ISG Provider Lens™

# Cybersecurity – Services and Solutions

Eine vergleichende Analyse des Cybersicherheitsmarktes hinsichtlich der Portfolioattraktivität und der Wettbewerbsstärke der Anbieter

**BROSCHÜRE | JANUAR 2025 | AUSTRALIEN, BRASILIEN, FRANKREICH, DEUTSCHLAND, SCHWEIZ, GROSSBRITANNIEN, USA, USA-AMERIKANISCHER PUBLIC SECTOR UND GLOBAL**

Inhaltsverzeichnis

**Cybersicherheit im Zeitalter der KI und neuer disruptiver Technologien**

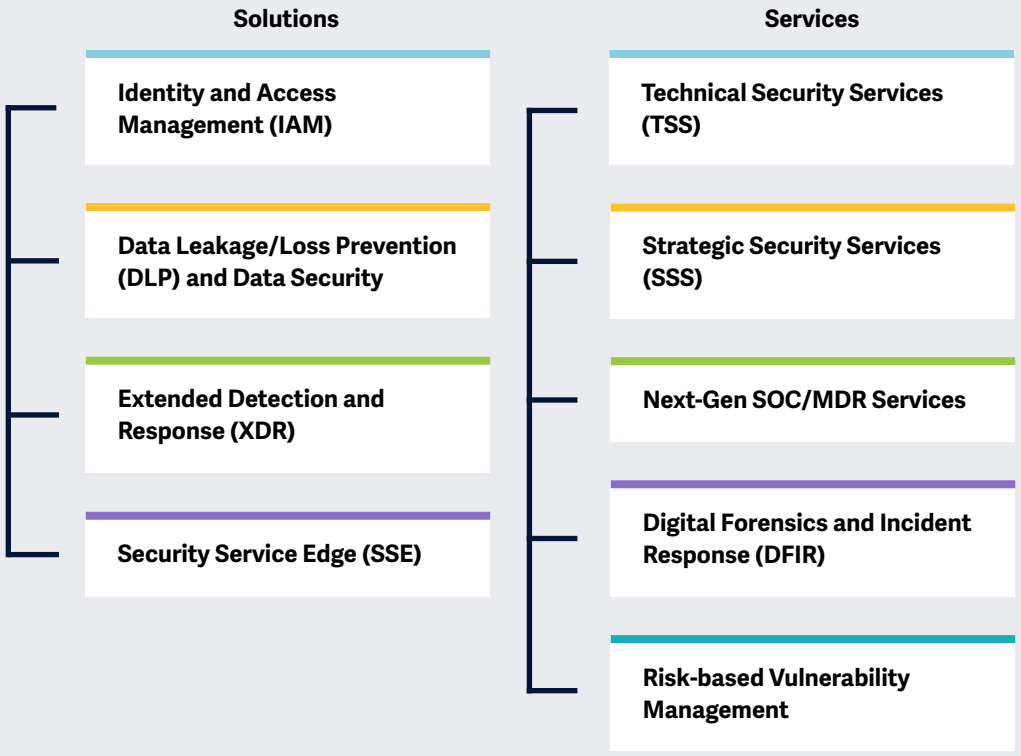
Im Zeitalter rascher technologischer Fortschritte und der KI-Integration in das Tagesgeschäft ist die Cybersicherheitslandschaft zunehmend komplexer und vielschichtiger geworden. Regulatorische Anforderungen wie die Richtlinie zur Netz- und Informationssicherheit (NIS) 2 der Europäischen Union erhöhen die Nachfrage nach robusten Cybersicherheitsmaßnahmen und zwingen Organisationen, ihre Security Frameworks angesichts neuer Bedrohungen auf den Prüfstand zu stellen. Gleichzeitig hat die Kommerzialisierung von Hacking Tools die Einstiegshürden für böswillige Akteure erheblich gesenkt, so dass cyberkriminelle Aktivitäten und entsprechende Risiken signifikant zugenommen haben.

Die zunehmende Verbreitung von Technologien hat die Angriffsfläche vergrößert und stellt Unternehmen vor große Herausforderungen hinsichtlich OT/IT Security. Der Mangel an qualifiziertem Cybersecurity-Personal hat diese Komplexität noch verstärkt und die Nachfrage nach Managed Security Services in die Höhe getrieben, denn zur Verstärkung ihrer Verteidigung greifen Unternehmen auf externes Fachwissen zurück.

Die Weiterentwicklung der KI birgt Risiken und Chancen im Bereich der Cybersicherheit. Sicherheitsdienstleister helfen ihren Kunden, sich in der Cybersicherheitslandschaft zurechtzufinden. Wachsamkeit ist entscheidend, um neue Bedrohungen zu erkennen und abzuschwächen und die transformativen Auswirkungen neuer Technologien wie Quantencomputing zu verstehen. In Reaktion auf diese Herausforderungen investieren Unternehmen zunehmend in Lösungen wie Identity & Access Management (IAM), Data Loss Prevention (DLP), Extended Detection & Response (XDR) und Security Service Edge (SSE), die fortschrittliche Tools und menschliches Fachwissen mit verhaltens- und kontextbezogener Intelligenz kombinieren, um die Sicherheitslage zu verbessern.

Abgedeckte Schwerpunkt-bereiche der Studie „Cybersecurity – Services and Solutions 2025".

Vereinfachte Darstellung. Quelle: ISG 2025




**Die ISG Provider Lens™ Studie „Cybersecurity – Services & Solutions " bietet Geschäfts- und IT-Entscheidern folgende Vorteile:**

- Transparente Darstellung der Stärken und Schwächen relevanter Anbieter
- Eine differenzierte Positionierung der Anbieter nach Segmenten, basierend auf Wettbewerbsstärken und Portfolio-Attraktivität
- Fokus auf verschiedene Märkte: Australien, Brasilien, Frankreich, Deutschland, Schweiz. Großbritannien, die USA und den US-amerikanischen Public Sector
- Die Themen IAM, SSE und XDR werden für den globalen Markt analysiert.
- Um länderspezifische Merkmale in dieser globalen Studie zu berücksichtigen, wird die XDR-Analyse auf Brasilien ausgeweitet. DLP wird ausschließlich für Deutschland analysiert. DFIR wird für Frankreich als Schwerpunktthema untersucht, und eine Analyse des Risk-Based Vulnerability Managements wird für Frankreich und Brasilien vorgenommen.

Die Studie bietet eine wesentliche Entscheidungsgrundlage für Positionierungs-, Kooperations- und Go-to-Market-Überlegungen. ISG Advisors und Unternehmenskunden nutzen Informationen aus diesen Reports auch zur Evaluierung ihrer derzeitigen sowie potenzieller neuer Anbieterbeziehungen.

**Definition**

Die im Rahmen dieses Quadranten bewerteten IAM-Lösungsanbieter differenzieren sich über ihre proprietäre Software, u.a. SaaS, und zugehörige Services für die Verwaltung von Benutzeridentitäten im Unternehmen. Reine Dienstleister, die keine IAM-Produkte (on-premise oder in der Cloud) auf Basis proprietärer Software anbieten, werden hier nicht berücksichtigt. Je nach den Anforderungen der jeweiligen Unternehmen können diese Lösungen vor Ort, in von Kunden verwalteten Clouds, als As-a-Service-Modelle oder in einer Kombination dieser Optionen bereitgestellt werden.

IAM-Lösungen fokussieren sich auf die Verwaltung von Benutzeridentitäten und Zugriffsrechten, einschließlich des spezialisierten Zugriffs durch Privileged Access Management (PAM), das durch definierte Richtlinien geregelt wird. IAM-Suites integrieren Sicherheitsmechanismen, Frameworks und Automatisierungen für die Erstellung von Benutzer- und Angriffsprofilen in Echtzeit, um den sich entwickelnden Anwendungsanforderungen gerecht zu werden. Von den Anbietern wird zudem erwartet, dass sie Funktionen für den Zugang zu sozialen Medien und für den mobilen Zugriff anbieten und damit Sicherheitsanforderungen erfüllen, die über die traditionelle Verwaltung von Webrechten hinausgehen. Dieser Quadrant adressiert auch Machine Identity Management.

Auswahlkriterien

1. Angebot an Lösungen, die **vor Ort, in der Cloud, als Identity-as-a-Service** (IDaaS) oder über ein gemanagtes Third-Party-Modell eingesetzt werden können
2. Lösungen mit **Authentifizierungs-Support** anhand einer Kombination von **Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA)**, risiko- und kontextbasierten Modellen
3. Unterstützung von **rollenbasiertem Zugriff** und PAM
4. **Zugriffsmanagement** für diverse Unternehmensanforderungen wie **Cloud, Endpunkte, mobile Geräte, APIs und Webanwendungen**
5. Lösungen mit Unterstützung für **einen oder mehrere ältere und neue IAM-Standards**, unter anderem SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM
6. Portfolio mit einer oder mehreren der folgenden Lösungen: **Directory, Dashboard oder Self-Service Management** sowie Lifecycle Management (Migration, Synchronisierung und Replikation) zur Unterstützung eines sicheren Zugangs

**Definition**

Die in diesem Quadranten bewerteten Anbieter von DLP-Lösungen zeichnen sich durch ihre proprietäre Software, u.a. SaaS, und die damit verbundenen Services aus. Reine Dienstleister, die keine DLP-Produkte (on-Premise oder in der Cloud) auf Basis proprietärer Software anbieten, werden hier nicht berücksichtigt. DLP-Lösungen können sensible Daten identifizieren und überwachen und autorisierten Benutzern Zugang gewähren. Sie bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf diversen Geräten bieten.

DLP-Lösungen helfen Unternehmen, die Herausforderungen bei der Kontrolle von Datenbewegungen zu bewältigen; schließlich haben über ein Drittel der Datenverletzungen ihren Ursprung im Unternehmen. Die zunehmende Verbreitung von mobilen und anderen Geräten zur Datenspeicherung verstärkt diese Sorgen, da Daten ohne zentrale Gateways ausgetauscht werden können.

Data-Security-Lösungen schützen vor unbefugtem Zugriff und Diebstahl durch die Priorisierung, Klassifizierung und Überwachung von Daten (im Ruhezustand und bei der Übertragung) und helfen, die Sicherheit der gefährdeten Daten zu verbessern.

Auswahlkriterien

1. DLP-Lösungen auf Basis von **proprietärer Software** und nicht auf Basis von Software von Drittanbietern
2. Nachweisliche DLP-Unterstützung über eine **beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt**
3. Schutz **sensibler Daten**, ob **strukturiert oder unstrukturiert**, in Text- oder Binärformaten
4. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung, sowie erweiterte Funktionen zur Erkennung von Bedrohungen
5. Angebot an Lösungen, die **sensible Daten erkennen, Richtlinien durchsetzen**, den Datenverkehr überwachen und die Daten-Compliance verbessern

**Definition**

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich durch ihre Plattformen aus, die Daten und Warnungen aus verschiedenen Komponenten zur Bedrohungsabwehr, -erkennung und -reaktion integrieren, korrelieren und kontextualisieren. XDR ist eine cloudbasierte Technologie, die mehrere Sicherheitslösungen integriert und Analysen zur Verbesserung der Erkennungsgenauigkeit einsetzt. Sie konsolidiert Sicherheitsprodukte für eine höhere Transparenz und einen besseren Bedrohungskontext in Arbeitsbereichen, Netzwerken und Workloads des jeweiligen Unternehmens.

XDR-Lösungen nutzen Telemetrie- und Kontextdaten zur Erkennung und Reaktion und integrieren mehrere Produkte in eine einheitliche Schnittstelle. Sie zeichnen sich durch einen hohen Automatisierungsgrad aus und priorisieren Warnungen nach ihrem Schweregrad, um die erforderlichen maßgeschneiderten Reaktionen festzulegen.

Reine Dienstleister, die keine XDR-Lösung auf Basis proprietärer Software anbieten, werden in diesem Quadranten nicht berücksichtigt. XDR-Lösungen zielen darauf ab, die Produktvielfalt, Alarmmüdigkeit und Integrationsprobleme zu verringern. Sie unterstützen Sicherheitsteams bei der Verwaltung von SIEM- (Security Information and Event Management) oder SOAR-Lösungen (Security Orchestration, Automation & Response) und helfen dabei, deren Wert zu steigern.

Auswahlkriterien

1. XDR-Lösungen auf Basis von **proprietärer Software** und nicht auf Basis von Software von Drittanbietern
2. Die XDR-Lösung muss zwei Hauptkomponenten umfassen: **XDR-Frontend und XDR-Backend**
3. Frontend mit **drei oder mehr Lösungen bzw. Sensoren**, einschließlich, aber nicht beschränkt auf, **Endpunkt-Erkennung und -Reaktion, Endpunkt-Schutzplattformen**, Netzwerkschutz (Firewalls und IDPS), **Netzwerk-Erkennung und -Reaktion**, Identitätsmanagement, E-Mail-Sicherheit, Erkennung mobiler Bedrohungen, Schutz von Cloud-Workloads und Betrugsidentifizierung
4. **Umfassende und vollständige Abdeckung und Visibilität aller Endpunkte** im Netzwerk
5. Nachweisliche **effektive Abwehr** von komplexen Bedrohungen wie **Advanced Persistent Threats, Ransomware** und Malware
6. Nutzung und Analyse von **Bedrohungsdaten** sowie **Echtzeit-Insights in Bedrohungen**, die von den Endpunkten ausgehen
7. Lösung mit **automatischen Reaktionsfunktionen**

**Definition**

Die für diesen Quadranten bewerteten SSE-Lösungsanbieter offerieren cloud-zentrierte Lösungen, die proprietäre Software und/oder Hardware und zugehörige Dienste zusammenführen und einen sicheren Zugang zu Cloud Services, SaaS-Anwendungen, Webdiensten und privaten Anwendungen ermöglichen. Die entsprechenden Provider bieten SSE-Lösungen als integrierten Sicherheitsdienst über global positionierte Points of Presence (PoP) mit Unterstützung für lokale Datenspeicherung an, der Einzellösungen wie Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateways (SWG) und Firewall as a Service (FWaaS) kombiniert. SSE kann auch andere Sicherheitslösungen wie DLP, Browser-Isolierung und Next-Generation Firewalls (NGFW) umfassen, um einen sicheren Zugriff auf Anwendungen in der Cloud wie auch vor Ort zu ermöglichen.

Die Anbieter demonstrieren ihre Erfahrung mit der Einhaltung lokaler, regionaler und nationaler Gesetze (z.B. hinsichtlich Datensouveränität) für globale Kunden. Die Netzwerkkomponenten von Secure Access Service Edge (SASE), wie SD-WAN, die in der ISG Provider Lens™ Studie „Network – Software-Defined Services & Solutions 2025“ abgedeckt werden, sind hier nicht berücksichtigt.

Auswahlkriterien

1. Bereitstellung von SSE als **integrierte Lösung** mit **ZTNA-, CASB-, SWG- und FWaaS-Komponenten**
2. Angebot an Lösungen **überwiegend auf Basis von proprietärer** Software, **evtl. in Teilen auch basierend auf Partnerlösungen, aber nicht vollständig** auf Basis von Software **von Drittanbietern**
3. Aufrechterhaltung **globaler Präsenzpunkte** zur Bereitstellung von Lösungen
4. **SSE-Funktionalitäten sowohl für Cloud- als auch für On-Premises-Umgebungen** (einschließlich hybrider Umgebungen)
5. **Kontextbezogene und verhaltensbezogene Auswertungen und Analysen** (Nutzeridentitäts- und Verhaltensanalysen bzw. User Entity & Behavior Analytics/UEBA) zur Aufdeckung und Verhinderung bösartiger bzw. verdächtiger Absichten
6. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
7. Gewährleistung der **weltweiten Verfügbarkeit der Lösungen**

**Definition**

Die für diesen Quadranten bewerteten TSS-Anbieter sind auf die Integration, Wartung und Unterstützung von IT- und OT-Sicherheitsprodukten bzw. -lösungen spezialisiert. TSS umfasst eine breite Palette von Sicherheitsprodukten, u.a. Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, OT-Sicherheit, SASE etc.

Diese Anbieter offerieren Playbooks und Roadmaps zur Verbesserung der Sicherheit mithilfe von Best-of-Breed Tools; sie verbessern damit die Sicherheitslage und reduzieren Bedrohungen. Mit ihren Portfolios unterstützen sie die Transformation kompletter oder einzelner Sicherheitsarchitekturen sowie die Identifizierung, Bewertung, Gestaltung und Implementierung von Produkten und Lösungen. Sie investieren in den Aufbau von Partnerschaften mit Anbietern von Sicherheitslösungen und -technologien, um spezialisierte Akkreditierungen zu erlangen und ihr Portfolio zu erweitern.

Dieser Quadrant umfasst auch klassische Managed Security Services, die ohne ein Security Operations Center erbracht werden. Es geht hier um Dienstleister, die sich nicht ausschließlich auf ihre eigenen Produkte fokussieren, sondern auch in der Lage sind, Lösungen anderer Anbieter und Dienstleister zu implementieren und zu integrieren.

Auswahlkriterien

1. Nachweisliche Erfahrung mit der **Entwicklung und Implementierung von Sicherheitslösungen** für Unternehmen im jeweiligen Land
2. **Autorisierung durch Sicherheitstechnologie-Anbieter** (Hardware und Software) für den Vertrieb und die Unterstützung von Sicherheitslösungen
3. **Experten mit Zertifizierungen** (von Herstellern, Verbänden und Organisationen, staatlichen Stellen), die in der Lage sind, Sicherheitstechnologien zu unterstützen
4. **Kein ausschließlicher Fokus auf proprietäre Produkte** oder Lösungen
5. Präsentation von **Fallstudien**, die die erfolgreiche Entwicklung, Einführung und Verwaltung von Cybersicherheitslösungen für Unternehmen im Zielland belegen

**Definition**

Die in diesem Quadranten bewerteten Provider von Strategic Security Services (SSS) bieten IT und OT Security Consulting an. Zu den Dienstleistungen zählen Sicherheitsaudits, Bewertungen, Sensibilisierung und Schulungen. Diese Anbieter helfen auch bei der Bewertung des Sicherheitsreifegrads und der Festlegung von Cybersicherheitsstrategien, um unternehmensspezifische Anforderungen zu erfüllen.

Sie beschäftigen erfahrene Sicherheitsberater für die Planung und Verwaltung von umfassenden Sicherheitsprogrammen für Unternehmenskunden. Angesichts der steigenden Nachfrage von KMUs und des Fachkräftemangels stellen SSS Provider Experten auf Abruf über virtuelle CISO-Dienste zur Verfügung.

Sie erstellen Geschäftskontinuitätspläne, legen Prioritäten für die Wiederherstellung kritischer Anwendungen fest und führen praktische Notfallübungen durch, um die Cyberkompetenz und die Reaktionsfähigkeit von Unternehmensführern und Mitarbeitenden zu verbessern. Hinzu kommt Unterstützung bei der Auswahl von Sicherheitstechnologien und Lieferanten, der Überprüfung von Organisationsstrukturen für die Cybersicherheit sowie der Bewertung von Sicherheitsprozessen und -praktiken und deren Verbesserung im Hinblick auf bestehende Risiken. In diesem Quadranten werden Dienstleister betrachtet, die sich nicht ausschließlich auf eigene Produkte bzw. Lösungen fokussieren.

Auswahlkriterien

1. Nachweisliche Leistungen in SSS-Bereichen wie **Evaluierung, Assessments, Anbieterauswahl, Lösungs- und Risikoberatung**
2. Kompetenz in der Anwendung von bewährten Verfahren und Security Frameworks wie ISO 27000, NIST und CIS
3. **Angebot von mindestens einem der oben genannten** Strategic Security Services im jeweiligen Land
4. Bereitstellung von **Sicherheitsberatungsdiensten unter Einsatz von Frameworks wie NIST und ISO**
5. **Kein ausschließlicher Fokus auf proprietäre Produkte** oder Lösungen

**Definition**

Die in diesem Quadranten bewerteten Anbieter offerieren Services im Zusammenhang mit der kontinuierlichen Überwachung von IT- und OT-Infrastrukturen durch ein Security Operations Center (SOC). Es werden Dienstleister untersucht, 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 Reaktion auf und Behebung von Problemen.

Next-Gen SOC Provider erleben eine hohe Nachfrage; sie sollen die Sicherheitslage von Unternehmen stärken und die Effektivität von Sicherheitsprogrammen verbessern. Sie verbinden traditionelle Managed Security Services mit Innovationen für ein Angebot an integrierten Cyber Defense und Managed Detection & Response Services (MDR). Diese Anbieter investieren auch in Threat Detection & Hunting, Threat Intelligence, Modellierung und Forensik, Incident Management und fortschrittliche Technologien wie Automatisierung, Big Data, KI und ML, um einen ganzheitlichen Ansatz zur proaktiven Bedrohungsabwehr und fortschrittlichen Sicherheit bieten zu können.

Auswahlkriterien

1. Angebot an Standardservices, u.a. **Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests** und alle anderen Betriebsservices für einen kontinuierlichen Echtzeitschutz ohne Beeinträchtigung der Geschäftsleistung
2. Angebot von Security-Diensten wie **Prevention und Detection, Security Information & Event Management (SIEM)** sowie Sicherheitsberatung und Audits, entweder remote oder vor Ort beim Kunden
3. MDR-spezifische Funktionen, u.a. **Advanced Threat Intelligence** sowie **verhaltensbasiertes und Human-led Threat Hunting, die offensive und defensive** Sicherheitsfunktionen mit einer **einheitlichen Ansicht** für Berichte und Metriken bereitstellen
4. **Akkreditierungen** von Anbietern von Security Tools
5. **Management eigener SOCs**
6. **Zertifizierte Mitarbeiter**, z.B. mit Zertifizierungen wie Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)
7. Verfügbarkeit einer Vielzahl von gestaffelten Preismodellen

**Definition**

Die im DFIR-Quadranten bewerteten Anbieter offerieren Leistungen im Zusammenhang mit der Reaktion auf Bedrohungen bei gleichzeitiger Sicherung von Beweisen gegen Angreifer. In diesem Quadranten werden Dienstleister untersucht, die bewährte DFIR-Techniken und -Methoden anbieten und Best-of-Breed Tools einsetzen, um auf Cybersicherheitsvorfälle reagieren zu können.

DFIR befasst sich mit der Ermittlung, Untersuchung, Eindämmung und Behebung von Cybersicherheitsvorfällen. Angesichts der zunehmenden Häufigkeit und Schwere solcher Vorfälle werden entsprechende DFIR Services in Anspruch genommen. DFIR spielt eine entscheidende Rolle, um Datenverluste nach einer Sicherheitsverletzung zu erkennen und mithilfe von Playbooks wirksame Reaktionen auf Bedrohungen festzulegen. Die Dienstleister weisen Fachkenntnisse im Bereich der digitalen Forensik nach, u.a. Triage, Zeitleisten- und Protokollanalyse, Untersuchung von Malware und Artefaktanalyse.

Sie haben auch Erfahrung in der Unterstützung bei Rechtsstreitigkeiten und Audits und beherrschen Tools wie SIEM, SOAR, Endpoint Detection & Response (EDR) und XDR.

Auswahlkriterien

1. **Spezielles Incident Response Team** (CERT oder CSIRT) mit Experten mit einschlägigen Zertifizierungen wie GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE) and CISSP, die nachweislich über Fachwissen hinsichtlich der Einhaltung von Branchenstandards verfügen
2. Erfahrung und Know-how im **Umgang mit einer Vielzahl** von SIEM-, SOAR-, EDR- und XDR-Lösungen
3. Angebot von DFIR-Diensten, die **die Ursache** eines **Verstoßes ermitteln** und dessen kurz- und langfristige Auswirkungen bewerten
4. **Fähigkeiten** in den Bereichen Malware-Analyse, Entschlüsselung von Ransomware und Datenwiederherstellung
5. Nachweisliche **Partnerschaften** mit Produktanbietern und Managed Security Service Providern, um ihre Fähigkeiten hinsichtlich Threat Intelligence, Dark Web Monitoring und SOC zu verbessern und komplexe andauernde Bedrohungen (Advanced Persistent Threats) mindern zu können

**Definition**

Die in diesem Quadranten bewerteten Anbieter von Diensten für das risikobasierte Schwachstellenmanagement verfügen über hochentwickelte technische Fähigkeiten und sind in der Lage, kontinuierlich Updates für bekannte Schwachstellen und ausgefeilte Methoden zur Umgehung etablierter Schutzmaßnahmen durch Praktiken wie Penetrationstests zu liefern. Mit Hilfe von generativen KI-Tools (GenAI) können Cyberkriminelle Schwachstellen in technologischen Systemen erkennen und ausnutzen, insbesondere wenn diese vom Internet aus zugänglich sind. Dieser Trend in Verbindung mit der Zunahme von Ransomware-Vorfällen unterstreicht die Notwendigkeit eines kontinuierlichen Schwachstellenmanagements, anstatt lediglich sporadisch Bewertungen durchzuführen.

In Anbetracht der raschen Aktualisierungshäufigkeit von Internetdiensten ist die Implementierung einer kontinuierlichen Schwachstellenerkennung für eine wirksame risikobasierte Cybersicherheitsstrategie von essenzieller Bedeutung. Die Anbieter müssen inzwischen gezielte Lösungen offerieren, die über die traditionellen Praktiken hinausgehen, und einsehen, dass ein risikobasiertes Framework für die effektive Verwaltung von Schwachstellen und die Minimierung der Auswirkungen in der sich schnell entwickelnden Bedrohungslandschaft von heute unerlässlich ist.

## Auswahlkriterien

1. Verfügbarkeit spezialisierter interner Teams, die in der Lage sind, **Schwachstellen einer strengen Auswertung zu unterziehen und Lösungen** zur Beseitigung von Schwachstellen bzw. zur schrittweisen Verringerung ihres Schweregrads auf Basis konkreter Hinweise auf Angriffsvektoren **aufzuzeigen**
2. Angebot von Diensten, die **Black-Box-, Grey-Box- und White-Box-Ansätze** umfassen, und Webanwendungen, mobile Geräte, interne Netzwerke, Cloud, APIs, IoT und andere exponierte Vermögenswerte bzw. Risikoelemente auswerten können
3. Einsatz von Methoden wie **dynamisches Testen der Anwendungssicherheit (DAST), statisches Testen der Anwendungssicherheit (SAST) und Penetrationstests** für bestimmte Ziele unter Verwendung manueller und/oder automatisierter Tools für die Bereitstellung von Services
4. Angabe von Sicherheitsmängeln **nachweislich auf Basis anerkannter Industriestandards** wie SOC 2, ISO 27001, NIST 800-53, PCI-DSS und HIPPA
5. Angebot von **Wiederholungstests, spezialisierter Unterstützung und Mechanismen** zur Überwachung von Korrekturmaßnahmen, Aktualisierung der Risiko- und Schweregradmatrix (Exposition gegenüber verbleibenden Vektoren)
6. Verfügbarkeit eines **technischen Expertenteams** (Ethical Hackings) mit Zertifizierungen wie Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), CompTIA Penetration Testing (CompTIA PenTest+) und GIAC Penetration Tester (GPEN)

## Quadranten nach Regionen

Im Rahmen dieser ISG Provider Lens™ Quadrantenstudie zum Thema „Cybersecurity – Services & Solutions 2025“ werden die folgenden neun Quadranten vorgestellt:

| Quadrant | USA | UK | Deutschland | Schweiz | Frankreich | Brasilien | Australien | USA Public Sector | Global |
|---|---|---|---|---|---|---|---|---|---|
| Identity and Access Management (IAM) | | | | | | | | | ✓ |
| Data Leakage/Loss Prevention (DLP) and Data Security | | | ✓ | | | | | | |
| Extended Detection and Response (XDR) | | | | | | ✓ | | | ✓ |
| Security Service Edge (SSE) | | | | | | | | | ✓ |
| Technical Security Services (TSS) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Strategic Security Services (SSS) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Next-Gen SOC/MDR Services | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Digital Forensics and Incident Response (DFIR) | | | | | ✓ | | | | |
| Risk-based Vulnerability Management | | | | | ✓ | ✓ | | | |

**Hauptmerkmale des proprietären Frameworks:**

- Zusammenstellung von weltweit getätigten Cybersecurity-Maßnahmen und Unterstützung von Unternehmen bei der Auswahl digitaler Lösungen
- Darstellung der gesamten Wertschöpfungskette von Angebot und Nachfrage auf dem Markt
- Die inneren Kacheln stehen für Unternehmensziele/Themen
- Die äußeren Kacheln stehen für Initiativen
- Hinter jeder äußeren Kachel stehen spezifische Fähigkeiten von bestimmten marktführenden Anbietern und Lösungen

Die Research-Phase umfasst die Befragung, Evaluierung, Analyse und Validierung und läuft von Januar bis Februar 2025. Die Ergebnisse werden den Medien im Juli 2025 präsentiert.

| Meilensteine | Beginn | Ende |
|---|---|---|
| Start der Umfrage | 7. Januar 2025 | |
| Umfrage-Phase | 7. Januar 2025 | 7. Februar 2025 |
| Sneak Preview | Mai 2025 | Juni 2025 |
| Pressemitteilung & Veröffentlichung | Juli 2025 | |

Das Einholen von Kundenstimmen im Rahmen des Star of Excellence-Programms erfordert frühzeitige Kundenempfehlungen (keine offizielle Referenz erforderlich), denn die CX-Bewertungen haben einen direkten Einfluss auf die Position des jeweiligen Anbieters im IPL-Quadranten und die Auszeichnungen.

Mit Klick auf diesen Link können Sie die ISG Provider Lens™ 2025 Research-Agenda einsehen bzw. 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!

**Buyers Guide**

ISG Software Research, ehemals „Ventana Research", bietet durch die Bewertung von Technologieanbietern und Produkten im Rahmen seiner „Buyers Guides" entsprechende Markteinblicke. Die Ergebnisse beruhen auf der forschungsbasierten Analyse von Produkt- und Kundenerfahrungskategorien sowie der Einstufung und Bewertung von Softwareanbietern und -produkten, um fundierte Entscheidungen und Auswahlprozesse für Technologien zu erleichtern.

Im Zuge der Einführung der IPL-Studie zum Thema Cybersecurity –Services & Solutions möchte ISG die Gelegenheit nutzen, um auf damit zusammenhängende Untersuchungen und Erkenntnisse aufmerksam zu machen, die ISG Research im Jahr 2025 veröffentlichen wird. Weitere Informationen finden Sie im Buyers Guide Researchplan.

**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 von geeigneten Anbietern für die von den Kunden identifizierten 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.

**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. Dieses 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. So werden alle ISG-Analysten 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 „Nominate (for Providers)" 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@cx.isg-one.com

**ISG Star of Excellence**

Die Marktforschungsstudie „ISG Provider Lens™ 2025 – Cybersecurity – Services and Solutions" analysiert die entsprechenden Softwareanbieter/Dienstleister im deutschen Markt auf Basis eines mehrstufigen Marktforschungs- und Analyseprozesses und positioniert diese Anbieter auf Basis der ISG Research™-Methodik.

**Sponsor der Studie:**
Heiko Henkes

**Leitende Analysten:**
Frank Heuer, Gowtham Kumar, Bhuvaneshwari Mohan, Benoit Scheuber, Dr. Maxime Martelli, Andrew Milroy und João Mauro

**Forschungsanalyst:**
Monica K, Sandya Kattimani, Rafael Rigotti and Bhuvaneshwari Mohan

**Projektmanager:**
Shreemadhu Rai B

Information Services Group übernimmt die alleinige Verantwortung für diesen Bericht. Soweit nicht anders angegeben, wurden sämtliche Inhalte, u.a. Abbildungen, Marktforschungsdaten, Schlussfolgerungen, Aussagen und Stellungnahmen im Rahmen dieses Berichtes von Information Services Group, Inc. entwickelt und sind Alleineigentum von Information Services Group Inc.

Die in dieser Studie vorgestellten Marktforschungs- und Analysedaten stammen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. ISG ist sich bewusst, dass in der Zeitspanne zwischen der Marktforschungsphase und der Veröffentlichung eventuell Marktentwicklungen in Form von Fusionen und Übernahmen stattfinden können und räumt ein, dass sich solche Veränderungen nicht in den Reports für diese Studie widerspiegeln werden.

Falls nicht anders angegeben, sind alle Umsätze in US-Dollar (USD) angegeben.

## Kontaktpersonen für diese Studie

### Sponsor der Studie

Heiko Henkes

**Director and Principal Analyst**

Frank Heuer

**Lead Analyst - Deutschland, Schweiz**

Gowtham Kumar

**Lead Analyst - U.S.A., U.S.A. Public Sector, Global**

Bhuvaneshwari Mohan

**Lead Analyst- U.K., U.S.A. Public Sector, Global**

Benoit Scheuber

**Lead Analyst - Frankreich**

Dr. Maxime Martelli

**Lead Analyst - Global**

Andrew Milroy

**Lead Analyst - Australien**

João Mauro

**Lead Analyst - Brasilien**

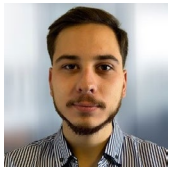
Monica K

**Research Analyst**

## Kontaktpersonen für diese Studie

Sandya Kattimani

**Research Analyst**



Rafael Rigotti

**Research Analyst**

Rajesh Chillappagari

**Data Analyst**

Laxmi Sahebrao

**Data Analyst**

Shreemadhu Rai B

**Project Manager**

**ISG Provider Lens Advisors Involvement Program**

Das ISG Provider Lens Programm bietet Marktbewertungen von praxiserfahrenen Experten; sie haben einen regionalen Fokus und beruhen auf unabhängigem 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 Consultant Advisors als Mitglieder des Quality & Consistency Review Teams für jede Studie teil.

Die Consultant Advisors stellen 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 Mitglieder der Beratergruppe teil und leisten entsprechend ihrer Verfügbarkeit und ihres Fachwissen auf verschiedenen Ebenen Beiträge.

Die Consultant 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

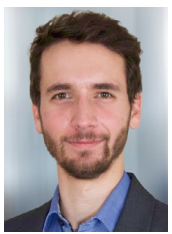
## ISG-Berater für diese Studie

Doug Saylors

**Partner, Co-lead ISG Cybersecurity**

David Gordon

**Principal Consultant Cybersecurity**



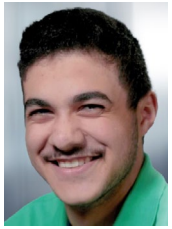
Anas Barmo

**Senior Consultant Cybersecurity**

Brendan Prater

**Consulting Manager Cybersecurity**

# ISG-Berater für diese Studie



Marco Ezzy

**Consultant Cybersecurity**

Tim Merscheid

**Consulting Manager Cybersecurity**

Christophe de Boisset

**Consulting Manager Cybersecurity**

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

Absolute Software*
AC3*
Accenture*
ACESI Group
Acronis*
Actar (Peers Group)
ActioNet*
Adarma*
ADIT Group
Advens*
Agility Networks*
Airbus Protect*
AISI
Akamai*
Algosecure
Alice&Bob.Company*
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
AntemetA
Apixit
Appdome
Apura Cyber Intelligence S/A
Arcon
Asper*
AT&T Cybersecurity*
Atos*
Avatier*
Aveniq*
Avertium*
Axians*
Axur
Azion
BAYOOSOFT*
BDO
Bechtle*
Berghem*
Beta Systems*
BeyondTrust*
BIP
Bitdefender*
BlackBerry*
Blaze Information Security*
BluePex*
BlueVoyant*
Brainloop*
Bravo GRC
Bridewell
Broadcom
BT*
CANCOM*
Capgemini*
Cato Networks*
CDW*
Century Data
CGI*
ChapsVision CyberGov
Check Point Software*

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

Cipher*
Cirion*
Cisco*
Citrix
Claranet*
Clavis*
ClearSale
Cloud Target
Cloudflare*
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Consulteer InCyber
Controlware*
CoSoSys (Netwrix)*
Critical Start*
Cross Identity*
CrowdStrike*
CTM*
CyberArk*
CyberCX*
Cybereason*
CyberProof*
Cyberprotect
CyberSecOp*
Cybersolutions
Cyderes*
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Delfia
Delinea
Deloitte*
Deutsche Telekom
Devensys
Devoteam*
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust
Edge UOL*
Embratel
EmpowerID*
Ensono
Entrust*
Ergon Informatik*
Ericom Software*
e-Safer
ESET*
E-TRUST*
Eviden*
EY*
FastHelp*
Fidelis Cybersecurity*
FireEye
Fischer Identity*

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Framatome Cybersecurity
Fujitsu*
FusionAuth*
Future Segurança da Informação
GBS*
GC Security*
Genetec
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec*
Hakai Offensive Security*
Happiest Minds*
HCLTech*
Headmind Partners*
HiSolutions*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iboss*
iC Consult*
Ilex IAM Platform*
Imperva
Imprivata*
IMS Networks
IN Groupe*
indevis*
InfoGuard*
Infosys*
Integrity360*
Interop
Intrinsec*
ISH Tecnologia*
ISPIN*
IT.eam*
It4us
Italtel*
ITC Secure*
I-Tracing
Itrust (Free Pro)*
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*
Kryptus*

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

Kudelski Security*
Kyndryl*
Lastpass*
Leidos*
Lexfo*
Logical IT
Logicalis*
Lookout*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Mandiant
Materna Radar*
Matrix42*
McAfee
Metsys*
Micro Focus
Microland*
Microsoft*
Modulo Security Solutions
Mphasis*
MTF*
NAVA*
NBS System
NCC Group*
NEC*
Neosoft
NetSecurity
Netskope*
Network Secure
Neverhack*
Nevis*
Nextios
Nok Nok Labs*
Nomios*
Novared
Noventiq
Npo Sistemas
NRI ANZ*
NTSEC
NTT DATA*
NTT Ltd.
NXO*
NYBBLE
OEDIV
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Optiv*
Oracle*
Orange Cyberdefense*
OST Tecnologia
P1 SECURITY
Palo Alto Networks*
pco*
Peers

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

| | | | |
|---|---|---|---|
| Performanta* | Rapid7* | SEC4U | Servix |
| Perimeter 81* | RCZ | SecureAuth* | Seti |
| Persistent Systems* | Red river | Secureway | SFR* |
| Ping Identity* | Redbelt | Secureworks* | Shearwater Group* |
| Presidio* | Redscan* | Securiti | Sigma |
| Pride Security* | Reply | SecurityHQ* | Sigma Telecom |
| Proficio* | RSA Security* | SecurityScorecard | Skyhigh Security* |
| Proofpoint* | Safeway | SEK (Security Ecossystem Knowledge)* | SLK Software* |
| Protega Managed Cybersecurity | Safeweb | Sekuro* | SNS Security |
| Protiviti/ICTS | SailPoint* | senhasegura* | Softcat* |
| PurpleSec* | SAP* | SenseOn* | SolarWinds* |
| PwC* | Saviynt* | SentinelOne* | Solor |
| Quorum Cyber* | SCC* | Seqrite | SONDA* |
| Rackspace Technology* | Scunna* | Sequretek | Sophos* |
| Radware | SCUTUM | Service IT* | Sopra Steria* |

## Eingeladene Unternehmen

**Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.**

*In der vorherigen Ausgabe bewertet

Spie ICS*
Splunk
Squad*
Stefanini*
suresecure*
Swisscom*
Symantec
Synetis*
Syntax*
Sysinterga
Systancia*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
TEHTRIS*
Telefonica Tech*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
TIVIT*
Trellix*
Trend Micro*
Trustwave*
T-Systems*
UMB*
Under Protection
Unisys*
United Security Providers*
ValueLabs*
Varonis*
Vectra*
Venturus
Verizon Business*
Versa Networks*
Vigilant
VMware Carbon Black
Vortex Security*
Vortex TI
WALLIX*
WatchGuard
Wavestone*
Wipro*
Xmco
YSSY*
Zensar Technologies*
Zscaler*

## ISG Provider Lens™

Die ISG Provider Lens™ Quadranten-Reports bieten Bewertungen von Dienstleistern und kombinieren als einzige Studien dieser Art datengestützte Forschung und Marktanalysen mit praktischen Erfahrungen und Beobachtungen, gestützt auf das globale ISGBeraterteam. Unternehmen erhalten eine Fülle detaillierter Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Sourcing- Partner helfen; die ISG-Berater wiederum nutzen die Berichte, um ihre Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG abzugeben. Die Studien decken derzeit Provider mit Angeboten in mehreren Regionen weltweit ab. Weitere Informationen über die ISG Provider Lens Studien finden Sie auf dieser Webseite.

## ISG Research™

Das ISG Research™ Angebot umfasst Research- Subskriptionsservices, Beratungs - Services und Executive Event Services mit Fokus auf Markttrends und disruptive Technologien im Unternehmensumfeld. ISG Research™ zeigt Unternehmen auf, wie sie ein schnelleres Wachstum und einen höheren Mehrwert erzielen können.

ISG bietet Recherchen speziell über Anbieter für Bundes-, Landes- und kommunale Behörden (einschließlich Landkreise und Städte) sowie für Hochschuleinrichtungen an.
Besuchen Sie : Öffentlicher Sektor.

Weitere Informationen zu den ISG Research™ Subskriptions-Services sind unter contact@isg-one.com, Tel.+49 (0) 561 50697524 oder auf unserer Website unter research.isg-one.com.

## ISG

ISG (Information Services Group) (Nasdaq: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 900 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 digitalin Transformation, inclusive AI und 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 1.600 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 Branchenund Technologie-Expertise sowie weltweit führende Marktforschungsund Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren.

Weitere Informationen unter isg-one.com.

ISG Provider Lens™

**JANUAR, 2025**

# BROSCHÜRE: CYBERSECURITY – SERVICES AND SOLUTIONS