ISG Provider Lens®

Cybersecurity — Services and Solutions

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

BROSCHÜRE | JANUAR 2026 | AUSTRALIEN, BRASILIEN, FRANKREICH, DEUTSCHLAND, SCHWEIZ, U.K., USA UND USA ÖFFENTLICHER SEKTOR

Inhaltsverzeichnis

Einleitung

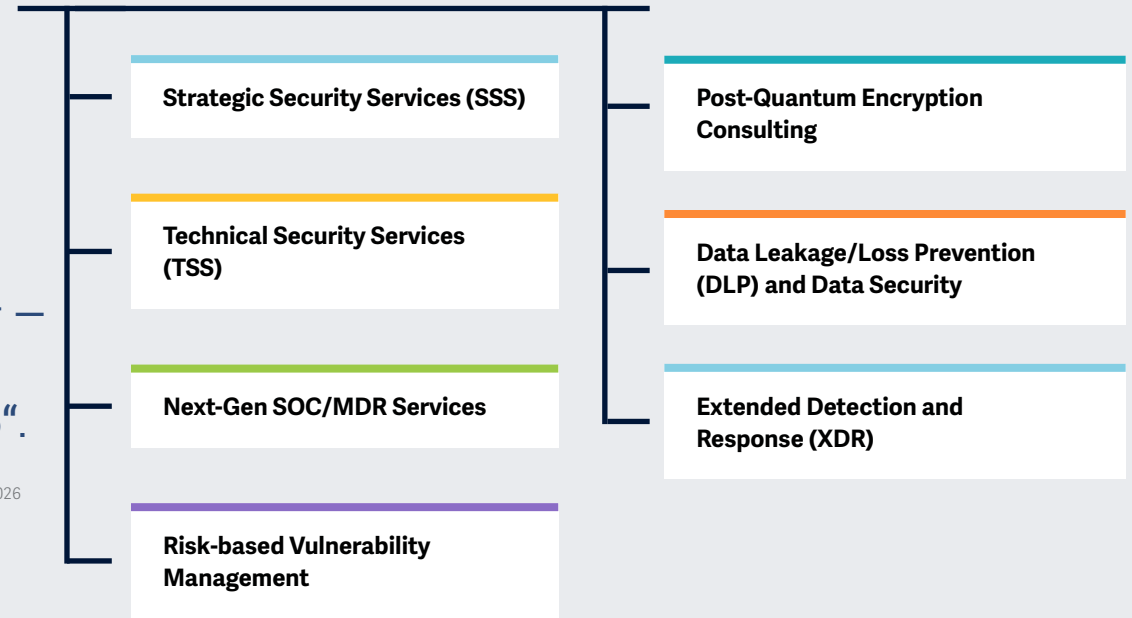
Für das Jahr 2026 ist im Bereich der Cybersicherheit mit immer komplexeren Bedrohungen, wachsenden regulatorischen Anforderungen und einer raschen Verlagerung hin zu intelligenzgesteuerten Verteidigungsmodellen zu rechnen. Unternehmen aller Branchen stehen unter dem Druck, ihre zunehmend verteilten Architekturen zu sichern, sensible Daten in hybriden Umgebungen zu schützen und auf die zunehmenden KI-gestützten Angriffe zu reagieren. Mittlerweile verlangen Geschäftsführungen und Aufsichtsbehörden nachweisbare Cyberresilienz sowie überprüfbare Kontrolleffektivität und ebnen damit den Weg für Sicherheitsprogramme als Teil der digitalen Transformations-Agenda.

Vor diesem Hintergrund kommt es im Markt zu einer Umstrukturierung in klar definierte Kompetenzbereiche. Technical Security Services (TSS) gewährleisten die Integrität von Konfigurationen, sichere Implementierungen und kontinuierliches Härten; Strategic Security Services (SSS) gewinnen wiederum zunehmend an Bedeutung, da Führungskräfte einer auf Governance, Risiken und Architektur abgestimmten Cybersicherheit eine hohe Priorität einräumen.

SOCs der nächsten Generation und Managed Detection & Response (MDR) Services sind im Zuge der Nachfrage nach 24/7-Bedrohungsüberwachung, KI-gestützten Analysen und ergebnisorientierten Reaktionsmodellen ebenfalls auf dem Vormarsch. Darüber hinaus stärkt das risikobasierte Schwachstellenmanagement die präventive Sicherheit; Schwachstellen werden entsprechend des Geschäftskontextes und der Erkenntnisse über Angriffspfade priorisiert. Zudem kommen Beratungsangebote zur Post-Quantum-Verschlüsselung auf den Markt, denn Unternehmen machen sich daran, Kryptografie-Inventare und Übergangsstrategien zur Sicherung der langfristigen Vertraulichkeit von Daten aufzusetzen.

Diese IPL-Studie deckt unter anderem die genannten Themenbereiche ab und bietet einen umfassenden Überblick darüber, wie sich Anbieter in einem von Geschwindigkeit, künstlicher Intelligenz und Resilienz geprägten Umfeld differenzieren.

Schwerpunkt-bereiche der Studie „Cybersecurity — Services und Solutions 2026“.



Vereinfachte Darstellung. Quelle: ISG 2026

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 Portfolioattraktivität
- Fokus auf verschiedene Märkte: Australien, Brasilien, Frankreich, Deutschland, Schweiz. Großbritannien, die USA und den US-amerikanischen Public Sector
- Länderspezifische Besonderheiten: Post-Quantum Encryption Consulting für Deutschland und die USA, XDR und Risk-Based Vulnerability Management für Brasilien sowie DLP für Deutschland.

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

Definition

Im Rahmen dieses Quadranten werden Dienstleister evaluiert, die beratungsgestützte Cybersicherheitsdienste mit Schwerpunkt auf Strategie, Governance, Risikomanagement und organisatorischer Transformation für IT- und OT-Umgebungen anbieten. Sie bewerten den Sicherheits-Reifegrad, quantifizieren die Risiken, definieren die angestrebten Betriebsmodelle und entwickeln Cybersicherheitsstrategien, -richtlinien und -pläne im Einklang mit den Unternehmenszielen und den gesetzlichen Anforderungen. Ihre Angebote umfassen Audits, Bewertungen, Programme zur Sensibilisierung für Sicherheitsfragen, die Planung der Geschäftskontinuität, theoretische Übungen und Beratung bei der Technologieauswahl. Diese Anbieter beschäftigen zudem erfahrene Berater, die Unternehmen bei der Programmgestaltung, der Verbesserung der Governance und der Entwicklung von Fähigkeiten begleiten, einschließlich virtueller Chief Information Security Officer (vCISO) Modelle für die kontinuierliche oder bedarfsorientierte strategische Führung. Im Gegensatz zu TSS, bei denen die praxisorientierte Integration und das Engineering im Vordergrund stehen, konzentrieren sich SSS-Anbieter auf Beratungsergebnisse und nicht auf die operative Überwachung oder die Umsetzung proprietärer Produkte.

Auswahlkriterien

1. **Anbieterunabhängige Sicherheitsberatung** in den Bereichen Reifegradbewertung, Strategieentwicklung, Policy Design, Governance-Modelle und Roadmap-Erstellung
2. Nachgewiesene Fähigkeiten in strategischen Bereichen wie Risikoquantifizierung, regulatorische Bereitschaft, Auswahl von Anbietern, Planung der Geschäftskontinuität und Beratung in Bezug auf Cyberrisiken im umfassenderen Sinne
3. **Anwendung anerkannter Frameworks** und Einhaltung von Standards (wie ISO 27000, NIST CSF, CIS Controls) bei der Steuerung von Unternehmensprogrammen
4. **Erbringung von mindestens einer der oben genannten** strategischen Sicherheitsdienstleistungen in der Zielregion durch **qualifizierte und zertifizierte** Berater
5. Vorlage **dokumentierter Nachweise über Projekte** , die die Sicherheitslage, die Governance-Strukturen, die regulatorische Bereitschaft oder die risikobasierte Entscheidungsfindung der Kunden verbessert haben
6. Bereitstellung von **strukturierten Beratungsmethoden**, Templates oder Playbooks für Bewertungen, die strategische Planung oder die organisatorische Transformation
7. Tätigkeit als **beratungsorientierter Dienstleister** und nicht als Produktanbieter, aber unter Nutzung proprietärer Frameworks oder Tools zur Unterstützung der Beratungsleistung
8. **Kein ausschließlicher Fokus** auf proprietäre Produkte

Definition

Im Rahmen dieses Quadranten werden Dienstleister bewertet, die IT- und OT-Sicherheitstechnologien in Multivendor-Umgebungen entwickeln, integrieren, implementieren und modernisieren. Ihre Leistungen umfassen die Bereitstellung und Konfiguration von Sicherheitslösungen für Identity & Access Management, Cloud und Rechenzentren, SASE/SSE, Endpoints, Netzwerke, OT und industrielle Steuersysteme (ICS) sowie verwandte Bereiche. Die Anbieter nutzen Referenzarchitekturen, Automatisierungs-Frameworks und proprietäre Beschleuniger für technikgetriebene Transformationen, die die Implementierung effizienter gestalten und die Kontrolleffektivität verbessern. Sie unterhalten enge Partnerschaften mit Sicherheitsanbietern, verfügen über spezielle Zertifizierungen und unterstützen Lebenszyklusaufgaben wie Härtung, Tuning, Patching und Geräteverwaltung. Im Gegensatz zu SSS, die sich auf Beratung und Governance fokussieren, legen TSS-Anbieter den Schwerpunkt auf die praxisorientierte technische Umsetzung. Sie bieten keine SOC-basierte Überwachung oder MDR-Abläufe an, erbringen aber manchmal traditionelle Managed Security Services.

Auswahlkriterien

1. Nachgewiesene **Erfahrung in der Entwicklung, Integration und Implementierung** von IT- und/oder OT-Sicherheitstechnologien, gestützt auf Zertifizierungen mehrerer Anbieter und OEM-Partnerschaften
2. Einsatz von **Beschleunigern, proprietären Toolsets oder Referenzarchitekturen**, die die Qualität der Implementierung, die Interoperabilität und die Zeit bis zur Wertschöpfung verbessern
3. **Zertifizierte Ingenieure und Architekten** mit Erfahrung in der Konfiguration, Anpassung und Optimierung von Sicherheitslösungen für Cloud-, Netzwerk-, Endpoint- und OT-Umgebungen
4. **Nachweis eines strukturierten, methodengesteuerten Ansatzes** für die Bewertung, Auswahl und Integration von Sicherheitstechnologien, der den Kundenanforderungen, Risikoprofilen und architektonischen Einschränkungen entspricht
5. **Lifecycle Engineering Services** wie Konfigurationsmanagement, Policy Tuning, Patching, Control Hardening und Technologie-Modernisierung
6. Präsentation von dokumentierten **Fallstudien** , die den erfolgreichen Einsatz von Sicherheitstechnologien oder deren Transformation in der Zielregion belegen
7. Tätigkeit als **dienstleistungsorientierter Integrator** und nicht als eigenständiger ISV, aber unter Einbeziehung proprietärer Beschleuniger oder intern entwickelter Tools zur Unterstützung der Dienstleistungserbringung
8. **Kein ausschließlicher Fokus** auf proprietäre Produkte

Definition

Im Rahmen dieses Quadranten werden Dienstleister bewertet, die kontinuierliche Überwachungs- und MDR-Dienste über SOCs offerieren. Ihre Angebote umfassen den gesamten Lebenszyklus eines Vorfalls, u.a. Erkennung, Triage, Untersuchung, Eindämmung und koordinierte Abhilfe. Die Anbieter integrieren und betreiben moderne Sicherheitstechnologien, setzen Bedrohungsdaten und fortschrittliche Analysen ein und bieten menschengesteuertes und automatisiertes Threat Hunting für mehr Resilienz im Unternehmen. Next-Gen SOC/MDR Services kombinieren verwaltete Sicherheitsabläufe mit innovativen KI-gesteuerten Analysen, autonomer Triage und Security Orchestration, Automation & Response (SOAR)-basierter Orchestrierung, um die Reaktionszeiten zu verkürzen und die Sichtbarkeit von Bedrohungen in IT- und OT-Umgebungen zu verbessern. Sie unterstützen gemeinsam verwaltete Modelle und fokussieren sich nicht auf strategische Beratung oder Technologieimplementierungen, was unter SSS bzw. TSS angesiedelt ist.

Auswahlkriterien

1. **24/7-Überwachungs-, Detection- und Response-Dienste** über **eigene SOCs**, die IT- und/oder OT-Umgebungen abdecken
2. **MDR-spezifische Funktionen**, u.a. Verhaltensanalyse, Integration von Bedrohungsdaten auf Basis eines Large Language Models (LLM), menschengesteuertes und automatisches Threat Hunting sowie Advanced Detection Engineering
3. **Betrieb und Verwaltung** von Security Information & Event Management (SIEM), SOAR, Endpoint Detection & Response (EDR), Network Detection & Response (NDR) und anderen relevanten Sicherheitstechnologien, gestützt auf OEM-Akkreditierungen
4. Nachweis eines strukturierten **Ansatzes für Incident Response**, einschließlich Triage, Untersuchung, Eindämmung, Koordination von Abhilfemaßnahmen und Verbesserung nach dem Vorfall
5. Einsatz von **KI-gesteuerten** Analysen, autonomen Triage-Agenten und SOAR-Workflows für eine schnellere Erkennung und kürzere mittlere Reaktionszeit (MTTR)
6. **Gemeinsam** mit Unternehmensteams **verwaltete Servicemodelle (co-managed)**, die shared Visibility, Zusammenarbeit mit Analysten und gemeinsame Response-Prozesse ermöglichen
7. **Referenzfälle**, die messbare Verbesserungen bei der Erkennungsabdeckung, der Reaktionseffizienz oder der operativen Resilienz in der Zielregion aufzeigen
8. **Kein ausschließlicher Fokus** auf proprietäre Produkte, sondern Management- und Betriebsleistungen für Best-of-Breed Security Tools

Definition

Im Rahmen dieses Quadranten werden Dienstleister bewertet, die kontinuierliche, risikobasierte Schwachstellenmanagementdienste für IT-, Cloud-, Anwendungs- und digitale Infrastrukturumgebungen anbieten. Diese Anbieter identifizieren, bewerten und priorisieren Schwachstellen auf Basis der Ausnutzbarkeit, der Gefährdung und der geschäftlichen Auswirkungen und nicht lediglich auf Grundlage des Schweregrads. Ihre Dienste kombinieren automatisierte Erkennung, Penetrationstests, Anwendungssicherheitstests und kontextbezogene Risikoanalysen, um sich schnell entwickelnde, u.a. durch GenAI beschleunigte Angriffstechniken und die zunehmenden Ransomware-Aktivitäten adressieren zu können. Das risikobasierte Schwachstellenmanagement ermöglicht einen kontinuierlichen Einblick in internetbasierte und interne Ressourcen sowie die Priorisierung von Abhilfemaßnahmen, die sich an den tatsächlichen Angriffspfaden und der Geschäftskritikalität orientieren, und hilft Unternehmen, das Risiko in sich schnell verändernden Technologielandschaften durch kontinuierliche Beobachtung, Bewertung, erneute Tests und Risikokalibrierung zu verringern.

Auswahlkriterien

1. Verfügbarkeit von **kontinuierlichen Schwachstellenbewertungsdiensten**, die Erkenntnisse auf Basis der Ausnutzbarkeit, Gefährdung und Geschäftsauswirkungen und nicht nur anhand von statischen Schweregradmetriken priorisieren
2. **Testdienste** für Web- und Mobilanwendungen, APIs, interne Netzwerke, Cloud-Umgebungen (Container, Kubernetes/K8S und Docker), Geldautomaten, User Risk Assessments (URAs), IoT und andere exponierte Assets
3. Anwendung **anerkannter Testmethoden** wie Penetrationstests, dynamische Anwendungssicherheitstests (DAST), statische Anwendungssicherheitstests (SAST), interaktive Anwendungssicherheitstests (IAST) und verwandte Techniken, die automatisierte Tools und manuelle Expertenvalidierung kombinieren
4. Anpassen der **Ergebnisse und des Reportings zu Sicherheitslücken** an relevante Standards und Frameworks wie ISO 27001, NIST SP 800-53, PCI DSS, SOC 2 sowie geltende regulatorische oder branchenspezifische Anforderungen
5. **Wiederholungstests, Nachverfolgung von Abhilfemaßnahmen und kontinuierliche Risikoneubewertung**, um Änderungen bezüglich Gefährdung, Bedrohungsdaten und Fortschritten bei der Schadensbegrenzung berücksichtigen zu können
6. Einsatz von **Sicherheitsexperten**, z.B. Ethical Hackers (CEHs), OSCPs (Offensive Security Certified Professionals bzw. zertifizierte Experten für offensive Sicherheit) und CISSPs (Information Systems Security Professionals bzw. Experten für die Sicherheit von Informationssystemen) sowie Experten mit CompTIA PenTest+- oder GIAC-Zertifizierungen für eine einheitliche Servicequalität

Definition

Im Rahmen dieses Quadranten werden beratungsorientierte Dienstleister bewertet, die Unternehmen bei der Vorbereitung und Durchführung der kryptografischen Umstellung unterstützen, die erforderlich ist, um die mit dem Quantencomputing verbundenen Risiken zu mindern. Diese Anbieter bewerten kryptografische Abhängigkeiten über IT-, OT-, IoT- und digitale Lieferkettenumgebungen hinweg, u.a. im Bereich des Cryptographic Inventory Managements, zur Identifizierung von Algorithmen, die durch Quantencomputing gefährdet sind, und zur Einschätzung der Gefährdung durch „Harvest Now, Decrypt Later"-Bedrohungen. Sie entwickeln risikobasierte Strategien für die Post-Quantum-Kryptografie (PQC), entwerfen Migrations- und hybride kryptografische Roadmaps und beraten bei der Einführung neuer Post-Quantum-Standards, die auf die Vorgaben des National Institute of Standards & Technology (NIST), des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und anderer Aufsichtsbehörden abgestimmt sind. Die PQC-Beratung befasst sich mit den Auswirkungen auf die Schlüsselverwaltung, Identitätssysteme, die Kommunikation, Anwendungen sowie Infrastrukturarchitekturen und ermöglicht es Unternehmen, eine konforme, skalierbare und zukunftssichere kryptografische Transformationen zu planen.

Auswahlkriterien

1. Durchführung von **kryptografischen und Quanten-Risikobewertungen**, u.a. bezüglich der Inventarisierung von kryptografischen Assets, Algorithmen und Schlüsselnutzungen in IT-, OT-, IoT-, Cloud-, Netzwerk- und Anwendungsumgebungen
2. Nachgewiesene **Beratungskompetenz bei der Entwicklung von PQC-Strategien**, u.a. schrittweise Migrationspläne, hybride Kryptografieplanung und Abhängigkeitsanalysen
3. Verfügbarkeit von Beratungsdiensten im Einklang mit **neuen Standards und Richtlinien** wie NIST PQC, BSI TR-02102, European Telecommunications Standards Institute (ETSI) und relevanten ISO/IEC-Vorgaben
4. Bewertung der **Auswirkungen hinsichtlich Schlüsselmanagement**, Public Key Infrastructure (PKI), Identitäty- & Access-Systemen, sicherer Kommunikation und Anwendungsarchitekturen
5. Nachgewiesene **PQC-bezogene Kundenmandate**, Piloten, Simulationen oder Proofs of Concepts, die sich mit quantenbasierter Risikominderung befassen
6. Herstellerneutrale Beratungsdienste bei nachgewiesenem Know-how hinsichtlich relevanter Technologie-Ökosysteme und kryptografischer Implementierungen
7. **Unterstützung bei der Einhaltung** staatlicher Vorgaben und Erfüllung der Ziele von branchenspezifischen oder nationalen kryptografischen Übergangsinitiativen

Definition

Im Rahmen dieses Quadranten werden unabhängige Softwareanbieter (ISVs) bewertet, die proprietäre DLP- und Datensicherheitslösungen entwickeln, welche als On-Premises-Software, Cloud-Plattformen oder SaaS verfügbar sind. Diese Produkte ermöglichen die Erkennung, Klassifizierung und Überwachung sensibler Daten auf Endgeräten, in Netzwerken, Cloud-Diensten und Speichersystemen und verhindern anhand von richtlinienbasierten Kontrollen den unbefugten Zugriff auf bzw. die Exfiltration von Daten. Moderne DLP-Technologien integrieren zunehmend Gerätehärtung, Anwendungskontrollen und Verhaltensanalysen, um Datenmissbrauch an den Endpoints zu verhindern und Richtlinien auch in Offline- oder nicht verwalteten Umgebungen durchzusetzen. Sie bieten zentralisierte Governance-, Reporting- und Compliance-Unterstützung zum Schutz strukturierter und unstrukturierter Daten während ihres gesamten Lebenszyklus. In einer verteilten IT-Landschaft mit erhöhtem Risiko von Sicherheitsverletzungen durch interne Mitarbeiter und Datenabflüsse bilden diese Lösungen die zentrale Sicherheitsmaßnahme zum Schutz kritischer Informationsbestände und zur Gewährleistung konsistenter Datenverarbeitungspraktiken.

Auswahlkriterien

1. Bereitstellung eines **proprietären DLP- oder Datensicherheitsproduktes** (keine eingebetteten DLP-Engines von Drittanbietern)
2. **Unterstützung von Kernarchitekturen** wie Endpoint-, Netzwerk-, Cloud- und Speicherumgebungen
3. **Erkennung, Klassifizierung und Schutz** von strukturierten und unstrukturierten Daten im Ruhezustand und bei der Übertragung
4. **Zentralisierte Verwaltungsfunktionen**, u.a. Richtlinienkontrolle, Reporting und Konfiguration
5. Datenerkennung, Echtzeitüberwachung und richtlinienbasierte Durchsetzungsmaßnahmen
6. **Nachgewiesene** Implementierungen auf Enterprise-Niveau und dokumentierte Kundenakzeptanz

Definition

Im Rahmen dieses Quadranten werden ISVs bewertet, die proprietäre XDR-Plattformen entwickeln, welche Telemetrie-, Analyse- und Reaktionsfunktionen für Endgeräte, Netzwerke, Identitäten, Cloud-Workloads und Anwendungen integrieren. Diese Lösungen korrelieren und kontextualisieren Daten aus verschiedenen Sicherheitskontrollen und verbessern so die Erkennungsgenauigkeit, verringern die Alarmmüdigkeit und steigern die betriebliche Effizienz. Moderne XDR-Plattformen vereinheitlichen die Sichtbarkeit von Bedrohungen in einer einzigen Schnittstelle, führen Verhaltens- und ML-Analysen durch und automatisieren Reaktionsmaßnahmen auf Basis des Schweregrads und des Geschäftskontexts. Es handelt sich um cloud-basierte oder hybride Architekturen mit einer definierten Sensorschicht im Frontend und einer Analyse- und Orchestrierungs-Engine im Backend. Unternehmen wollen Tools konsolidieren und für eine bessere Erkennung sorgen; XDR dient dabei als strategische Grundlage für eine koordinierte, erkenntnisgesteuerte Verteidigung.

Auswahlkriterien

1. Bereitstellung einer **proprietären XDR-Plattform** (keine Abhängigkeit von XDR-Engines von Drittanbietern)
2. **Definiertes XDR-Frontend** (Integration mehrerer Sensoren) und XDR-Backend (Analytik, Korrelation und Orchestrierung)
3. **Integration von mindestens drei** nativen oder eng gekoppelten Sensoren, z.B. EDR/Endpoint Protection Platform (EPP), NDR, Identity, E-Mail, mobiler oder Cloud-Workload-Schutz
4. **Einheitliche Sichtbarkeit** über Endgeräte, Netzwerke und Cloud-Umgebungen hinweg
5. Nachgewiesene **Fähigkeit, komplexe Bedrohungen** wie Advanced Persistent Threats (APTs), Ransomware und hochentwickelte Malware **zu erkennen und zu blockieren**
6. **Nutzung von Threat Intelligence**, Verhaltensanalysen und Echtzeit-Telemetrie-Korrelationen
7. Verfügbarkeit **automatischer oder halbautomatischer** Reaktionsmaßnahmen mit messbarer Wirkung

Quadranten nach Regionen

Im Rahmen der ISG Provider Lens® Quadrantenstudie „Cybersecurity – Services und Solutions 2026“ werden die folgenden sieben Quadranten präsentiert.

Quadrant	Australien	Brasilien	Frankreich	Deutschland	Schweiz	UK	USA	USA Public Sector
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	Großkunden & Mittelstand	Großkunden & Mittelstand	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	Großkunden & Mittelstand	Großkunden & Mittelstand	✓
Next-Gen SOC/MDR Services	✓	Großkunden & Mittelstand	✓	Gesamtmarkt & Mittelstand	Gesamtmarkt & Großkunden & Mittelstand	Großkunden & Mittelstand	Großkunden & Mittelstand	✓
Risk-based Vulnerability Management		✓						
Post-Quantum Encryption Consulting				✓			✓	
Data Leakage/Loss Prevention (DLP) and Data Security				✓				
Extended Detection and Response (XDR)		✓						

Die Research-Phase umfasst die Befragung, Evaluierung, Analyse und Validierung und läuft von Januar bis Juni 2026. Die Ergebnisse werden den Medien im Juli 2026 vorgestellt.

Meilensteine	Beginn	Ende
Start der Umfrage	7. Januar 2026	
Umfrage-Phase	7. Januar 2026	13. Februar 2026
Webinar Call	12. Januar 2026	
Sneak Preview	Mai 2026	Juni 2026
Pressemitteilung & Veröffentlichung	Juli 2026	

Mit Klick auf diesen Link können Sie die **ISG Provider Lens® 2026** 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!

Kaufberatung

Buyers Guide ISG Software Research, ehemals „Ventana Research", bietet im Rahmen seiner „Buyers Guides" Markteinblicke auf Basis der Evaluierung und Einstufung von Technologieanbietern und Produkten. Die Ergebnisse werden aus der researchbasierten Analyse von Produkt- und Kundenerfahrungskategorien gewonnen, die Software-Anbieter und -Produkte bewerten, um eine fundierte Entscheidungsfindung und die Auswahlprozesse für Technologie zu erleichtern.

Im Zuge des Starts der Cybersecurity — Services and Solutions IPL-Studie möchten wir Sie auf damit zusammenhängende Research und Erkenntnisse aufmerksam zu machen, die ISG Research im Jahr 2026 veröffentlichen wird. Weitere Informationen finden sich im Buyers Guide Research-Zeitplan.

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 Lead 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 zusammenhängen. 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® 2026 – 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.

Studiensponsor:
Heiko Henkes

Leitende Analysten:
Frank Heuer, Bhuvaneshwari Mohan, Yash Jethani, Benoit Scheuber, Andrew Milroy und João Mauro

Forschungsanalyst en:
Monica K und Rafael Rigotti

Projektleiter:
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

Bhuvaneshwari Mohan

Lead Analyst – U.K., USA Öffentlicher Sektor

Yash Jethani

Lead Analyst – USA

Benoit Scheuber

Lead Analyst – Frankreich

Andrew Milroy

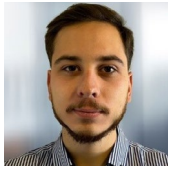
Lead Analyst – Australien

João Mauro

Lead Analyst – Brasilien

Monica K

Research Analyst



Rafael Rigotti

Research Analyst

Rajesh Chillappagari

Data Analyst

Laxmi Sahebrao Kadve

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.

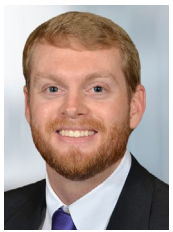
ISG-Berater für diese Studie

Doug Saylors

Partner, Lead ISG Cybersecurity

David Gordon

Director Cybersecurity



Jason Stading

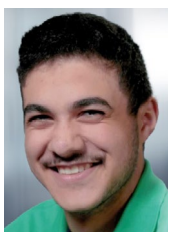
Director Cybersecurity

Brendan Prater

Principal Consultant Cybersecurity

Christophe deBoisset

Consulting Manager



Marco Ezzy

Consultant 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 ansprechen

*In der vorherigen Ausgabe bewertet

8com	AlmavivA*	Azion	Broadcom*
Absolute Software*	Almond*	BDO	BT*
AC3*	Alten*	Bechtle/Apixit*	CANCOM*
Accenture*	Amazon Web Services	Berghem	Capgemini*
Acronis*	Appdome	BeyondTrust	Capita*
Actar (Peers Group)	Apura Cyber Intelligence S/A	BIP	CDW*
ActioNet*	Arcon	Bitdefender	Century Data
Addvalue	Arctic Wolf Networks, Inc.	Blaze Information Security	CGI*
Advania	Asper*	Bluepex*	Check Point Software*
Advens*	Atos*	BlueVoyant*	CI&T*
Agility Networks*	Aveniq*	Brainloop*	Cipher*
Airbus Protect*	Avertium*	Bravo GRC	Cirion Technologies*
Aizoon*	Avivatec	Brennan IT*	Cisco*
Akamai Technologies	Axians*	Bricon	Citrix
All for One Group*	Axur	Bridewell*	Claranet*

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 ansprechen

*In der vorherigen Ausgabe bewertet

Claro empresas	Crowdstrike*	deepwatch, Inc.	ESET
Clavis*	CTM*	Defcon1	E-TRUST
ClearSale	CyberArk	Delfia	Expel, Inc
Cloud Target*	CyberProof*	Delinea	EY*
CloudFlare	CyberSecOp*	Deloitte*	FastHelp
Cognizant*	Cyderes*	Deutsche Telekom*	Fidelis Cybersecurity*
Combate a Fraude (Caf)	Cyera	Devoteam*	FireEye
Compugraf	Cynet Security Ltd.	Dfense	Forcepoint*
Computacenter*	Darktrace	DIGITALL*	ForgeRock (Ping Identity)
Consort Group*	Data#3*	DriveLock*	Formind*
Controlware*	Datacom*	DXC Technology*	Fortinet*
CoSoSys (Netwrix)*	DATAGROUP*	EcoTrust*	Fortra*
C-Risk	dataRain	Edge UOL*	Fujitsu*
Critical Start*	Data-Sec	e-Safer	Future Segurança da Informação

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 ansprechen

*In der vorherigen Ausgabe bewertet

GBS*
GC Security
Genetec
Genpact
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec
Hakai Offensive Security
Happiest Minds*
HCLTech*
Headmind Partners*
Hillstone Networks
HiSolutions*
Holiseum*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iC Consult*
ID Quantique
Imperva
inCloud Tecnologia
indevis*
Inetum*
InfoGuard*
Infosys*
Innova Solutions*
Insight*
Inspira*
Integrity360*
Interactive*
Interop
Intrinsec*
IonQ Quantum, Inc
IPTRUST*
ISH Tecnologia*
iSPIN*
iT.eam*
It4us
Italtel*
ITC Secure*
I-tracing
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*

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 ansprechen

*In der vorherigen Ausgabe bewertet

KRYPTUS*	Matrix42*	NEC	Novared
Kudelski Security*	McAfee	NetBr	Noventiq
Kyndryl*	McKinsey	Netconn	Npo Sistemas
L8 Group	Metsys*	Netfive	NRI*
Leidos*	Micro Focus	NetSecurity	NTSEC
LevelBlue (Trustwave)*	Microland*	Netskope*	NTT DATA*
Littlefish	Microsoft*	NetSurion	Nv7
Logical IT	Mimecast*	Network Secure	NXO*
Logicalis*	MindPoint Group LLC	Network Security Professionals, Inc.	Okta
LRQA Nettitude*	Minsait (Indra)	Neverhack*	One Identity
LTIMindtree*	Modulo Security Solutions*	Nextios	Ontinue (Open Systems)*
Lumen Technologies*	Mphasis*	Niji*	OpenText*
Macquarie Telecom Group*	MTF*	Nomios*	Oplium
ManageEngine*	NAVA*	Nova8	Optiv*
Materna*	NCC Group*	Novacoast	Optus*

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 ansprechen

*In der vorherigen Ausgabe bewertet

Opus Tech	Proficio*	Rackspace Technology*	SCC*
Oracle	Proofpoint*	Radware	Scunna*
Orange Cyberdefense*	Protega Managed Cybersecurity	Rapid7	SEC4U
ORBIT*	Protiviti/ICTS	RCZ	Secureway
Ornisec*	PsiQuantum Corp.	Redbelt	Secureworks*
OST Tecnologia	PurpleSec*	ReliaQuest	Securiti
Palo Alto Networks*	PwC*	Reply	Security First
pco*	qbeyond	Riedel Networks	SecurityHQ*
Peers	Qrypt	Rpost	SecurityScorecard
Performanta*	Quantinuum LLC	RSA Security	SEK (Security Ecossystem Knowledge)*
Persistent Systems*	Quantum Xchange	Safe Inc	Sempre IT
Post-Quantum	QuEra Computing, Inc.	Safeweb	Senhasegura
PQShield	QuintessenceLabs	SailPoint	Sequretek*
Presidio*	Quorum Cyber*	Samsung	Service IT*
PRIDE Security*	QuSecure	Scaltel	Servix

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 ansprechen

*In der vorherigen Ausgabe bewertet

Seti
SFR*
Sigma Telecom
Skaylink
Skyhigh Security*
SLK Software*
Smarttech247*
SNS Security*
Softcat PLC*
Solo Iron*
Solo Networking
Solor
Sonda*
Sophos*
Sopra Steria*
Splunk
Squad*
Stefanini*
Strati
suresecure*
SVA*
Swisscom*
Symantec
Synetis*
Syntax*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
Telefonica*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
Tidalcyber
TIVIT*
Trellix*
Trend Micro*
Trigent
T-Systems*
UMB*
Under Protection*
Unisys*
United Security Providers*
Varonis*
Vectra*
Venturus
Verizon Business*
Vigilant
VIVO
VMware Carbon Black
Vodafone
Vortex Security*
Vortex TI

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 ansprechen

*In der vorherigen Ausgabe bewertet

Vultus*
WatchGuard
Wavestone*
Wipro*
Wizard Group
WWT*
Xantaro*
XYPRO Technology Corp.
You IT
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 ISG Beraterteam. 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 erhältlich.

ISG

ISG (Nasdaq: III) ist ein globales, KI-orientiertes Technologieforschungs- und Beratungsunternehmen. Als vertrauenswürdiger Partner von mehr als 900 Kunden, darunter 75 der 100 weltweit führenden Unternehmen, ist ISG seit langem führend in der Beschaffung von Technologie- und Business-Services und nimmt inzwischen eine Spitzenstellung bei der KI-Nutzung ein; damit kann Organisationen zu operativer Exzellenz und schnellerem Wachstum verholfen werden.

Das 2006 gegründete Unternehmen ist bekannt für seine proprietären Marktdaten, sein fundiertes Wissen über Anbieter-Ökosysteme und die Kompetenz seiner 1.600 Experten weltweit, die gemeinsam Kunden dabei unterstützen, den Wert ihrer Technologieinvestitionen zu maximieren.

Weitere Informationen unter isg-one.com.

ISG Provider Lens®

JANUAR, 2026

BROSCHÜRE: CYBERSECURITY — SERVICES AND SOLUTIONS