zu messen und aufzuzeigen sowie die mit Bedrohungen verbundenen Risiken zu quantifizieren. Die Ausgereiftheit der verfügbaren Technologien, die Schwierigkeiten bei der Erkennung und Behebung von Schwachstellen und die mangelnde Sensibilisierung der Endbenutzer bereiten Unternehmen und ihren Führungskräfte weiterhin Kopfzerbrechen.

Andererseits bedeutet der Einsatz angemessener Sicherheitstools nicht, dass ein Unternehmen gegen Schwachstellen immun ist; der Faktor Mensch ist und bleibt das schwächste Glied in der Sicherheits-Kette, das von Angreifern durch Cyberbedrohungen wie Trojaner- und Phishing-Angriffe entsprechend ausgenutzt wird. Ein zu geringes Sicherheitsbewusstsein der Endanwender kann zu gezielten Angriffen wie Advanced Persistent Threats (APTs) und Ransomware führen, die den guten Ruf des Unternehmens beeinträchtigen, Daten- und finanzielle Verluste verursachen und zu Betriebsausfällen führen. Daher werden Benutzerschulungen, Risikobewertungen und Beratungsdienste weiterhin eine Schlüsselrolle bei der Gewährleistung der Sicherheit der unternehmensweiten Informations- und Kommunikationstechnologie (IKT)-Infrastruktur spielen.

Die ISG Provider Lens™ Studie „Cybersecurity – Solutions and Services 2022“ soll ICT-Entscheidern mit folgenden Informationen dabei zu unterstützen, ihre knappen Sicherheitsbudgets optimal zu nutzen:

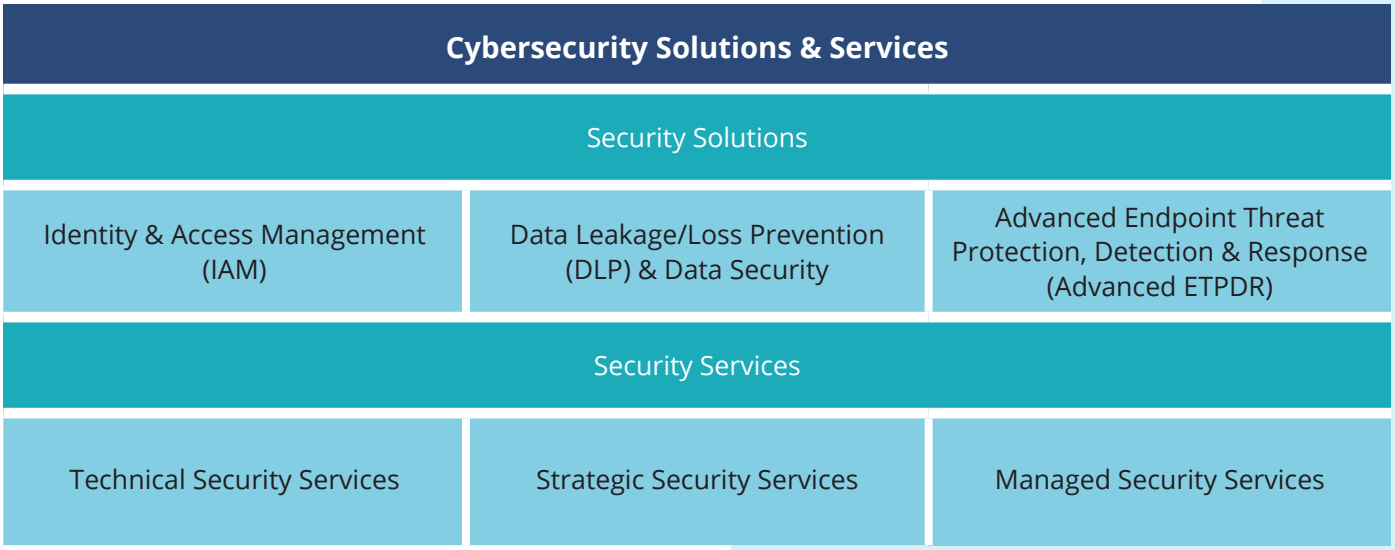
- Transparente Darstellung der Stärken und Herausforderungen relevanter Anbieter
- Differenzierte Positionierung der Anbieter nach Marktsegmenten
- Betrachtung verschiedener Märkte

Diese Studie bietet IT-Dienstleistern und Vendoren somit eine wesentliche Entscheidungsgrundlage für Positionierungs-, Beziehungs- und Go-to-Market-(GTM)-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.

Simplified illustration



Source: ISG 2022

Security Solutions

Im Rahmen der Lösungs-Quadranten werden nur Software- und Lösungsanbieter untersucht, die Sicherheitssoftware mit einem Lizenzierungsmodell und als On-Demand-as-a-Service-Lösung anbieten. Dienstleister mit gleichwertigen Lösungen, die als Teil eines umfassenderen Projekts einen Mehrwert schaffen, aber keine Lizenzmodelle anbieten, werden in den Lösungsquadranten nicht berücksichtigt.

Identity & Access Management (IAM)

IAM-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die 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 den definierten 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 Funktionalitäten im Zusammenhang mit Social Media und mobilen Anwendungen erwartet, um deren Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Auch das Machine Identity Management (MIM), also die Verwaltung von Maschinenidentitäten, ist hier mit berücksichtigt.

Auswahlkriterien:

- Die Lösung sollte in Kombination vor Ort, in der Cloud, als Identity as a Service (IDaaS) und einem verwalteten Modell eines Drittanbieters eingesetzt werden können.
- Authentifizierungs-Unterstützung anhand einer Kombination von Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA) sowie risiko- und kontextbasierten Modellen
- Unterstützung von rollenbasiertem Zugriff und Privileged Access Management (PAM)
- Zugriffsmanagement für eine oder mehrere Unternehmensanforderungen wie Cloud, Endpunkte, mobile Geräte, Anwendungsprogrammierschnittstellen (APIs) und Webanwendungen
- Unterstützung von einem oder mehreren älteren und neueren IAM-Standards, einschließlich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM
- Sicherer Zugriff durch eine oder mehrere der folgenden Möglichkeiten: 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 gewährleisten.

Sie gewinnen erheblich an Bedeutung, da es für Unternehmen immer schwieriger wird, Datenbewegungen und -übertragungen zu kontrollieren. Die Zahl der Geräte, einschließlich der Mobilgeräte, 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. Datensicherheitslösungen schützen Daten vor unberechtigtem Zugriff, Offenlegung oder Diebstahl.

Auswahlkriterien:

- DLP-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
- DLP-Unterstützung über eine beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt
- Schutz von sensiblen Daten schützen, egal ob es sich dabei um strukturierte oder unstrukturierte Daten, Text- oder Binärdaten handelt
- Grundlegender Management-Support verfügbar, einschließlich, aber nicht nur Reporting, Richtlinienkontrolle, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
- Fähigkeit, sensible Daten zu erkennen, Richtlinien durchzusetzen, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern

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. Endpunkt-Sicherheitslösungen, die Secure Access Service Edge (SASE) integrieren, werden hier ebenfalls berücksichtigt. Für ISG umfasst die Endpunktsicherheit auch den entsprechenden Schutz von OT-Lösungen (Operational Technology).

Diese Lösungen gehen über einen reinen signaturbasierten Schutz hinaus und beinhalten auch den Schutz vor Risiken 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 gefährdeten 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 dem Agenten, der im Host-System residiert und die Überwachungs- und Reporting-Funktionen für die Vorfälle bereitstellt.

Auswahlkriterien:

- 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
- Automatische Reaktionsfunktionen, unter anderem das Löschen bösartiger Dateien, Sandboxing, das Beenden verdächtiger Prozesse, das Isolieren infizierter Endpunkte und das Sperren verdächtiger Konten

Security Services

Im Rahmen der folgenden Service-Quadranten werden nur Anbieter untersucht, die Sicherheitsdienstleistungen mit einem engagierten und zertifizierten Expertenteam anbieten. Produkt- und Lösungsanbieter mit gleichwertigen Angeboten, die nur mit ihrer Lösung als Teil von Support-Services einen Mehrwert schaffen, werden in den Service-Quadranten nicht berücksichtigt.

Managed Security Services (MSS)

Unter MSS fallen Betrieb und Management von IT- und OT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). **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:

- Zu den typischen Dienstleistungen gehören Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests, Firewall-Betrieb, Anti-Virus-Betrieb, Identity & Access Management (IAM)-Betriebsservice, Data Leakage/Loss Prevention (DLP)-Betrieb und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Insbesondere ist auch Secure Access Service Edge (SASE) mit berücksichtigt.
- Angebot von Sicherheitsdiensten wie Erkennung und Vorbeugung, Security Information & Event (SIEM) sowie Sicherheitsberatung und Audits, per Fernzugriff oder vor Ort beim Kunden
- 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) und Global Information Assurance Certification (GIAC)

Technical Security Services (TSS)

TSS umfassen Integration, Wartung und Support von IT- wie auch OT (Operational Technology) Sicherheitsprodukten oder -lösungen. Auch DevSecOps-Dienste werden hier berücksichtigt. Sie adressieren alle Sicherheitsprodukte, einschließlich Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, Unified Threat Management (UTM), OT Security, SASE und weitere Angebote. **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**.

Auswahlkriterien:

- Nachweisliche Erfahrung mit der Implementierung von Cybersecurity-Lösungen für Unternehmen im jeweiligen Land
- Autorisierung durch Sicherheitstechnologie-Anbieter (Hardware und Software) für den Vertrieb und die Unterstützung von Sicherheitslösungen
- Experten mit Zertifizierungen (von Herstellern, Verbänden und Organisationen, staatlichen Stellen), die in der Lage sind, Sicherheitstechnologien zu unterstützen

Strategic Security Services (SSS)

SSS umfassen in erster Linie die Beratung für IT- und OT-Sicherheit. Die in diesem Quadranten abgedeckten Services beinhalten 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 einer auf die individuellen Anforderungen zugeschnittenen Cybersicherheits-Strategie für Unternehmen. **In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf eigene Produkte oder Lösungen konzentrieren**. Die hier analysierten Dienste decken alle Sicherheitstechnologien ab, insbesondere OT-Sicherheit und SASE.

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

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

Quadrants	USA	UK	Nordische Länder	Deutschland	Schweiz	Frankreich	Brasilien	Australien	Singapur & Malaysia	US Public Sector
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 **Februar bis März 2022**. Die Ergebnisse werden den Medien im **Juli 2022** präsentiert.

Meilensteine	**Beginn**	**Beginn**
Start	16. Februar 2022	
Umfrage-Phase	16. Februar 2022	14. März 2022
Sneak Preview	April 2022	
Pressemitteilung	Juli 2022	

Mit Klick auf diesen Link können Sie die ISG Provider Lens™ 2022 Research-Agenda einsehen oder herunterladen.

Zugang zum Online-Portal

Hier können Sie über Ihre bereits erstellten Zugangsdaten den Fragebogen einsehen bzw. herunterladen. Um ein neues Passwort zu erstellen, befolgen Sie bitte die Anweisungen in der Einladungs-E-Mail. Wir freuen uns auf Ihre Teilnahme!

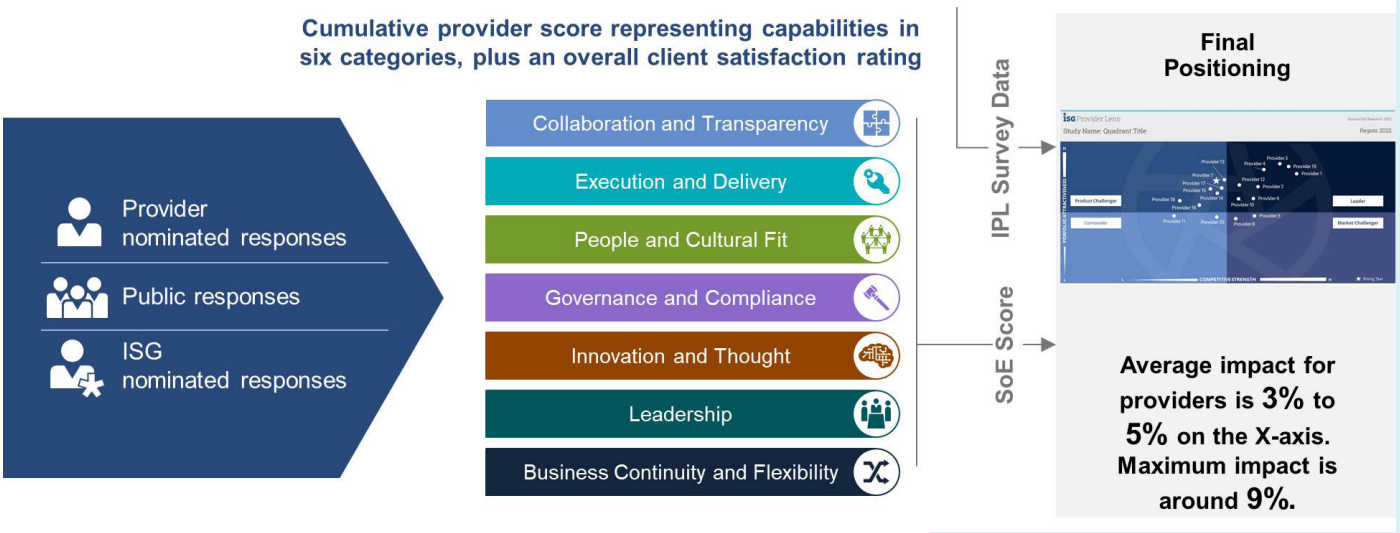
Haftungsausschluss für die Forschungsproduktion:

ISG sammelt Daten zum Zwecke der Recherche und Erstellung von Dienstleister-/Anbieterprofilen. Die Profile und unterstützenden Daten werden von den ISG-Beratern verwendet, um Empfehlungen auszusprechen und ihre Kunden über die Erfahrungen und Qualifikationen der von den Kunden identifizierten geeigneten Dienstleistern/Anbietern für Outsourcing-Arbeiten zu informieren. Diese Daten werden im Rahmen des ISG FutureSource-Prozesses und des Candidate Provider Qualification (CPQ)-Prozesses erhoben. ISG kann sich dafür entscheiden, diese gesammelten Daten, die sich auf bestimmte Länder oder Regionen beziehen, nur für die Ausbildung und die Zwecke ihrer Berater zu verwenden und keine ISG Providers Lens™-Berichte zu erstellen. Diese Entscheidungen werden auf der Grundlage des Umfangs und der Vollständigkeit der direkt von den Dienstleistern/Anbietern erhaltenen Informationen und der Verfügbarkeit von erfahrenen Analysten für diese Länder oder Regionen getroffen. Die eingereichten Informationen können auch für einzelne Forschungsprojekte oder für Briefing-Notizen verwendet werden, die von den leitenden Analysten verfasst werden.

ISG Star of Excellence™ - Aufruf zur Nominierung

Der „Star of Excellence“ ist eine unabhängige Auszeichnung für herausragende Serviceleistungen, die auf dem Konzept der „Stimme des Kunden“ basieren. Das Programm wurde von ISG entwickelt, um Kundenfeedback über den Erfolg von Dienstleistern zu sammeln, die die höchsten Standards für exzellenten Kundenservice und Kundenorientierung demonstrieren.

In der globalen Umfrage geht es um Dienstleistungen, die mit IPL-Studien zu tun haben. Alle ISG-Analysten werden kontinuierlich mit Informationen über die Kundenerfahrungen aller relevanten Dienstleister versorgt. Diese Informationen ergänzen das bereits vorhandene Feedback von Beratern aus erster Hand, welches für die IPL-Studien im Rahmen des praxisorientierten Beratungsansatzes genutzt wird.



Anbieter sind eingeladen, ihre Kunden unter Nominate zur Teilnahme aufzurufen. Nach Abgabe der Nominierung versendet ISG eine E-Mail-Bestätigung an beide Seiten. Selbstverständlich werden alle Kundendaten anonymisiert und nicht an Dritte weitergegeben.

Unsere Vision ist es, den Star of Excellence als die führende Auszeichnung für herausragenden Kundenservice und als Maßstab für die Messung der Kundenzufriedenheit zu etablieren.

Bitte nutzen Sie den Abschnitt „Client Nomination“ auf der Star of Excellence Website, um sicherzustellen, dass Ihre ausgewählten Kunden das Feedback für Ihr nominiertes Engagement abgeben.

Wir haben eine E-Mail eingerichtet, an die Sie Fragen oder Kommentare richten können. Diese E-Mail wird täglich überprüft. Bitte berücksichtigen Sie, dass eine Antwort bis zu 24 Stunden dauern kann. Hier ist die E-Mail Adresse: Star@isg-one.com.

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
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

Kontaktpersonen für diese Studie

Frank Heuer
Lead Analyst, Germany, Switzerland

Gowtham Kumar
Lead Analyst, U.S.

Arun Kumar Singh
Lead Analyst, U.K., Nordics

Benoit Scheuber
Lead Analyst, France

Dr. Maxime Martelli
Co-Lead Analyst, France

Craig Baty
Lead Analyst, Australia

Sergio Rezende
Lead Analyst, Brazil

Keao Caindec
Lead Analyst, U.S. Public Sector

Monica K
Research Analyst

Ridam Bhattacharjee
Project Manager

ISG Provider Lens QCRT Programmbeschreibung

Das ISG Provider Lens Programm bietet Marktbewertungen von praxiserfahrenen Experten; sie haben einen regionalen Fokus und beruhen auf unabhängiger Research. ISG stellt sicher, dass in jede Studie Advisors einbezogen werden, um die entsprechenden Marktgegebenheiten in Bezug auf die jeweiligen Servicebereiche/ Technologietrends, die Präsenz der Serviceanbieter und den Unternehmenskontext abzudecken. ISG verfügt in jeder Region über fachkundige Vordenker und angesehene Advisors, die sich sowohl mit den Portfolios und Angeboten der Provider als auch den Anforderungen der Unternehmen und den Markttrends auskennen. Im Durchschnitt nehmen drei Berater als Mitglieder des Quality & Consistency Review Teams (QCRT) für jede Studie teil. Das QCRT stellt sicher, dass in jede Studie ergänzend zur Primär- und Sekundärrecherche der Analysten auch die Erfahrungen der ISG Advisors im jeweiligen Bereich einfließen. Die ISG Advisors nehmen an jeder Studie als QCRT-Mitglieder teil und leisten entsprechend ihrer Verfügbarkeit und ihres Fachwissen auf verschiedenen Ebenen Beiträge.

Die QCRT Advisors.

- helfen, Quadranten und Fragebögen zu definieren und zu validieren,
- beraten bei der Einbeziehung von Dienstleistern, nehmen an Briefing-Gesprächen teil,
- stellen ihre Sicht der Bewertungen von Dienstleistern dar und überprüfen Berichtsentwürfe.

Das ISG Provider Lens QCRT Programm vervollständigt den Research-Prozess und leistet Unterstützung zur Durchführung umfassender research-orientierter Studien.

Quality & Consistency Review Team für diese Studie

Doug Saylors
Co-Lead, ISG Cybersecurity

Roger Albrecht
Co-Lead, ISG Cybersecurity

Anand Balasubramanium
Senior Consultant

Benötigen Sie weitere Informationen?

Bei Fragen können Sie uns gerne unter isglens@isg-one.com kontaktieren.