ISG Provider Lens®

Cybersecurity – Services and Solutions

Eine Analyse des Cybersecurity-Marktes, die die Attraktivität der Portfolios und die Wettbewerbsstärke der Anbieter vergleicht

Customized report courtesy of:

QUADRANT REPORT | JUNI 2026 | DEUTSCHLAND

Inhaltsverzeichnis

Autor des Berichts: Frank Heuer

Technische Revolution, Verunsicherung und Fachkräftemangel treiben den deutschen Cybersecurity-Markt

Diese ISG Provider Lens®-Studie vergleicht Anbieter in Deutschland, die Cybersecurity-Dienstleistungen in den Bereichen Beratung (speziell auch zu Post-Quantum Encryption), technische Dienstleistungen und Next-Gen SOC/MDR Services offerieren, und zudem Anbieter von DLP-Produkten. Die Provider-Bewertung erstreckt sich über die Kundensegmente der Groß- und mittelständischen Unternehmen und untersucht, wie die Anbieter es Unternehmen ermöglichen, den Herausforderungen hinsichtlich Cyberkriminalität, Regulierung und Effizienzsteigerung zu begegnen.

Ein herausforderndes Marktumfeld

Deutschland befindet sich 2026 in einem wirtschaftlich und sicherheitspolitisch herausfordernden Umfeld. Geopolitische Spannungen, insbesondere rund um die Straße von Hormus, sorgen weiterhin für Unsicherheit auf den internationalen Märkten. Als eine der wichtigsten Handelsrouten für Öl und Gas beeinflusst die Region maßgeblich die Energiepreise. Bereits geringe Eskalationen können die Inflation erneut antreiben und die ohnehin fragile wirtschaftliche Entwicklung in Deutschland zusätzlich belasten.

Das ökonomische Umfeld bleibt angespannt. Nach Angaben des Statistischen Bundesamtes wuchs das Bruttoinlandsprodukt im ersten Quartal 2026 gegenüber dem Vorquartal lediglich um 0,3 Prozent. Viele Ökonomen sehen darin eher eine kurzfristige Stabilisierung als einen nachhaltigen Aufschwung. Unternehmen agieren bei Investitionen weiterhin vorsichtig, solange hohe Kosten und globale Unsicherheiten die Wettbewerbsfähigkeit beeinträchtigen.

Parallel dazu verschärft sich der Fachkräftemangel, insbesondere im Bereich Cybersecurity. Die Digitalisierung der Wirtschaft erhöht den Bedarf an spezialisierten IT- und Sicherheitsexperten erheblich. Gleichzeitig fehlen qualifizierte Fachkräfte,

Ein herausforderndes Marktumfeld fördert die Nachfrage nach externen Security-Dienstleistungen.

um Unternehmen und kritische Infrastrukturen wirksam gegen digitale Bedrohungen zu schützen. Diese Entwicklung gewinnt zusätzlich an Bedeutung, da regulatorische Anforderungen weiter zunehmen. Mit der europäischen NIS-2-Richtlinie verschärfen sich die Vorgaben für Cybersicherheit, Risikomanagement und Meldepflichten deutlich. Viele Unternehmen stehen dadurch unter erheblichem organisatorischem und finanziellem Druck.

Hinzu kommt ein signifikanter Anstieg der Cyberkriminalität. Kriminelle Gruppen nutzen zunehmend raffinierte und sich schnell wandelnde Angriffsmethoden, darunter KI-gestützte, automatisierte Phishing-Kampagnen, Ransomware und Angriffe auf Lieferketten. Die Bedrohungslage entwickelt sich dynamisch und erfordert kontinuierliche Investitionen in Technologie, Personal und Sicherheitsstrategien. Ein Beispiel ist die Bedrohung der Verschlüsselung vertraulicher Daten durch Quanten-Technologie. Obwohl diese Technologie erst in einigen Jahren marktgängig sein wird, sind Kriminelle bereits mit dem „Harvest Now, Decrypt Later"-Ansatz (HNDL) aktiv.

Managed Security Services und kostenoptimierte Lösungen sind gefragt

In der aktuellen IT-Budget-Studie von ISG zeigt sich, dass Datensicherheit und -schutz zu den Top-Prioritäten von Unternehmen in Westeuropa zählen. Für 96 Prozent der Befragten in westeuropäischen Unternehmen ist dies ein wichtiges, für 36 Prozent sogar ein kritisches Thema. Dies spiegelt zum einen die vorgehend beschriebene angespannte geopolitische Lage und zum anderen die gestiegene Bedrohung durch Cyberkriminalität wider. Während bis vor einigen Jahren vor allem Großunternehmen betroffen waren, sind inzwischen auch verstärkt mittelständische Firmen und kommunale Behörden in den Fokus von Cyberangriffen geraten, da in ihnen – häufig nicht unberechtigt – ein leichtes Ziel vermutet wird. Entsprechend wächst die Nachfrage nach Cybersecurity-Dienstleistungen in diesen Zielsegmenten besonders stark. Diese Kundengruppen erwarten kostenoptimierte und modulare, auf ihre Bedürfnisse zugeschnittene Angebote. Zudem wünschen sich Mittelständler unkomplizierte Lösungen, die es ihnen erlauben, sich auf ihr Kerngeschäft zu konzentrieren. Datensouveränität ist aufgrund der aktuellen geopolitischen Gegebenheiten ein immer häufiger erwartetes Merkmal von (Managed) Security Services; mittelständische Firmen bevorzugen schon seit längerer Zeit verstärkt Betrieb und Delivery aus Deutschland bzw. aus der EU.

Bedrohungen durch KI-basierte Angriffe gewinnen an Relevanz. Laut der aktuellen Cybersecurity-Marktstudie von ISG zählen diese in den nächsten zwei Jahren zu den Top-5-Cybersecurity-Herausforderungen von Unternehmen mit mindestens 1.000 Beschäftigten in Westeuropa – für 15 Prozent der Befragten ist dies sogar das wichtigste Problem. Die Veröffentlichungen von Anthropic AI hinsichtlich des Aufspürens von Software-Schwachstellen haben dieses Thema unter einem speziellen Aspekt in den Fokus öffentlicher Diskussionen gerückt. Gleichzeitig nennen 41 Prozent der Entscheider in westeuropäischen Unternehmen mangelnde KI-Kompetenzen als wichtige, zehn Prozent der Befragten sogar als wichtigste organisatorische Herausforderung. Der allgemeine Security-Fachkräftemangel ist für immerhin noch 28 Prozent eine organisatorische Top-5-Security Challenge; bei kleinen und mittelständischen Unternehmen dürfte dieser Wert noch höher liegen.

So ist es nicht verwunderlich, dass für fast die Hälfte der oben genannten Befragtengruppe kontinuierliche Threat Protection & Response, etwa durch ein Security Operations Center (SOC), eine Top-5-Priorität bei der Cybersecurity-Realisierung darstellt – für zwölf Prozent hat dieses Thema sogar die höchste Priorität. Dies spiegelt sich auch in dem für 2026 erwarteten Wachstum des deutschen Marktes für Managed Security Services von über 15 Prozent gegenüber dem Vorjahr wider.

Gleichwohl zeigt sich die verhaltene wirtschaftliche Gesamtlage auch in den Cybersecurity-Budgets. Für 18 Prozent der Befragten in Westeuropa sind Budgetlimitierungen eine Top-3-Herausforderung. Auch für Großunternehmen sind anpassbare und günstige Lösungen wichtig.

Vielfältige technische und organisatorische Optionen für die Wettbewerbsdifferenzierung

Im deutschen Markt sind besonders diejenigen Cybersecurity Provider im Vorteil, die optimal auf die Anforderungen der Anwenderunternehmen eingehen. Unter anderem profitieren Dienstleister, die ihren Kunden unkompliziert bruchlose End-to-End Services und die Integration von IT- und Security-Lösung aus einer Hand bieten können. Darüber hinaus können sich Berater mit tiefen Kenntnissen regulatorischer Regelungen profilieren. Dienstleister, die schon Beratung zu Post-Quantum Encryption anbieten, sind im Vorteil in Kundensegmenten, deren Unternehmensvermögen stark auf digitalen Assets basieren, wie zum Beispiel Banken und Versicherungen.

Im Markt der Technical Security Services sind insbesondere Dienstleister gefragt, die ein breites Leistungsspektrum an Services aus einer Hand bieten können, da IT-Security-Projekte häufig anspruchsvoll und vielfältig angelegt sind.

Die immer komplexeren Cyberattacken fördern insbesondere auch die Nachfrage nach Security Operations Centers (SOCs) sowie Managed Detection & Response (MDR) Services. Der Mangel an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen machen diese Dienstleistungen für deutsche Unternehmen noch interessanter.

Dabei werden Anbieter bevorzugt, die SOCs mit deutschem oder EU-Standort betreiben, da immer mehr Interessenten solche SOCs aufgrund des wichtiger gewordenen Datenschutzaspektes (digitale Souveränität) zu schätzen wissen. Eine hohe Innovationskraft ist wichtig, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Um der Cyberbedrohungen Herr zu werden, setzen Managed Security Services Provider vermehrt Automatisierung und künstliche Intelligenz ein. Ideal ist eine Kombination der maschinellen Effizienz mit umfassender menschlicher Expertise. Ein wichtiger Wettbewerbsfaktor ist aktuellste Threat Intelligence, um möglichst direkt auf Bedrohungen reagieren zu können. Hierbei sind besonders die Anbieter von SOC/MDR-Dienstleistungen im Vorteil, die zugleich auch Netzbetreiber sind, da sie unmittelbarer als andere Netznutzer Bedrohungen aus dem Netz erkennen (Threat Intelligence).

Im Bereich der DLP-Produkte werden vermehrt Anbieter geschätzt, die eine „No-Backdoor"-Garantie offerieren, mit der gewährleistet wird, dass Dritte keinen heimlichen Zugang erhalten können. Ferner empfehlen sich DLP-Produkte, die durch einen hohen Automatisierungsgrad für die Entlastung der IT-Mitarbeiter sorgen. Die zeitnahe Reaktion auf Sicherheitsvorfälle mit Hilfe von definierten Prozessen für die Untersuchung und Beseitigung der Auswirkungen ist ein Differenzierungsmerkmal. Auch fertige Richtlinienvorlagen, die den Regeln der EU-Datenschutz-Grundverordnung entsprechen, werden von Anwenderunternehmen begrüßt.

Im deutschen Cybersecurity-Markt sind Anbieter speziell dann erfolgreich, wenn sie einen ausgewogenen Zielgruppenmix adressieren. Dabei ist besonders die Fähigkeit zu nennen, sowohl die Anforderungen der Großkunden als auch die Bedürfnisse von Mittelständlern adressieren zu können. Damit können die betreffenden Provider sowohl von den umfangreichen Budgets der großen Klienten als auch von der dynamisch wachsenden Nachfrage der mittelgroßen Firmen profitieren.

Ausblick: Herausforderungen und Chancen

Die Cyber-Bedrohungslage in Deutschland wird sich weiter verschärfen; dazu tragen (missbräuchlich genutzte) Technologien und der Fachkräftemangel bei. Daraus ergeben sich Herausforderungen für die Anwenderunternehmen, aber auch Chancen für die Anbieter von Cybersecurity-Lösungen.

In den kommenden zwei Jahren werden KI-gestützte Cyberangriffe deutlich professioneller und schwerer erkennbar. Künstliche Intelligenz ermöglicht es Angreifern, hochpersonalisierte Phishing-Mails, realistische Deepfakes und automatisierte Social-Engineering-Attacken in großem Maßstab zu erstellen. Gleichzeitig werden Schadprogramme zunehmend lernfähig und können Sicherheitsmechanismen dynamisch umgehen. Auch die Geschwindigkeit von Angriffen nimmt zu, da KI Schwachstellen

automatisiert identifiziert und ausnutzt. Unternehmen stehen dadurch vor einer wachsenden Herausforderung: Klassische Sicherheitskonzepte reichen künftig nicht mehr aus. Um mit der zunehmenden Dynamik und Komplexität moderner Cyberbedrohungen Schritt halten zu können, sind KI-basierte Verteidigungssysteme, schnelle Reaktionsprozesse sowie gut geschulte Mitarbeiter entscheidend.

Gleichzeitig wird der akute Fachkräftemangel im Cybersecurity-Bereich auf absehbare Zeit nicht an Bedeutung verlieren, auch wenn künstliche Intelligenz immer mehr Aufgaben übernehmen wird. Mittelgroße Unternehmen bleiben davon besonders betroffen. Neben den Mittelständlern werden voraussichtlich auch (Kommunal-) Verwaltungen weiterhin verstärkt in das Visier von Cyberkriminellen geraten. So wird die Nachfrage dieser Zielgruppen nach externen Dienstleistungen, insbesondere SOC-/MDR-Diensten, weiter überdurchschnittlich steigen. Aufgrund der auch in der nächsten Zukunft zu erwartenden geopolitischen Spannungen werden digital souveräne Lösungen eine hohe Präferenz genießen.

Immer akuter wird in den kommenden Jahren die Gefährdung der Datenverschlüsselung durch Quanten-Computer. Der „Q-Day" rückt näher; es wird immer gefährlicher, sich nicht auf die Bedrohungen durch die neue Technologie einzustellen, da der „Harvest Now, Decrypt Later"-Ansatz mit jedem Tag lohnender wird. Rechtzeitige Beratung und Maßnahmen sind empfehlenswert.

Für die nächste Zukunft werden Cybersecurity-Anbieter im Vorteil sein, die umfassend Sicherheit für, mit und gegen künstliche Intelligenz beherrschen. Ferner werden Dienstleister mit einer ausgewogenen Kundenzielgruppe und Klienten aus dem öffentlichen Sektor profitieren, die zudem SOC-Betrieb aus Deutschland vorweisen können. Überdurchschnittliche Wachstumschancen bieten sich Beratern, die Post-Quantum Encryption Consulting offerieren und dabei perspektivisch die Breite des Marktes adressieren.

Schneller als erwartet wird Quantentechnologie zu einer Bedrohung für Anwender, bietet aber wie künstliche Intelligenz auch neue Chancen für Cybersecurity-Dienstleister. Vorteile haben dabei Provider, die bedarfsgerechte, souveräne Lösungen bieten, eine ausgewogene Zielgruppe adressieren und sowohl technische als auch regulatorische Aspekte beherrschen.

Anbieterpositionierung

Page 1 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
8com	Not In	Not In	Not In	Product Challenger	Not In	Not In
Absolute Software	Not In	Not In	Not In	Not In	Not In	Contender
Accenture	Leader	Leader	Leader	Not In	Leader	Not In
Acronis	Not In	Not In	Not In	Not In	Not In	Product Challenger
All for One Group	Contender	Contender	Not In	Not In	Not In	Not In
Argos Security	Not In	Product Challenger	Market Challenger	Rising Star ★	Not In	Not In
Atos	Leader	Leader	Leader	Not In	Not In	Not In
Axians	Leader	Leader	Leader	Leader	Not In	Not In
Bechtle	Market Challenger	Leader	Leader	Leader	Rising Star ★	Not In
Brainloop	Not In	Not In	Not In	Not In	Not In	Product Challenger
Broadcom	Not In	Not In	Not In	Not In	Not In	Leader

Anbieterpositionierung

Page 2 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
CANCOM	Market Challenger	Leader	Product Challenger	Leader	Not In	Not In
Capgemini	Leader	Leader	Leader	Not In	Not In	Not In
CGI	Contender	Not In	Not In	Contender	Not In	Not In
Computacenter	Leader	Leader	Product Challenger	Contender	Not In	Not In
Controlware	Leader	Leader	Leader	Leader	Not In	Not In
CoSoSys (Netwrix)	Not In	Not In	Not In	Not In	Not In	Contender
DATAGROUP	Not In	Not In	Market Challenger	Leader	Contender	Not In
Deloitte	Leader	Product Challenger	Product Challenger	Not In	Leader	Not In
Deutsche Telekom	Leader	Leader	Leader	Leader	Not In	Not In
DriveLock	Not In	Not In	Not In	Not In	Not In	Leader

Anbieterpositionierung

Page 3 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
DXC Technology	Contender	Leader	Contender	Not In	Not In	Not In
EY	Leader	Not In	Product Challenger	Not In	Leader	Not In
Fidelis Security	Not In	Not In	Not In	Not In	Not In	Contender
Forcepoint	Not In	Not In	Not In	Not In	Not In	Leader
Fortra	Not In	Not In	Not In	Not In	Not In	Leader
GBS	Not In	Not In	Not In	Not In	Not In	Leader
Getronics	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In
glueckkanja	Not In	Not In	Rising Star ★	Leader	Not In	Not In
Google	Not In	Not In	Not In	Not In	Not In	Contender
HCLTech	Leader	Leader	Leader	Product Challenger	Not In	Not In

Anbieterpositionierung

Page 4 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
HiSolutions	Product Challenger	Not In	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Leader	Not In	Leader	Leader
InfoGuard	Not In	Product Challenger	Leader	Leader	Not In	Not In
Infosys	Product Challenger	Product Challenger	Leader	Not In	Not In	Not In
itWatch	Not In	Not In	Not In	Not In	Not In	Product Challenger
KPMG	Leader	Not In	Not In	Not In	Leader	Not In
Kyndryl	Product Challenger	Product Challenger	Contender	Not In	Not In	Not In
Logicalis	Contender	Contender	Not In	Product Challenger	Not In	Not In
LTM	Not In	Not In	Not In	Product Challenger	Not In	Not In
ManageEngine	Not In	Not In	Not In	Not In	Not In	Leader

Anbieterpositionierung

Page 5 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
Materna	Leader	Market Challenger	Not In	Not In	Not In	Not In
Microsoft	Not In	Not In	Not In	Not In	Not In	Leader
Mimecast	Not In	Not In	Not In	Not In	Not In	Product Challenger
Netskope	Not In	Not In	Not In	Not In	Not In	Product Challenger
NTT DATA	Rising Star ★	Product Challenger	Product Challenger	Product Challenger	Leader	Not In
OpenText	Not In	Not In	Not In	Not In	Not In	Product Challenger
Orange Cyberdefense	Product Challenger	Market Challenger	Leader	Not In	Not In	Not In
ORBIT	Contender	Contender	Not In	Not In	Not In	Not In
pco	Not In	Not In	Contender	Product Challenger	Not In	Not In
Proofpoint	Not In	Not In	Not In	Not In	Not In	Market Challenger

Anbieterpositionierung

Page 6 of 7

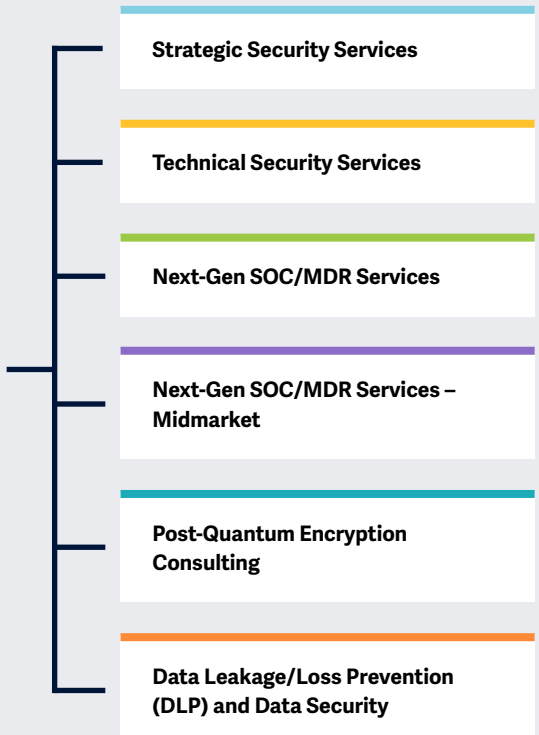
	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
PwC	Product Challenger	Not In	Not In	Not In	Product Challenger	Not In
q.beyond	Not In	Not In	Not In	Product Challenger	Not In	Not In
Rohde & Schwarz	Not In	Not In	Not In	Not In	Product Challenger	Not In
secunet	Not In	Not In	Not In	Not In	Product Challenger	Not In
SITS	Product Challenger	Product Challenger	Not In	Product Challenger	Market Challenger	Not In
Skaylink	Not In	Not In	Not In	Contender	Not In	Not In
Skyhigh Security	Not In	Not In	Not In	Not In	Not In	Product Challenger
Sopra Steria	Market Challenger	Not In	Market Challenger	Market Challenger	Not In	Not In
suresecure	Product Challenger	Product Challenger	Product Challenger	Leader	Not In	Not In
SVA	Not In	Not In	Not In	Product Challenger	Not In	Not In

Anbieterpositionierung

Page 7 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
Syntax	Not In	Product Challenger	Contender	Market Challenger	Not In	Not In
TCS	Product Challenger	Product Challenger	Leader	Not In	Product Challenger	Not In
Tech Mahindra	Not In	Product Challenger	Product Challenger	Product Challenger	Not In	Not In
Trellix	Not In	Not In	Not In	Not In	Not In	Leader
Unisys	Market Challenger	Market Challenger	Contender	Not In	Not In	Not In
Varonis	Not In	Not In	Not In	Not In	Not In	Product Challenger
Verizon Business	Not In	Not In	Product Challenger	Not In	Not In	Not In
Wavestone	Product Challenger	Not In	Not In	Not In	Product Challenger	Not In
Wipro	Leader	Product Challenger	Product Challenger	Not In	Contender	Not In
Zscaler	Not In	Not In	Not In	Not In	Not In	Product Challenger

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



Simplified Illustration Source: ISG 2026

Definition

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.

Betrachtungsumfang der Studie

Dieser ISG Provider Lens® Quadrantenreport deckt die folgenden fünf Themen für Dienstleistungen/Lösungen ab: Strategic Security Services (SSS), Technical Security Services (TSS), Next-Gen SOC/MDR Services, Post-Quantum Encryption Consulting und Data Leakage/Loss Prevention (DLP) & Data Security.

Diese ISG Provider Lens®-Studie bietet IT-Entscheidungsträgern:

- Transparenz über die Stärken und Schwächen der jeweiligen Anbieter und Softwarehersteller
- eine differenzierte Positionierung der Anbieter nach Segmenten (Quadranten)
- Fokus auf den regionalen Markt

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

Klassifizierung der Anbieter

Die Anbieterpositionierung spiegelt die Eignung des jeweiligen IT-Anbieters für ein definiertes Marktsegment (Quadrant) wider. Falls nicht anderweitig angegeben, gilt die Positionierung für alle Unternehmensgrößenklassen und Branchen. Unterscheiden sich die IT-Serviceanforderungen von Großunternehmen und Mittelständlern und ist das Spektrum der auf dem lokalen Markt tätigen IT-Anbieter ausreichend groß, erfolgt eine weitere Differenzierung der IT-Anbieter nach Leistungen entsprechend der Zielgruppe für Produkte und Dienstleistungen. Dabei werden entweder Branchenanforderungen oder die Mitarbeiterzahl sowie die Unternehmensstrukturen der Kunden berücksichtigt und die IT-Anbieter entsprechend ihrem Schwerpunkt positioniert. Im Ergebnis wird gegebenenfalls zwischen zwei Kundengruppen unterschieden, die wie folgt definiert werden:

- **Midmarket:** Unternehmen mit 100 bis 4.999 Mitarbeitern bzw. einem Umsatz zwischen 20 und 999 Mio. USD, zentraler Hauptsitz im jeweiligen Land, meistens in Privatbesitz.
- **Large Accounts:** Multinationale Unternehmen ab 5.000 Mitarbeitern oder mit Umsätzen von über einer Milliarde USD, weltweit aktiv und mit weltweit verteilten Entscheidungsstrukturen.

Die ISG Provider Lens® Quadranten werden auf Basis einer Bewertungsmatrix erstellt und enthalten vier Felder, in die die Anbieter eingeteilt werden: Leader, Product & Market Challenger und Contender. Jeder Quadrant einer ISG Provider Lens® Studie kann auch einen Anbieter beinhalten, der nach Meinung von ISG großes Potential hat, eine Leader-Position zu erreichen. Solche Anbieter können als Rising Star eingestuft werden.

- **Anzahl Anbieter pro Quadrant:** ISG bewertet und positioniert die wichtigsten Anbieter entsprechend dem Betrachtungsumfang der jeweiligen Studie; die Anzahl der pro Quadrant positionierten Anbieter ist auf 25 begrenzt (Ausnahmen sind möglich).

Anbieterklassifizierungen: Bewertungskategorien

Product Challenger:
Die Product Challenger decken mit ihren Produkten und Services die Anforderungen der Unternehmen überdurchschnittlich gut ab, können aber in den verschiedenen Kategorien der Marktbearbeitung nicht die gleichen Ressourcen und Stärken vorweisen wie die als Leader positionierten Anbieter. Häufig liegt dies in der Größe des Anbieters oder dem schwachen „Footprint" im jeweiligen Zielsegment begründet.

Leader:
Die als Leader eingeordneten Anbieter verfügen über ein hoch attraktives Produkt- und Serviceangebot sowie eine ausgeprägt starke Markt- und Wettbewerbsposition und erfüllen daher alle Voraussetzungen für eine erfolgreiche Marktbearbeitung. Sie sind als strategische Taktgeber und Meinungsführer anzusehen. Darüber hinaus sind sie ein Garant für Innovationskraft und Stabilität.

Contender:
Unternehmen, die als Contender positioniert sind, mangelt es bisher noch an ausgereiften Produkten und Services bzw. einer ausreichenden Tiefe und Breite des Offerings. Anbieter in diesem Bereich sind häufig auch Generalisten oder auch Nischenanbieter.

Market Challenger:
Market Challenger verfügen naturgemäß über eine hohe Wettbewerbsstärke, haben allerdings auf der Portfolio Seite noch ausgeprägtes Verbesserungspotenzial und liegen hier klar hinter den Unternehmen, die als „Leader" positioniert sind. Häufig sind es etablierte Anbieter, die Trends aufgrund ihrer Größe und der damit einhergehenden Unternehmensstruktur nicht schnell genug aufgreifen und in puncto Portfolioattraktivität deshalb Optimierungspotentiale vorweisen.

Anbieterklassifizierungen: Bewertungskategorien

★ Rising Stars
Ein solches Unternehmen kann zum Zeitpunkt der Auszeichnung ein vielversprechendes Portfolio bzw. die erforderliche Markterfahrung inkl. der notwendigen Roadmap mit adäquater Ausrichtung an den wichtigen Markttrends bzw. Kundenanforderungen vorweisen. Zudem verfügt das Unternehmen über ein ausgezeichnetes Management mit Verständnis für den lokalen Markt. Dieses Prädikat erhalten daher nur Anbieter oder Dienstleister, die in den letzten zwölf Monaten extreme Fortschritte hinsichtlich der gesteckten Zielerreichung verzeichnet haben und dank ihres überdurchschnittlichen Impacts und ihrer Innovationskraft auf dem besten Weg sind, innerhalb von 12-24 Monaten zu den Top-Anbietern zu gehören.

Not in
Diese Anbieter konnten aus einem oder mehreren Gründen nicht in den jeweiligen Quadranten positioniert werden: ISG konnte nicht genug Informationen für eine Positionierung einholen, das Unternehmen bietet nicht die entsprechend relevanten Services bzw. Lösungen, die für die einzelnen Quadranten definiert wurden, oder das Unternehmen konnte aufgrund seines Marktanteils, der Leistungsfähigkeit, der Kundenzahl oder anderer Größenmetriken mit den anderen Mitbewerbern im jeweiligen Quadranten nicht direkt verglichen werden. Eine „Nicht-Aufnahme" bedeutet weder, dass der Anbieter diese Leistungen oder Lösungen nicht bereitstellt noch soll damit etwas anderes ausgesagt werden.

Strategic Security Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Strategic Security Services (SSS)** in **Deutschland** anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz.

Cybersicherheits-Experten

sollten diesen Bericht lesen, um besser mit den sich entwickelnden Risiken umgehen zu können, die Fähigkeiten zur Erkennung von Bedrohungen zu stärken und zu verstehen, wie Anbieter fortschrittliche Bedrohungen mit neuen Technologien wie KI angehen. Die Erkenntnisse helfen dabei, Cybersecurity-Strategien mit umfassenderen Unternehmenszielen in Einklang zu bringen und gleichzeitig über wichtige Trends im Bereich Sicherheit und Risikomanagement auf dem Laufenden zu bleiben.

Technologieexperten

können anhand dieses Berichts Security-Partner identifizieren, die den Schutz in digitale Initiativen einbinden. Die Analyse zeigt auf, wie Anbieter KI, Automatisierung und maßgeschneiderte Sicherheitsdienste nutzen, um raffinierte Bedrohungen abzuwehren, Sicherheit in komplexe Umgebungen zu integrieren und sichere Innovationen im Rahmen groß angelegter digitaler Transformationsprogramme zu unterstützen.

Strategieexperten, CFOs und CEOs

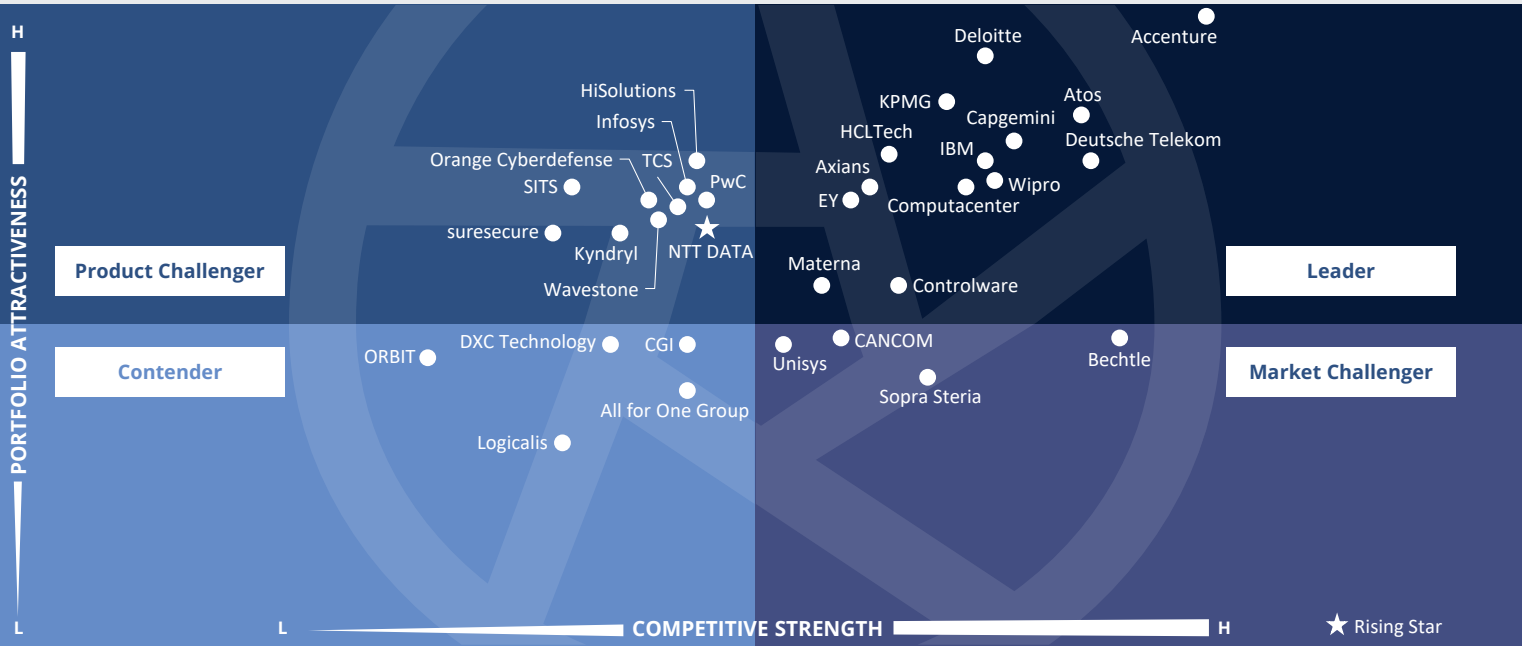
können mit Hilfe dieses Berichts die Partnerschaften, die Skalierbarkeit und das Kostenoptimierungspotenzial der Anbieter bewerten. CFOs und CEOs helfen diese Erkenntnisse, kosteneffiziente Sicherheitslösungen zu bewerten, die Cybersicherheit des Unternehmens zu stärken und sicherzustellen, dass die Investitionen auf die langfristige Resilienz des Unternehmens und die strategischen Prioritäten abgestimmt sind.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Strategic Security Services

Deutschland 2026



In diesem Quadranten geht es um die **relevantesten** Cybersecurity-Berater in Deutschland, die Leistungen **nicht nur für die eigenen Produkte** offerieren. Zunehmende Cyberbedrohungen mit neuen kriminellen Strategien **erhöhen die Nachfrage**.

Frank Heuer

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

Beobachtungen

Cybersecurity-Herausforderungen sind vielfältig, wandeln sich immer schneller, werden immer bedrohlicher und betreffen neue Zielgruppen. Daran müssen sich die Beratungsleistungen anpassen, um effektive Orientierung und Unterstützung zu bieten.

Zunehmender Beratungsbedarf ergibt sich aus globalen Konflikten und Spannungen und nach wie vor auch aus kommerzieller Cyberkriminalität mit immer neuen Methoden. Hinzu kommt die Erkenntnis, dass auf den Zero-Trust-Ansatz gesetzt werden muss.

Neben den Bedrohungen stellen regulatorische Anforderungen und die Berücksichtigung geschäftlicher Verhältnisse eine zunehmende Herausforderung dar. Europäische Unternehmen benötigen zudem zunehmend Bewertungen der digitalen Souveränität, da geopolitische Spannungen die Bedenken zum Beispiel hinsichtlich des Datenstandorts verstärken. Somit sind Dienstleister im Vorteil, die sowohl technisches als auch Business- und Compliance-Know-how vorweisen können.

Wie schon Großunternehmen bisher, sind viele mittelständische Unternehmen derzeit in mehrfacher Hinsicht betroffen. Sie geraten als vermeintlich leichtes Ziel vermehrt ins Visier von Cyberkriminellen. Zudem gelten zahlreiche Mittelständler aufgrund der NIS-2-Richtlinie neu als kritische Infrastruktur – und müssen infolgedessen (zusätzliche) Cybersecurity-Maßnahmen ergreifen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin; darunter leidet besonders der Mittelstand. Aufgrund dieser Faktoren benötigen Unternehmen zunehmend externe Unterstützung. Am Anfang steht hierbei häufig die Beratung.

Materna ist dieses Jahr vom Rising Star zum Leader aufgestiegen. NTT DATA ist der neue Rising Star. PwC und SITS sind neu im Quadranten vertreten.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 33 für diesen Quadranten qualifizieren. Dabei erreichten 14 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Führende Kompetenz und Erfahrung sowie ein umfassendes Leistungsangebot, das systematisch weiterentwickelt wird, tragen zu **Accentures** großem Erfolg in der Cybersecurity-Beratung in Deutschland bei.

Atos

Atos zeichnet sich mit seinem ganzheitlichen Ansatz im deutschen Markt für Cybersecurity-Beratung als Leader aus.

axians

Mit seinem zielgerichteten, pragmatischen Ansatz in der Cybersecurity-Beratung entspricht **Axians IT Security** besonders den Bedürfnissen der mittelständischen Zielgruppe.

Capgemini

Capgemini überzeugt seine Kunden für Cybersecurity Consulting in Deutschland mit einem breiten Beratungsspektrum, Erfahrung und aktuellen Beratungsansätzen.

Computacenter

Computacenter unterstützt seine Kunden mit Cybersecurity-Beratung, die in einen ganzheitlichen End-to-End-Ansatz eingebunden ist, und kann sich so als strategischer Partner mit Verständnis für die Infrastruktur- und Geschäftsanforderungen der Kunden positionieren.

controlware

Mit einem großen, qualifizierten Expertenteam und ausgeprägter Kundenorientierung wächst **Controlware** im deutschen Markt für Strategic Security Services kontinuierlich und positioniert sich erfolgreich als ein führender Anbieter.

Deloitte.

Deloitte verfügt über eine starke globale Präsenz und versteht sich im Cybersecurity Consulting auf die Synthese von Business- und Technologieberatung.

Mit großer Erfahrung in anspruchsvollen Umgebungen sowie mit End-to-End-Dienstleistungen aus einer Hand überzeugt die **Deutsche Telekom** als Cybersecurity-Berater in Deutschland.

EY

EY überzeugt mit einem ganzheitlichen Beratungsansatz, umfangreicher Erfahrung und innovativen Services und sichert sich damit eine führende Position im deutschen Markt für Strategic Security Services.

HCLTech

Durch ein innovatives, breit aufgestelltes und kundenorientiertes Portfolio positioniert sich **HCLTech** erfolgreich als führender Anbieter für Strategic Security Services in Deutschland.

IBM

Die Kunden von **IBM** profitieren in der Cybersecurity-Beratung von dem umfassenden Portfolio sowie den tiefen technologischen Kompetenzen des Anbieters; das macht IBM in Deutschland zu einem führenden Beratungshaus.

KPMG

KPMG profiliert sich in der Cybersecurity-Beratung in Deutschland mit hohen strategischen Kompetenzen sowie der geschickten Integration von technischen und Business-Aspekten.

MATERNA

Materna wird immer erfolgreicher und entwickelt sich vom „Rising Star" zu einem führenden Anbieter von Cybersecurity-Beratungsleistungen in Deutschland.

wipro

Wipro überzeugt seine Kunden in Deutschland mit umfassendem technischem Know-how und umfangreicher Cybersecurity-Beratung.

NTT DATA

NTT DATA ist dank eines innovativen, attraktiven Portfolios und wachsender Marktbedeutung der neue Rising Star für Strategic Security Services in Deutschland.

Leader

"Die großen Erfahrungen und Kompetenzen in anspruchsvollen Umgebungen tragen zum Erfolg und zur führenden Position der Deutschen Telekom im deutschen Markt für Cybersecurity-Beratung bei."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 198.000 Mitarbeitende in 50 Ländern. Im GJ25 erwirtschaftete das Unternehmen einen Umsatz von 119,1 Mrd. €. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom / T-Systems (nachfolgend „Deutsche Telekom") im Bereich Security mehr als 2.600 Mitarbeitende. Neben Managed Security Services und Technical Security Services werden auch Strategic Security Services angeboten.

Stärken

Langjährige zertifizierte Cybersecurity-Kompetenz: Die Deutsche Telekom kann auf über 25 Jahre Sicherheits- und Projektexpertise zurückgreifen und konnte eine der größten Datenbanken für Threat Intelligence aufbauen. Die Mitarbeitenden der Deutschen Telekom sind hoch zertifizierte Berater für verschiedene Standards und Technologien.

Experte für anspruchsvolle Umgebungen: Die Deutsche Telekom ist Spezialist für die Sicherheit kritischer nationaler Infrastrukturen. Darüber hinaus verfügen die Security-Berater der Deutschen Telekom über Expertise hinsichtlich der speziellen Bedingungen regulierter Branchen.

Kombinierte IT- und TK-Kompetenz: Die Deutsche Telekom ist in der Lage, IT- und TK-Sicherheit zu kombinieren und verschiedene Technologien führender Anbieter zu integrieren – das ist besonders wichtig für SASE-Lösungen.

Anbieter von End-to-End-Dienstleistungen: Die Deutsche Telekom ist nicht nur ein leistungsfähiger Cybersecurity-Berater, sondern insbesondere ein renommierter Anbieter von Managed Security Services, zudem sehr kompetent in der technischen Umsetzung von IT-Security-Projekten und somit in der Lage, die eigenen Empfehlungen auch bruchlos und in einem Guss in die Praxis umzusetzen.

Herausforderungen

Es empfiehlt sich zu prüfen, ob ein weiterer Ausbau der globalen Präsenz möglich ist. Die Deutsche Telekom ist inzwischen auf drei Kontinenten vertreten, gemessen an anderen herausragenden, führenden Anbietern ist die internationale Präsenz aber noch ausbaufähig.

Technical Security Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Technical Security Services (TSS)** in **Deutschland** anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz.

Technologie-Experten

erfahren aus diesem Bericht, wie die Anbieter Compliance-Anforderungen, die sich entwickelnde Marktdynamik und Integrations-Herausforderungen angehen. Die Erkenntnisse helfen bei Entscheidungen über die Einführung fortschrittlicher Technologien, die Innovationen ermöglichen, die Skalierbarkeit verbessern, Sicherheitsbedrohungen verringern und dabei stabile, zukunftsfähige digitale Architekturen unterstützen.

Sicherheits- und Datenexperten

gewinnen aus diesem Bericht ein tieferes Verständnis der Compliance-Ansätze der Anbieter, der wichtigsten Markttrends und der Rolle herstellerneutraler Lösungen. Die Ergebnisse unterstützen eine fundierte Entscheidungsfindung für groß angelegte Architekturtransformationen, bei denen Interoperabilität, eine verbesserte Sicherheitslage und langfristiger Datenschutz im Vordergrund stehen.

Experten auf der Geschäftsseite

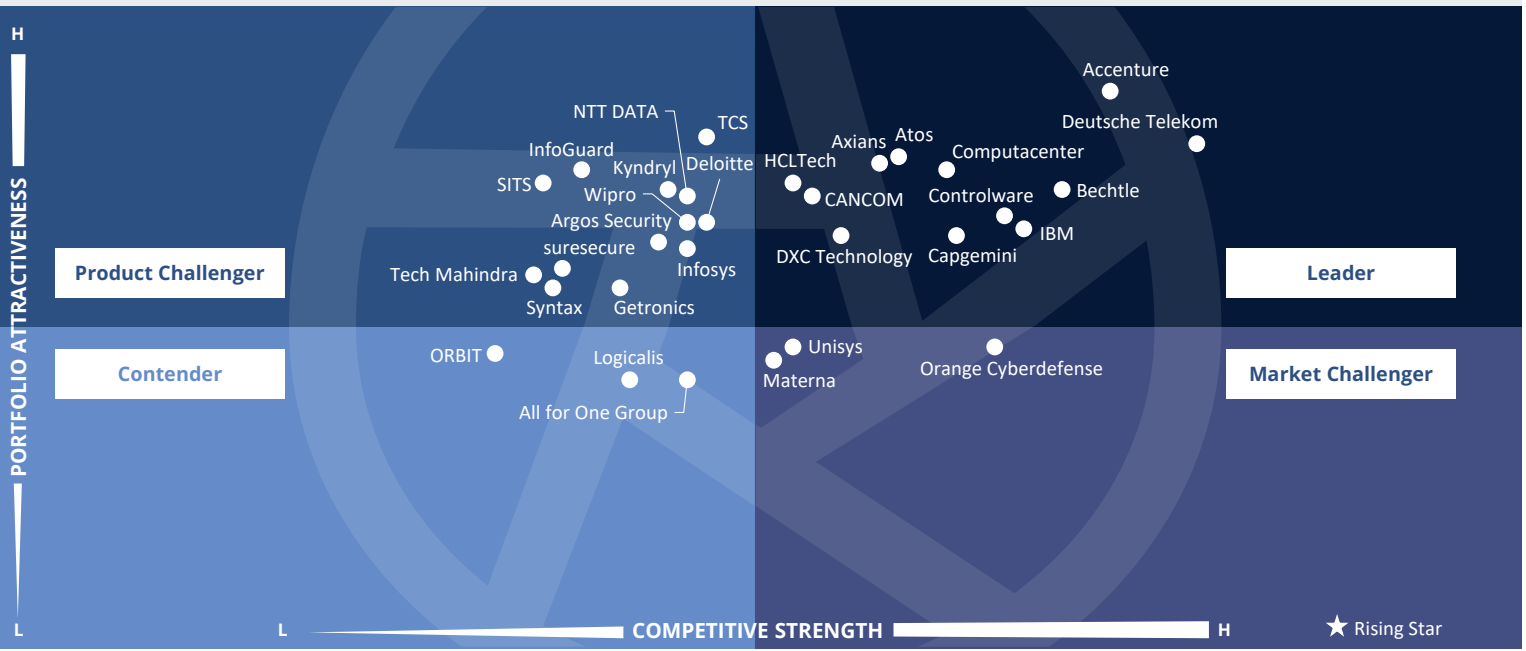
sollten diesen Bericht lesen, um Datensicherheit, Kundenerfahrung und Datenschutzanforderungen besser aufeinander abzustimmen. Die Erkenntnisse zeigen auf, wie Unternehmen Risiken und Vertrauen managen und gleichzeitig digitale Transformationsinitiativen ermöglichen können, die für modernes Unternehmenswachstum, die Einhaltung von Vorschriften und die Wettbewerbsdifferenzierung von zentraler Bedeutung sind.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services

Deutschland 2026



In diesem Quadranten geht es um die **relevantesten** Anbieter von technischen Security Services in Deutschland, deren Leistungen **nicht nur die eigenen Produkte** abdecken. Durch zunehmende Herausforderungen und den Fachkräftemangel werden **externe Provider** immer **wichtiger**.

Frank Heuer

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

Beobachtungen

Die immer intensiveren und ständig neuen Cyberattacken sind für Unternehmen in Deutschland nach wie vor eine Herausforderung, die durch den Mangel an Cybersecurity-Experten noch erschwert wird. Dies treibt die Nachfrage nach externen Dienstleistungen. Vorteile besitzen dabei Provider, die aktuelle Technologien wie auch die Ansprache verschiedener Zielgruppen beherrschen.

Nach wie vor ist die Identitätssicherheit ein zentrales Thema für deutsche Unternehmen und gewinnt durch den Schutz nicht-menschlicher Identitäten zusätzliche Bedeutung. Angesichts der zunehmenden Einführung von KI in Unternehmen rücken KI-Sicherheit, Plattformschutz und sichere KI-Infrastruktur immer mehr in den Fokus. Neben Sicherheit für KI wird vor allem auch Sicherheit durch KI immer wichtiger. Die Aktualisierung der Threat Intelligence ist dabei besonders zu nennen. Datensicherheit – on premises und in der Cloud – ist weiterhin eine Herausforderung mit hoher Priorität, die mit entsprechenden Anforderungen an das Data Security Posture Management einhergeht.

Provider mit einer ausgewogenen Kundenstruktur aus Großkunden und mittelständischen Unternehmen profitieren sowohl von den umfangreichen Budgets der Großkunden als auch vom überdurchschnittlichen Nachfragewachstum der Mittelständler.

Argos Security ist aus der Verbindung der deutschen Anbieter indevis und Data-Sec hervorgegangen und neu an Stelle von indevis im Quadranten vertreten. Auch den Schweizer Dienstleistern InfoGuard und SITS ist der Einstieg gelungen. Noch nicht für den Quadranten hat sich Riedel Networks qualifiziert, bringt für die Zukunft aber gute Voraussetzungen mit. Der brasilianische Dienstleister Stefanini expandiert in Deutschland und hat Chancen, zukünftig im Quadranten vertreten zu sein.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten zwölf eine Position als Leader.

accenture

Durch Automatisierung und ein breites Leistungsportfolio ermöglicht **Accenture** kosteneffiziente End-to-End-Sicherheit und positioniert sich als führender Anbieter von Technical Security Services in Deutschland.

Atos

Ein großes, qualifiziertes Team und ein breites Serviceportfolio machen **Atos** zu einem leistungsstarken, führenden Anbieter für Technical Security Services in Deutschland.

axians

Mit umfassenden technischen Cybersecurity-Dienstleistungen, Partnerschaften mit zahlreichen renommierten Cybersecurity-Technologieanbietern und einer ausgewogenen Kundenstruktur ist **Axians IT Security** im deutschen Markt erfolgreich.

BECHTLE

Bechtle punktet mit großer lokaler Marktpräsenz sowie umfangreichen Ressourcen und positioniert sich so als ein führender Anbieter von Technical Security Services in Deutschland, insbesondere für das dynamisch wachsende Marktsegment der mittelständischen Unternehmen.

CANCOM

CANCOM überzeugt seine Kunden mit maßgeschneiderten Lösungen auf Basis eines umfangreichen Themen- und Leistungsspektrums. Für den Mittelstand und auch für anspruchsvolle KRITIS-Branchen bietet CANCOM leistungsfähige technische Cybersecurity-Dienstleistungen an.

Capgemini

Capgemini profiliert sich als ein innovativer Anbieter von Technical Security Services und kann ein großes internationales Team vorweisen.

Computacenter

Computacenter kombiniert sein starkes Partnernetzwerk mit umfassenden Dienstleistungen sowie umfangreichem eigenem Know-how und positioniert sich so als Leader im deutschen Markt für technische Security Services.

controlware

Mit seinen zielgerichteten und modularen technischen Cybersecurity-Dienstleistungen sowie seinen deutschen Wurzeln ist **Controlware** im wachstumsstarken Mittelstandssegment erfolgreich.

Basierend auf einem großen, hoch qualifizierten Team sowie einem End-to-End-Service-Angebot made in Germany ist die **Deutsche Telekom** mit ihrer Tochter Deutsche Telekom Security ein Leader im Bereich der Technical Security Services in Deutschland.

DXC

Die Kunden von **DXC Technology** profitieren von integrierten IT-/Security-Lösungen sowie der Leistungsfähigkeit eines international aktiven, umfangreichen Teams.

HCLTech

Mit internationaler Erfahrung, einem breiten Portfolio und starken Technologiepartnerschaften positioniert sich **HCLTech** als führender Anbieter von Technical Security Services in Deutschland.

IBM

IBM überzeugt Großkunden mit großer Erfahrung, umfassenden Kompetenzen für Cybersecurity sowie starken, internationalen Delivery-Möglichkeiten.

Leader

"Dank eines großen, hoch qualifizierten Teams und End-to-End-Services „Made in Germany" ist die Deutsche Telekom mit ihrer Tochter Deutsche Telekom Security ein führender Anbieter von Technical Security Services in Deutschland."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 198.000 Mitarbeitende in 50 Ländern. Im GJ25 erwirtschaftete das Unternehmen einen Umsatz von 119,1 Mrd. €. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom / T-Systems (nachfolgend „Deutsche Telekom") im Bereich Security mehr als 2.600 Mitarbeitende. Neben Managed Security Services und Strategic Security Services werden auch Technical Security Services angeboten.

Stärken

Services aus Deutschland: Mit „Security made in Germany" kann die Deutsche Telekom speziell bei mittelständischen Kunden punkten. Die Kundennähe und lokale Erbringung der Technical Security Services ist ein starker Pluspunkt, nicht nur für Mittelstandskunden.

End-to-End-Lösungen für Cybersecurity: Die Deutsche Telekom bietet umfangreiche Technical Security Services, die ein sehr viele Themen abdecken, um für die Kunden Lösungen auf Zero-Trust-Basis zu ermöglichen. Neben Technical Security Services werden auch Beratung und Managed Security Services aus einer Hand angeboten, so dass der gesamte Lifecycle eines Security-Projektes abgedeckt werden kann. Darüber hinaus werden IT-Lösungen mit damit verbundener Cybersecurity ermöglicht. Vorteilhaft ist auch die spezielle Kompetenz hinsichtlich der Kombination von IT- und TK-Security.

Sehr großes, qualifiziertes Team: Die große Manpower ermöglicht große Kundennähe – die Deutsche Telekom beschäftigt das größte Spezialistenteam für Cybersecurity in Deutschland. Zudem verbessert das Unternehmen die Fachkenntnisse seiner Experten durch umfangreiche Schulungs- und Zertifizierungsmaßnahmen, die zu mehr als 2.000 Zertifizierungen der Mitarbeitenden geführt haben. Nicht zuletzt können die Experten die profunden Erfahrungen aus den Cybersecurity-Leistungen für den Deutsche-Telekom-Konzern vorweisen.

Herausforderungen

Mittlerweile ist die Deutsche Telekom auf drei Kontinenten vertreten; gemessen an anderen herausragenden, führenden Anbietern auf dem Leistungsniveau der Deutschen Telekom ist die internationale Präsenz jedoch noch ausbaufähig.

Next-Gen SOC/MDR Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Next-Gen SOC/MDR Services** in **Deutschland** anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz.

Cybersicherheits-Experten

gewinnen aus diesem Bericht ein klares Verständnis der neuen Bedrohungsmuster, der sich entwickelnden Angriffsvektoren und der kurzfristigen Risiken, die die Sicherheitslandschaft prägen. Die Erkenntnisse unterstützen eine fundierte Sicherheitsplanung, ermöglichen eine schnelle Priorisierung von Kontrollen und helfen den Teams, ihre Verteidigung zu stärken und dabei die betriebliche Effizienz zu verbessern und die Gesamtkomplexität der Sicherheit zu reduzieren.

Technologieexperten

informiert dieser Bericht über die wichtigsten Trends im Bereich der Cybersicherheit; sie erfahren, wie integrierte, plattformbasierte Sicherheitsansätze zu den umfassenderen Zielen im Hinblick auf die IT und die digitale Transformation passen. Der Bericht bietet Einblicke in moderne Sicherheitsarchitekturen sowie strategische Ziele und hilft Technologieführern bei der Entwicklung stabiler Umgebungen, die mit den sich schnell ändernden Sicherheitsanforderungen Schritt halten.

Verantwortliche auf der Geschäftsseite

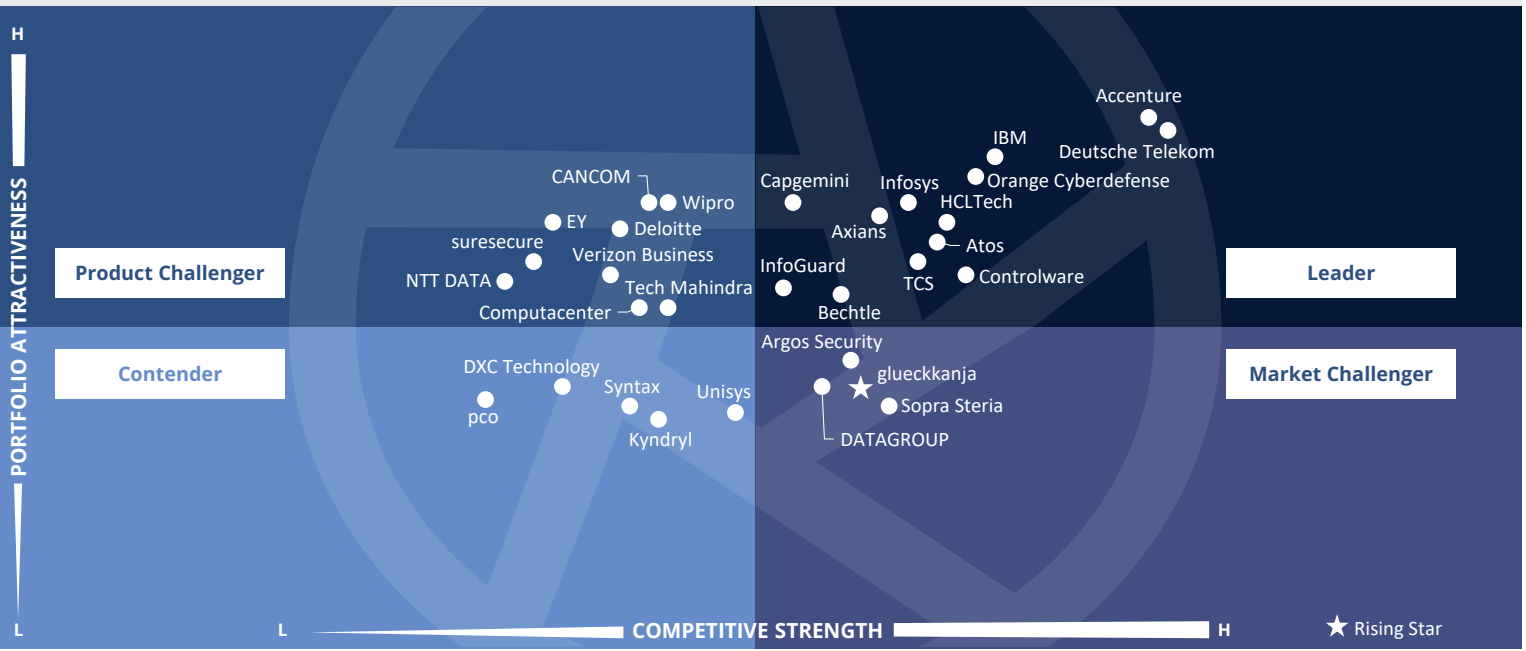
erhalten aus diesem Bericht praxisbezogene Einblicke dahingehend, wie Sicherheitsabläufe bei gleichzeitiger Abwägung von Risiko, Kosten und Effizienz vereinfacht werden können. Er zeigt umsetzbare Ansätze und Lösungen auf, die die betriebliche Komplexität reduzieren, eine bessere Entscheidungsfindung unterstützen und Unternehmen in die Lage versetzen, ihre Sicherheitsergebnisse zu verbessern, ohne die Unternehmensleistung oder Innovationen auszubremsen.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC/MDR Services

Deutschland 2026



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/ MDR Services** auf dem deutschen Markt, ohne Dienstleister, die ihre Leistungen nur auf eigene Produkte beziehen. Bedrohungslage und Fachkräftemangel **fördern** den Markt.

Frank Heuer

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.

Im Folgenden werden „Managed Services" synonym für „Next-Gen SOC/MDR Services" verwendet.

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 schnellerer 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

Beobachtungen

Die Nachfrage nach Managed Detection & Response (MDR) Services und Diensten von Security Operations Centers (SOCs) wird durch immer raffiniertere, häufigere, komplexere und wandlungsfähigere Cyberattacken getrieben. Für 2026 prognostiziert ISG ein Wachstum des deutschen Marktes für Managed Security Services – deren wesentlicher Bestandteil SOC- und MDR-Services sind – von mehr als 15 Prozent, nach 16,5 Prozent im Jahr 2025.

Das erforderliche stets aktuelle Spezialistenwissen und der gleichzeitige Mangel an qualifizierten Fachleuten rücken diese Managed Services zunehmend in den Fokus deutscher Unternehmen.

Für Großunternehmen spielen wegen ihrer häufig internationalen Präsenz global verteilte SOCs eine besondere Rolle. Aber auch EU- und deutsche SOC-Standorte wissen Großunternehmen aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen.

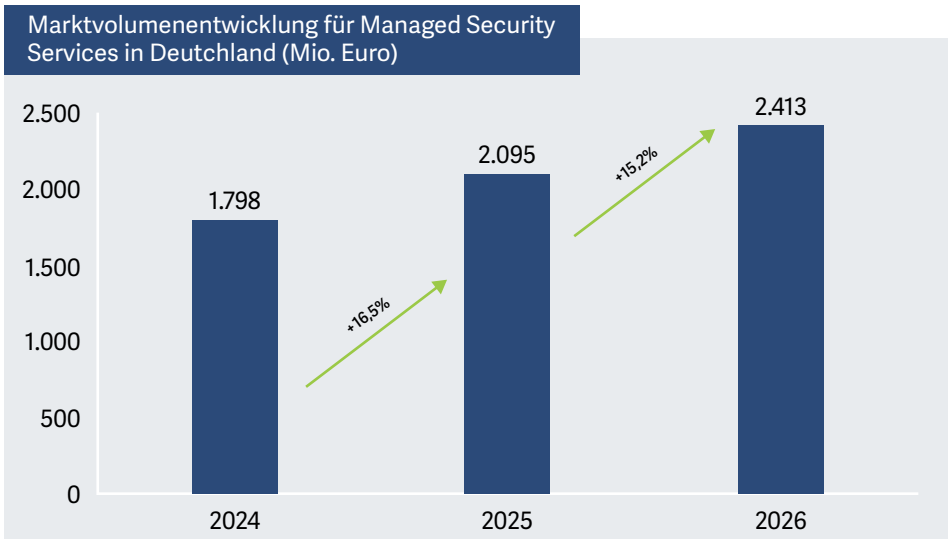
Auch Mittelständler interessieren sich verstärkt für SOC- und MDR-Services, um die wachsenden Herausforderungen bei gleichzeitig starkem Fachkräftemangel meistern zu können. Für diese Zielgruppe sind SOCs in Deutschland und deutschsprachige Ansprechpartner Pluspunkte.

Generell wird zudem von den Anbietern eine hohe Innovationskraft erwartet. Hierzu zählt unter anderem die Effizienzsteigerung durch Automatisierung, z.B. Agentic AI. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen interessant.

InfoGuard ist in diesem Jahr vom Rising Star zum Leader aufgestiegen. Der neue Rising Star ist glueckkanja. Argos Security ist aus der Verbindung der deutschen Anbieter indevis und Data-Sec hervorgegangen und neu an Stelle von indevis im Quadranten vertreten. Auch EY ist der Einstieg gelungen.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten 13 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Ein stark wachsender Markt



Quelle: ISG Research DACH

accenture

Umfassende Dienstleistungen und ein breites Spektrum adressierter Technologien sowie eine globale Präsenz und die Erschließung neuer Zielgruppen sind die Basis für **Accentures** großen Erfolg im deutschen Markt für Next-Gen SOC/MDR Services.

Atos

Mit innovativen Ansätzen und der globalen Präsenz seiner Next-Gen SOC/MDR Services zählt **Atos** zu den führenden Anbietern im deutschen Markt.

axians

Mit umfangreichen, kundenorientierten Leistungen ist **Axians IT Security** im deutschen Markt für Next-Gen SOC/MDR Services erfolgreich.

BECHTLE

Bechtle überzeugt seine Kunden mit umfangreichen, zertifizierten sowie modular anpassungsfähigen Next-Gen SOC/MDR Services und positioniert sich so als Leader in Deutschland.

Capgemini

Capgeminis Erfolg im deutschen Markt für Next-Gen SOC/MDR Services basiert auf umfassenden Dienstleistungen, starken Ressourcen und internationaler Präsenz.

controlware

Modulare, individualisierbare Services und SOC Services made in Germany tragen zum Erfolg von **Controlware** im deutschen Markt für Next-Gen SOC/MDR Services bei.

T

Mit ihren umfassenden, weiterentwickelten Next-Gen SOC/MDR Services, ihrem großen qualifizierten Team und dem Betrieb in Deutschland überzeugt die **Deutsche Telekom** als führender Anbieter.

HCLTech

Dank leistungsfähiger, kontinuierlich weiterentwickelter Services und starkem Engagement im deutschen Markt baut **HCLTech** seine führende Position bei Next-Gen SOC/MDR Services weiter aus.

IBM

IBM kombiniert leistungsstarke Technologie mit umfassenden, global verfügbaren Next-Gen SOC/MDR Services zum Vorteil international aktiver Großkunden.

InfoGuard
SWISS CYBER SECURITY

InfoGuard erreicht durch hohe technologische Dynamik und zunehmenden Erfolg den Aufstieg vom „Rising Star" zum führenden Anbieter von Next-Gen SOC/MDR Services in Deutschland.

Infosys

Infosys hat umfangreiche Ressourcen, entwickelt seine Next-Gen SOC/MDR Services kontinuierlich zum Vorteil seiner Großkunden weiter und positioniert sich damit als Leader für diese Dienstleistungen.

orange Cyberdefense

Orange Cyberdefense punktet mit europäischer Herkunft, globaler und lokaler Präsenz sowie kontinuierlich optimierten Next-Gen SOC/MDR Services.

Globale Präsenz und umfangreiche Technologieabdeckung, inklusive OT-Sicherheit, machen **TCS** zu einem Leader im deutschen Markt für Next-Gen SOC/MDR Services.

glueckkanja erschließt gezielt Wachstumssegmente im Markt, verzeichnet ein starkes Wachstum und ist damit der neue Rising Star im Markt der Next-Gen SOC/MDR Services in Deutschland.

Leader

"Mit ihren umfassenden, innovativen Next-Gen SOC/MDR Services „Made in Germany" und ihrem großen, qualifizierten Team überzeugt die Deutsche Telekom als ein führender Anbieter in Deutschland."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 198.000 Mitarbeitende in 50 Ländern. Im GJ25 erwirtschaftete das Unternehmen einen Umsatz von 119,1 Mrd. €. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom / T-Systems (nachfolgend „Deutsche Telekom") im Bereich Security mehr als 2.600 Mitarbeitende. Das SOC kombiniert auf maschinellem Lernen basierende künstliche Intelligenz, Verhaltensanalysen und Threat Hunting. Mit Magenta Security Shield und Magenta Security MDR Pro werden differenzierte Leistungen geboten.

Stärken

Zahlreiche qualifizierte Spezialisten: In Deutschland unterhält die Deutsche Telekom ein sehr großes, hochqualifiziertes Expertenteam für ihre Managed Security Services und bietet ihren Kunden die gleichen Technologien und Services, die das Unternehmen auch zum Schutz der Deutschen Telekom AG weltweit einsetzt. Daher kennen die Experten der Deutschen Telekom die Komplexität des Schutzes eines globalen Unternehmenskunden und verfügen über die nötige Erfahrung und das Wissen, um Kunden mit dem gleichen hohen Standard schützen zu können.

SOC-Betrieb in Deutschland: Die Deutsche Telekom betreibt ihre Managed Security Services unter anderem in Deutschland und bietet „Security made in Germany", was im Zuge der Datenschutzdiskussion als Vorteil gesehen wird. Die Deutsche Telekom betreibt hochmoderne Cyber Defense & Security Operations Center und generiert als globaler Carrier umfangreiche Threat Intelligence. Die Telekom Threat Library, eine umfangreiche Datenbank mit Malware, APT-Angriffen, Zero-Day-Exploits und Angriffsmustern, wird kontinuierlich aktualisiert.

Expandierendes Angebot: Die Deutsche Telekom entwickelt ihr bereits sehr umfassendes Angebot kontinuierlich weiter, um auch zukünftig ein leistungsfähiges Portfolio anbieten zu können, und plant umfangreiche Ergänzungen des Portfolios – die Roadmap zählt zahlreiche Vorhaben auf.

Herausforderungen

Die Deutsche Telekom ist im Markt für Managed Security Services bereits sehr erfolgreich Mit dem Angebot eines Co-Managed SOC/MDR Services könnten noch weitere Kundengruppen erschlossen werden, für die sich ein solches Angebot besonders eignen würde.

Next-Gen SOC/MDR Services – Midmarket

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Next-Gen SOC/MDR Services** in **Deutschland** für den Mittelstand anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für mittelständische Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz.

Verantwortliche auf der Geschäftsseite

gewinnen aus diesem Bericht praxisbezogene Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht werden und dabei ein effektives Risikomanagement beibehalten werden kann. Es werden praxisnahe Ansätze und Lösungsmodelle vorgestellt, die dazu beitragen, die betriebliche Komplexität zu verringern, die Effizienz zu steigern und eine bessere Abstimmung zwischen Sicherheitsinvestitionen, geschäftlichen Prioritäten und der Gesamtleistung des Unternehmens zu ermöglichen.

Cybersicherheit-Experten

werden mit diesem Bericht über neue Trends, sich entwickelnde Bedrohungsszenarien und kurzfristige Risiken im Hinblick auf moderne SOC- und MDR-Umgebungen informiert. Diese Erkenntnisse unterstützen strategische Sicherheitsentscheidungen, helfen Teams bei der Priorisierung von Erkennungs- und Reaktionsfähigkeiten und ermöglichen eine verbesserte Produktivität bei gleichzeitiger Reduzierung der betrieblichen und architektonischen Sicherheitskomplexität.

Technologieexperten

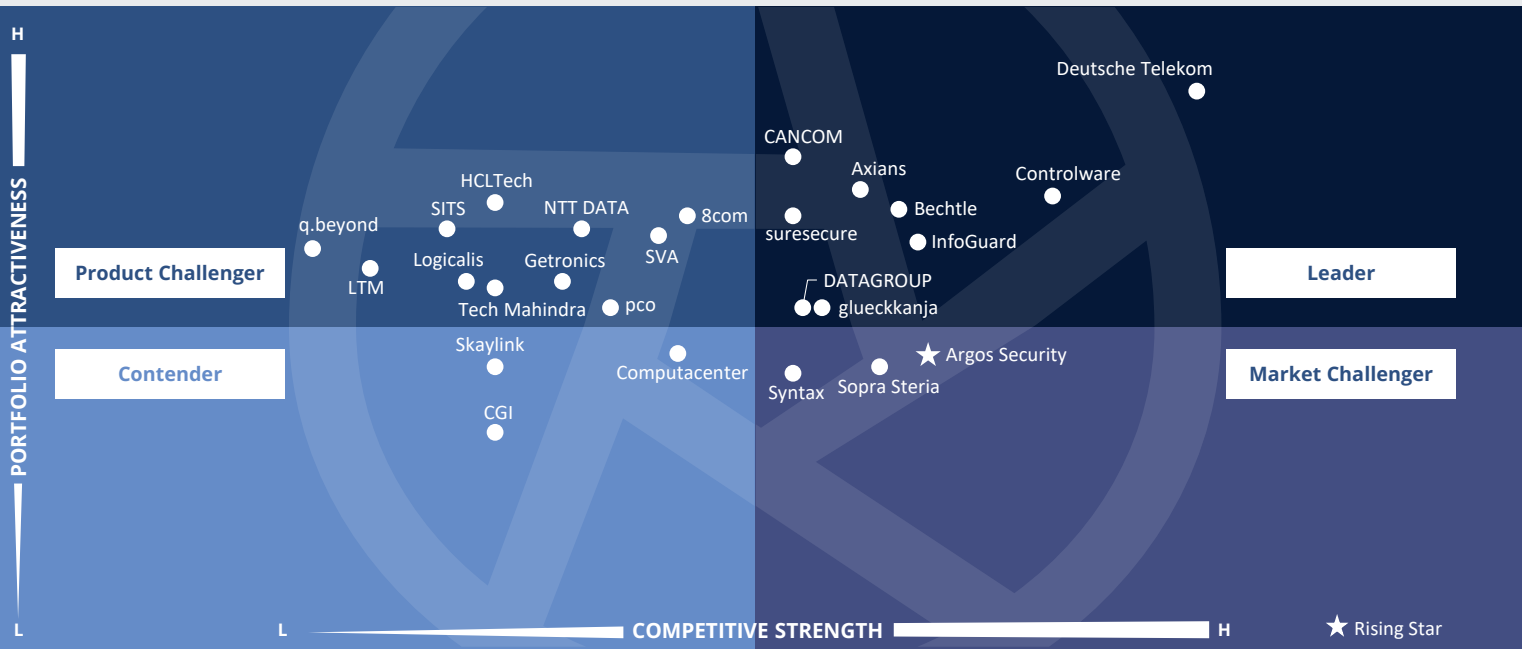
erhalten aus diesem Bericht Einblicke in neue Sicherheitstrends, SOC/MDR-Plattformen der nächsten Generation und die strategischen Ziele, die deren Einführung vorantreiben. Er hilft Technologieführern zu verstehen, wie maßgeschneiderte Sicherheitsarchitekturen in bestehende IT-Umgebungen integriert werden können und skalierbare, resiliente Verteidigungsmaßnahmen in einer sich schnell verändernden Sicherheitslandschaft unterstützen.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC/MDR Services – Midmarket

Deutschland 2026



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/ MDR Services** für deutsche **Mittelständler**, ohne Provider, die nur eigene Produkte betreuen. Zunehmende Cyberangriffe und Fachkräftemangel bewirken eine **steigende Nachfrage**.

Frank Heuer

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.

Im Folgenden werden „Managed Services" synonym für „Next-Gen SOC/MDR Services" verwendet.

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

Beobachtungen

Noch stärker als im Gesamtmarkt wächst die Nachfrage nach Next-Gen SOC/MDR Services im Segment der Mittelstandskunden. Dazu tragen zwei Hauptfaktoren bei: Mehr noch als Großunternehmen sind mittelständische Unternehmen in Deutschland vom Cybersecurity-Fachkräftemangel betroffen. Gleichzeitig sind auch sie mit immer mehr und immer komplexeren Sicherheitsherausforderungen konfrontiert und geraten nun öfter ins Visier von Cyberkriminellen, die in dieser Zielgruppe leichte Opfer vermuten. Zudem sind durch die NIS-2-Richtlinie an viele Mittelständler inzwischen erhöhte Sicherheitsanforderungen gestellt. Daher sind auch mittelgroße Unternehmen verstärkt auf externe (SOC-/MDR-) Dienstleistungen angewiesen.

Für das Mittelstandssegment sind SOCs in Deutschland aus Gründen des Vertrauens und des Datenschutzes ein Pluspunkt. Auch deutschsprachige Ansprechpartner spielen eine wichtige Rolle. Viele Mittelständler wünschen sich von ihren SOC-Dienstleistern ein unkompliziertes, rasches Onboarding.

Auch Mittelständler erwarten von SOC-Dienstleistern eine hohe Innovationskraft, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Nutzung von Automatisierung, z.B. Agentic AI, um auch komplexere Bedrohungen effizient zu meistern. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen zunehmend interessant.

glueckkanja ist in diesem Jahr zum Leader aufgestiegen. Der neue Rising Star ist Argos Security, hervorgegangen aus der Verbindung der deutschen Anbieter indevis und Data-Sec, und neu an die Stelle von indevis getreten. 8com, q.beyond, SITS und Skaylink ist der Einstieg in diesen Quadranten gelungen.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 26 für diesen Quadranten qualifizieren. Dabei erreichten neun eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

axians

Mit umfangreichen und bedarfsgerechten Next-Gen SOC/MDR Services ist **Axians IT Security** in der Lage, seine mittelständischen Kunden zu überzeugen. Damit zählt der Anbieter zu den führenden SOC-Dienstleistern in Deutschland.

BECHTLE

Bechtle ist mit seinen umfangreichen und anpassungsfähigen Dienstleistungen sowie der Delivery aus Deutschland ein Leader hinsichtlich Next-Gen SOC/MDR Services für den deutschen Mittelstand.

CANCOM

CANCOM adressiert die Anforderungen des Mittelstands im deutschen Markt für Next-Gen SOC/MDR Services passgenau, unter anderem auch im Hinblick auf Datensouveränität.

controlware

Controlware ist mit flexiblen, kundenorientierten Services ein Leader im Markt für Next-Gen SOC/MDR Services für den deutschen Mittelstand.

DATAGROUP

DATAGROUP überzeugt im Markt für SOC-Services für den deutschen Mittelstand mit hochwertigen, integrierten Dienstleistungen.

Die **Deutsche Telekom** ist mit einem großen Team und einem umfangreichen Angebot „made in Germany" der führende Anbieter von Next-Gen SOC/MDR Services für den deutschen Mittelstand.

glueckkanja

glueckkanja verzeichnet ein starkes Wachstum und etabliert sich damit als einer der führenden Anbieter von Next-Gen SOC/MDR Services im deutschen Mittelstandssegment.

InfoGuard
SWISS CYBER SECURITY

InfoGuard hat nach der Übernahme von Com-Sys seine Position im Markt für Next-Gen SOC und MDR Services im Mittelstandssegment in Deutschland deutlich gestärkt und ausgebaut.

sure[secure]

suresecure hat sich erfolgreich als innovativer und führender Anbieter im deutschen Mittelstandsmarkt für SOC Services etabliert.

Argos Security

Argos Security ist durch die Vereinigung der Kräfte von indevis und Data-Sec der neue Rising Star im Markt der Next-Gen SOC/MDR Services für den deutschen Mittelstand.

Leader

"Mit „Security made in Germany" und einem innovativen Angebot, das von hoch qualifizierten Mitarbeitern bereitgestellt wird, positioniert sich die Deutsche Telekom als führender Anbieter von SOC-/MDR-Dienstleistungen für den deutschen Mittelstand."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 198.000 Mitarbeitende in 50 Ländern. Im GJ25 erwirtschaftete das Unternehmen einen Umsatz von 119,1 Mrd. €. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom / T-Systems (nachfolgend „Deutsche Telekom") im Bereich Security mehr als 2.600 Mitarbeitende. Das SOC kombiniert auf maschinellem Lernen basierende künstliche Intelligenz, Verhaltensanalysen und Threat Hunting.

Stärken

Umfangreiches, wachsendes Portfolio: Um auch zukünftig ein leistungsfähiges Portfolio anbieten zu können, entwickelt die Deutsche Telekom ihr bereits sehr umfassendes Angebot kontinuierlich weiter und plant weitere umfangreiche Ergänzungen des Portfolios – die Roadmap zählt zahlreiche Vorhaben auf.

Großes, qualifiziertes Team: Die Deutsche Telekom unterhält in Deutschland ein sehr großes, hochqualifiziertes Expertenteam für ihre Managed Security Services und bietet ihren Kunden die gleichen Services und Technologien, die das Unternehmen auch zum Schutz der Deutschen Telekom AG weltweit einsetzt. Die Experten der Deutsche Telekom kennen daher die Herausforderung im Zusammenhang mit dem Schutz von Unternehmenskunden und verfügen über das nötige Wissen und die Erfahrung, um Kunden mit dem gleichen hohen Standard schützen zu können.

Services aus Deutschland: Die Deutsche Telekom bietet „Security made in Germany" und erbringt ihre Managed Security Services unter anderem in Deutschland, was besonders von vielen Mittelstandskunden geschätzt wird. Der Anbieter betreibt hochmoderne Cyber Defense & Security Operations Center. Mit „Security made in Germany" kann die Deutsche Telekom speziell angesichts der Datenschutzdiskussion – und besonders in der Zielgruppe des Mittelstandes – punkten. Im Herbst 2024 hat die Deutsche Telekom ihr neues SOC in Bonn eröffnet.

Herausforderungen

Die Deutsche Telekom ist insgesamt sehr erfolgreich im Mittelstandssegment. Das Schwerpunktsegment sind dabei die gehobenen Mittelstandskunden. Mit einem stärkeren Fokus auch auf das darunter liegende Marktsegment könnte die Deutsche Telekom aufgrund dessen überdurchschnittlich stark wachsender Nachfrage noch erfolgreicher sein.

Post-Quantum Encryption Consulting

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Anbieter von Beratungsleistungen für **Post-Quanten-Verschlüsselung** in **Deutschland** von Nutzen, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. In diesem Quadranten hebt ISG die aktuelle Marktpositionierung dieser Unternehmen hervor, und zwar auf Basis der Tiefe ihrer auf Kryptografie ausgerichteten Leistungen, ihrer Bereitschaft zur Einführung der Post-Quanten-Kryptografie (PQC) und ihrer allgemeinen Marktpräsenz.

Verantwortliche auf der Geschäftsseite

erhalten aus diesem Bericht Einblicke in die strategische Bedeutung des Wechsels zur post-quanten-fähigen Verschlüsselung. Er hilft ihnen, die Auswirkungen von PQC auf die Risikominderung, den langfristigen Datenschutz und die Compliance zu verstehen, und klärt darüber auf, wie Beratungspartner den Umstieg vereinfachen und eine sichere digitale Transformation unterstützen können.

Cybersicherheits-Experten

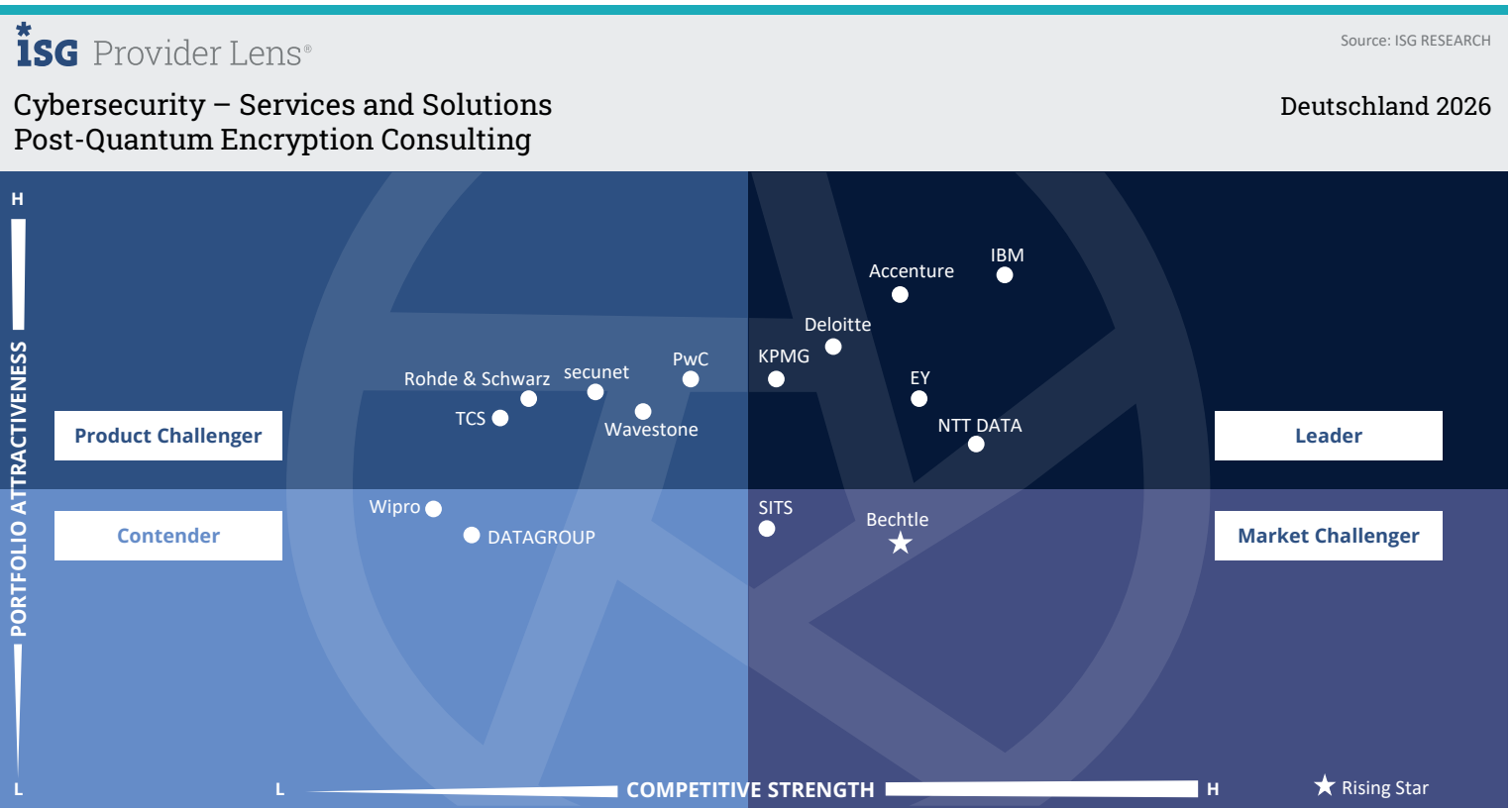
können sich mit diesem Bericht über neue Trends, Risiken und Strategien zur Risikominderung im Zusammenhang mit Post-Quanten-Bedrohungen informieren. Er unterstützt eine fundierte Entscheidungsfindung im Hinblick auf kryptographische Modernisierung, hebt die Stärken der Anbieter hervor und ermöglicht es den Teams, die Resilienz zu verbessern, komplexe Sicherheitsabläufe zu optimieren und sich auf eine quantensichere Zukunft vorzubereiten.

Technologieexperten

informiert dieser Bericht über sich entwickelnde Verschlüsselungsstandards, PQC-Migrations-Frameworks und die zur Unterstützung quantensicherer Architekturen erforderlichen Werkzeuge. Es bietet Klarheit über die Leistungen der Anbieter, ihre Integrationsansätze und Best Practices, die Teams dabei helfen können, ihre Modernisierungsprioritäten mit der sich schnell verändernden Sicherheitslandschaft in Einklang zu bringen.

Verantwortliche aus den Bereichen IT und digitale Transformation

erfahren aus diesem Bericht, wie Beratung zur Post-Quanten-Verschlüsselung ihre langfristige Sicherheitsplanung unterstützen kann. Die Analyse hilft ihnen, die Expertise der Anbieter in den Bereichen Bewertung, Roadmap-Entwicklung und Implementierung zu evaluieren, und ermöglicht so fundiertere Entscheidungen bei der Vorbereitung von Infrastrukturen und Anwendungen auf eine quantenresiliente Umgebung.



In diesem Quadranten geht es um die **relevantesten** Anbieter von Post-Quantum Encryption Consulting in Deutschland, die Leistungen **nicht nur für die eigenen Produkte** offerieren. „Harvest Now, Decrypt Later" macht dies zu einem **drängenden** Thema.

Frank Heuer

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), Identity- & Access-Systemen, sicherer Kommunikation und Anwendungsarchitekturen
5. Nachgewiesene **PQC-bezogene Kundenmandate in Deutschland**, 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

Beobachtungen

Die kommende Quanten-Technologie stellt durch ihre bahnbrechende Leistungsfähigkeit eine massive Gefährdung für die bisherige Verschlüsselung sensibler Daten dar. Die Marktgängigkeit von Quanten-Computern wird gegen Ende dieses/Anfang des nächsten Jahrzehnts erwartet.

Die neuen Strategien von Cyberkriminellen lassen jedoch ein Abwarten bis zu diesem „Q-Day" häufig nicht mehr zu. Mit dem „Harvest Now, Decrypt Later"-Ansatz ist die Bedrohung aktuell geworden. Dies betrifft vor allem Unternehmen, deren Existenz stark von Daten abhängt, wie zum Beispiel Banken und Versicherungen. Daher suchen besonders diese Wirtschaftszweige bereits nach Beratung hinsichtlich der besten Abwehrstrategien.

Mit dem Näherrücken des Q-Days werden sich vermehrt auch andere Branchen und auch die Breite der Unternehmen mit diesem Thema befassen. So beginnt der Beratungsmarkt für Post-Quantum Encryption sich bereits in dieser frühen Marktphase allmählich nach verschiedenen Zielgruppen auszudifferenzieren.

In dieser frühen Marktphase stehen insbesondere noch Beratungsleistungen im Vordergrund, die auf die Bedrohungsanalyse – auch unter Berücksichtigung regulatorischer Vorgaben – sowie die Inventarisierung potenziell bedrohter Daten gerichtet sind. Demnächst werden auch Pläne zur konkreten Maßnahmenumsetzung sowie Implementierungsdienstleistungen signifikant stärker nachgefragt werden.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 15 für diesen Quadranten qualifizieren. Dabei erreichten sechs eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Accenture überzeugt auch auf C-Level mit umfassender Expertise und klaren strategischen Empfehlungen zum Thema Post-Quantum-Encryption und positioniert sich damit in diesem Bereich als führender Berater in Deutschland.

Deloitte.

Deloitte kombiniert in der Post-Quantum-Encryption-Beratung regulatorische Expertise mit fundierter Risikobewertung und gehört damit zu den führenden Anbietern im deutschen Markt.

EY

EY differenziert sich im Post-Quantum Encryption Consulting durch ein risikoorientiertes, regulatorisch abgestimmtes Beratungsmodell und zählt damit zu den führenden Dienstleistern in Deutschland.

IBM

IBM ist ein Pionier in der Quantencomputerentwicklung und zugleich ein Vorreiter sowie führender Berater im Bereich Post-Quantum Encryption in Deutschland.

KPMG

KPMG positioniert sich mit der Verbindung aus Strategie-, Regulierungs- und Transformationskompetenz als ein führender Anbieter im deutschen Markt für Post-Quantum-Encryption-Beratung.

NTT DATA

Dank eines umfassenden, herstellerunabhängigen Portfolios ist **NTT DATA** im deutschen Markt für Post-Quantum-Encryption-Beratung bereits erfolgreich etabliert und als ein führender Anbieter positioniert.

BECHTLE

Bechtle verzeichnet starkes Wachstum, antizipiert die Expansion im Zukunftsmarkt der Post-Quantum-Encryption-Beratung und qualifiziert sich damit in Deutschland als Rising Star für dieses Thema.

Data Leakage/Loss Prevention (DLP) and Data Security

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Anbieter von Lösungen für **Data Leakage/Loss Prevention (DLP) und Datensicherheit** in **Deutschland** von Nutzen, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Lösungsangebots und ihrer Marktpräsenz.

IT-Sicherheitsexperten

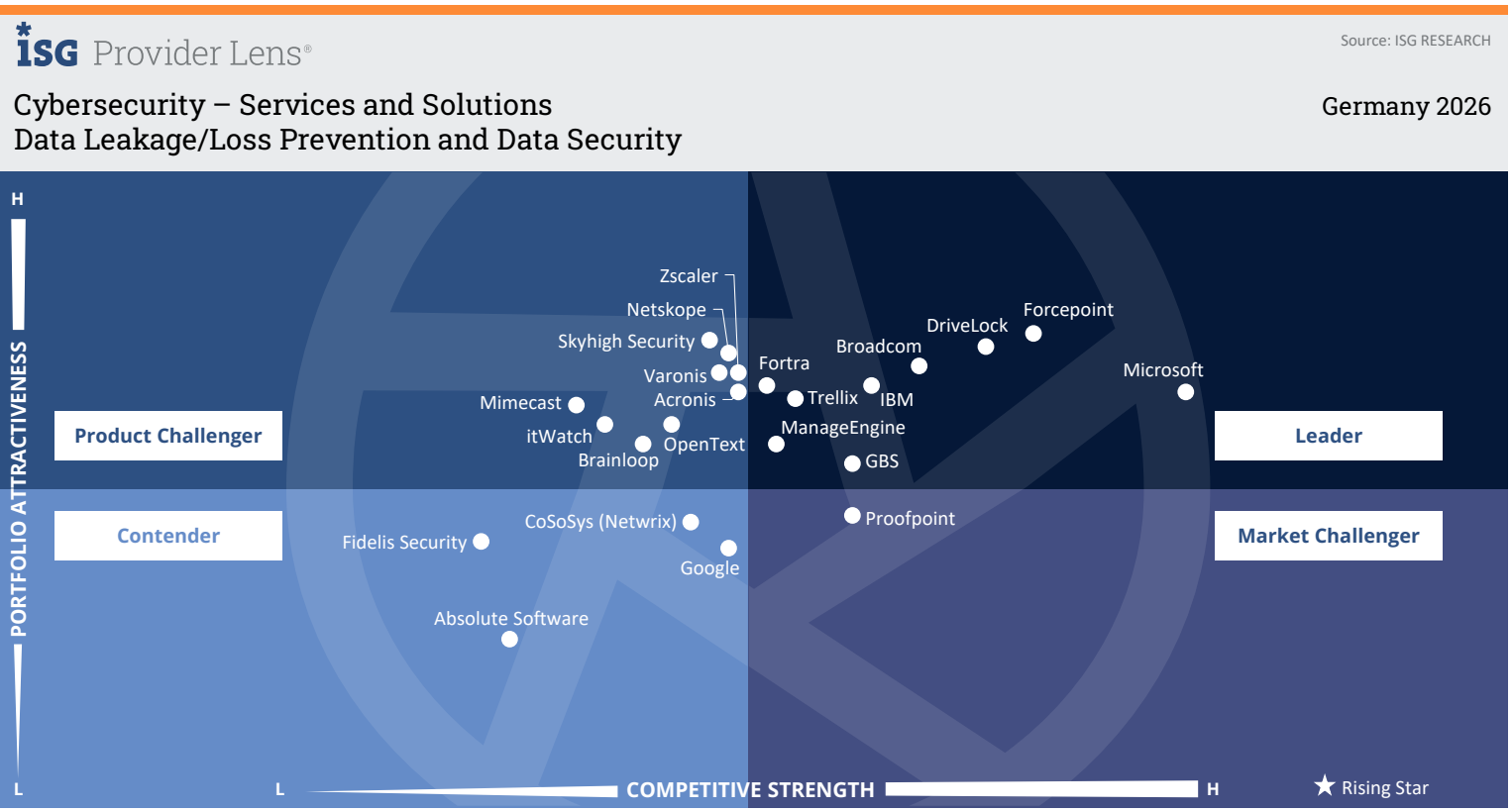
können sich mit diesem Bericht über den aktuellen Stand des DLP- und Datensicherheitsmarktes in Deutschland informieren Er bietet Einblicke in die Fähigkeiten der Anbieter, ihre Service-Tiefe und Marktpositionierung sowie in neue Trends, innovative Funktionen und Best Practices. Der Bericht hilft diesen Experten, Lösungen zu vergleichen, Stärken und Lücken zu identifizieren und effektive Datenschutzstrategien zu entwickeln, die auf die sich entwickelnden Bedrohungslandschaften abgestimmt sind.

Chief Information Security Officers (CISOs)

erhalten aus diesem Bericht einen strategischen Überblick über die sich entwickelnde DLP-Landschaft in Deutschland. Er hebt die führenden Anbieter, den Reifegrad der Lösungen und die Marktpräsenz hervor und unterstützt damit eine fundierte Entscheidungsfindung. CISOs können diese Erkenntnisse nutzen, um Investitionen zu priorisieren, DLP-Initiativen mit Geschäfts- und Risikozielen abzustimmen und die Resilienz des Unternehmens im Hinblick auf Datenlecks und gesetzliche Vorschriften zu stärken.

Compliance-Beauftragte

die für den Datenschutz und die Einhaltung gesetzlicher Vorschriften verantwortlich sind, gewinnen aus diesem Bericht ein besseres Verständnis dahingehend, wie DLP-Lösungen die Einhaltung der deutschen und EU-Datenschutzanforderungen unterstützen. Der Bericht erläutert, wie die Leistungen der Anbieter die Anforderungen an Datentransparenz, Kontrolle und Berichterstattung erfüllen und Unternehmen dabei helfen, Compliance-Risiken zu verringern, die Erfüllung ihrer Rechenschaftspflichten nachzuweisen sowie die Compliance mit Datenschutz- und Sicherheitsvorschriften zu gewährleisten.



Hier werden die **relevantesten** DLP-Anbieter in Deutschland, die eigenerstellte **Software** anbieten bzw. betreiben, bewertet. Die verstärkte **Datenschutzdiskussion** und die Sicherung **geistigen Eigentums** tragen zur Bedeutung des Marktes bei.

Frank Heuer

Data Leakage/Loss Prevention (DLP) and Data Security

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. Daten**erkennung**, Echtzeit**überwachung** und richtlinienbasierte **Durchsetzungsmaßnahmen**
6. **Nachgewiesene** Implementierungen auf Enterprise-Niveau und dokumentierte Kundenakzeptanz

Beobachtungen

Zahlreiche Faktoren tragen zur wachsenden Bedeutung von DLP-Lösungen bei. Daten haben sich zu immer wichtigeren und teilweise existenziell bedeutsamen Unternehmens-Assets entwickelt. Die enorme Zunahme an Unternehmensdaten erfordert leistungsfähige DLP-Lösungen, die die Daten schnell aufspüren, klassifizieren und entsprechend ihrem Schutzbedarf vor unerlaubten Aktionen schützen. Mit der Datenschutz-Grundverordnung und der NIS-2-Richtlinie hat die Bedeutung des Datenschutzes in Unternehmen weiter zugenommen.

Die Vielfalt der Speicherorte von Daten erfordert einen konsistenten Datenschutz über diese hinweg. Die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen und teilweise auch aus rechtlichen Gründen nicht umfassend betrieblich überwacht werden dürfen.

Cloud-Speicherlösungen und -Apps führen dazu, dass Daten bei der Verarbeitung unter Umständen ungewollt das Firmennetzwerk verlassen.

Social-Media- und Kommunikations-Plattformen eröffnen Kommunikationskanäle, über die Daten abfließen können; hinzu kommen nicht zuletzt die Risiken durch Datentransfers via E-Mail.

Nicht nur ungewollt können Daten durch internes Verschulden abfließen; auch vor ungetreuem Verhalten interner Beteiligter müssen sich Unternehmen schützen können.

KI hilft zunehmend bei der Bewältigung der Herausforderungen. Zunehmende Bedeutung hat datenzentrierte Sicherheit, also der direkte Schutz der Daten bei ihrer Nutzung, Weitergabe und Speicherung.

Der letztjährige Rising Star ManageEngine ist in diesem Jahr zum Leader aufgestiegen.

Von den 71 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 23 für diesen Quadranten qualifizieren. Dabei erreichten neun eine Position als Leader.

Broadcom

Broadcom verbindet Leistungsfähigkeit mit einfacher Verwaltung und großer Flexibilität – und ist damit ein führender Anbieter von DLP-Lösungen in Deutschland.

DriveLock

Der deutsche DLP-Anbieter **DriveLock** schafft Vertrauen mit den Devisen „Made in Germany" und „No Backdoor" – und unterstützt seine Kunden über den gesamten Datenlebenszyklus und auch in der Cloud effizient bei der Einhaltung von Richtlinien.

Forcepoint

Forcepoint hilft den Anwendern und erleichtert DLP durch fortschrittliche Lösungen, schnelle Abhilfe bei Vorfällen und Einhaltung des Datenschutzes.

Fortra

Fortra bietet ein vielseitiges DLP-Portfolio, das die Einhaltung des Datenschutzes für Anwenderunternehmen vereinfacht, und zwar mit Hilfe von proaktiver Datenklassifizierung sowie fortschrittlichen Analyse- und Reporting Services.

GBS

Der deutsche DLP-Anbieter **GBS** sorgt mit ausgefeilter Technik und Vier-Augen-Prinzip für sichere Kommunikation und Zusammenarbeit – bei gleichzeitig unbeeinträchtigten Geschäftsprozessen.

IBM

Mit Guardium bietet **IBM** eine umfassende, flexibel anwendbare DLP-Lösung an, die kompetent und zukunftsweisend mit künstlicher Intelligenz und Post-Quantum Encryption unterstützt wird.

ManageEngine

Mit starkem Wachstum gelingt **ManageEngine** der Aufstieg vom „Rising Star“ zu einem Leader im deutschen Markt für DLP-Lösungen. Dazu tragen die leichtere Einhaltung von Vorschriften, die Vereinfachung durch Automatisierung sowie die einheitliche Analyse bei.

Microsoft

Durch Unterstützung für umfassenden Datenschutz sowie geschicktes Marketing – z.B. Integration und Bundling – baut **Microsoft** mit Purview seine Leader-Position im deutschen DLP-Markt aus.

Trellix

Eine umfassende Lösung für verschiedenste Datentypen und eine große Reichweite im deutschen Markt macht **Trellix** zu einem führenden Anbieter für Data Loss/Leakage Prevention Deutschland.

Anhang

Die Marktforschungsstudie „ISG Provider Lens® 2026 – Cybersecurity – Solutions and Services" analysiert die entsprechenden Softwareanbieter/Dienstleister im globalen Markt auf Basis eines mehrstufigen Marktforschungs- und Analyseprozesses und positioniert diese Anbieter auf Basis der ISG Research-Methodik.

Sponsor der Studie:
Heiko Henkes

Federführender Autor:
Frank Heuer

Editorin:
Maria Müller-de Haen

Forschungsanalystin:
Monica K

Datenanalysten:
Rajesh Chillappagari und Laxmi Sahebrao

Beratender Berater:
Marco Ezzy

Projektleiterin:
Smita S M

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.

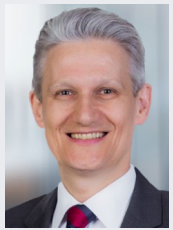
Die in diesem Bericht vorgestellten Marktforschungs- und Analysedaten umfassen Research-Informationen aus dem ISG Provider Lens® Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. Die für diesen Bericht erhobenen Daten und Informationen, entsprechen nach Ansicht von ISG sowohl für Anbieter, die aktiv teilgenommen haben, als auch für Anbieter, die nicht teilgenommen haben, dem aktuellen Stand vom Mai 2026. ISG ist sich darüber im Klaren, dass zwischenzeitlich eventuell Fusionen und Übernahmen stattgefunden haben; diese Veränderungen werden in diesem Bericht allerdings nicht berücksichtigt.

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

Die Studie wurde in folgenden Schritten durchgeführt:

1. Definition des Marktes für Cybersecurity – Solutions and Services
2. Fragebogenbasierte Studien über Dienstleister/Anbieter und zu allen Trendthemen
3. Interaktive Gespräche mit Dienstleistern/Anbietern über ihre Leistungen und Use Cases
4. Nutzung der ISG-internen Datenbanken sowie des Know-hows und der Erfahrung der ISG Advisors (soweit möglich)
5. Detaillierte Analyse und Evaluierung von Services und entsprechenden Dokumentationen auf Basis der von den Anbietern zur Verfügung gestellten Daten und Zahlen sowie anderer Quellen
6. Auswertung auf Basis der folgenden Kriterien:
   * Strategie und Vision
   * Innovationen
   * Markenbekanntheitsgrad und Marktpräsenz
   * Vertriebs- und Partnerlandschaft
   * Breite und Tiefe des Service-Angebots
   * Technologische Weiterentwicklungen

Autor



Frank Heuer
Principal Analyst

Frank Heuer ist Principal Analyst bei ISG Germany. Sein Schwerpunkt liegt auf den Themen Cybersecurity, Digital Workspace, Communication, Social Business & Collaboration sowie Cloud Computing.

Zu seinen Aufgabengebieten gehört vor allem die Beratung von ICT-Anbietern zum strategischen und operativen Marketing sowie Vertrieb. Herr Heuer ist als Sprecher bei Konferenzen und Webcasts zu seinen Themenschwerpunkten im Einsatz und Mitglied des IDG-Expertennetzwerks. Herr Heuer ist seit 1999 als Analyst und Berater im IT-Markt aktiv.

Enterprise Context und Global Overview Analyst

Monica K
Research Analyst

Monica K. ist Manager, Research bei ISG, wo sie auch als Digitalexpertin tätig ist. Sie ist Mitverfasserin der Provider Lens® Studien, des globalen zusammenfassenden Berichts und der Unternehmensperspektive für die Märkte Cybersicherheit, ESG und Nachhaltigkeit. Zu ihren Aufgaben gehören die Leitung umfassender Forschungsprojekte und die Zusammenarbeit mit internen Stakeholdern bei verschiedenen Beratungsinitiativen.

Mit mehr als einem Jahrzehnt Erfahrung in den Bereichen Technologie, Wirtschaft und Marktforschung bringt Monica wertvolles Fachwissen für ISG-Kunden mit. Zuvor arbeitete sie bei einem Forschungsunternehmen, das sich auf IoT, Produktentwicklung, Anbieterprofile und Talent Intelligence spezialisiert hat.

Sponsor der Studie

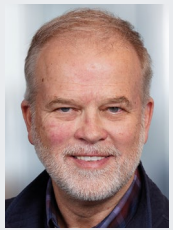
Heiko Henkes

Direktor und leitender Analyst

Heiko Henkes ist Director und Principal Analyst bei ISG und leitet das globale ISG Provider Lens® (IPL)-Programm für alle IT-Outsourcing (ITO)-Studien neben seiner Schlüsselrolle in der globalen IPL-Abteilung als strategischer Programmmanager und Vordenker für IPL-Lead-Analysten.

Henkes leitet Star of Excellence, die globale Kundenerfahrungsinitiative von ISG, und steuert das Programmdesign und dessen Integration mit IPL und ISGs Sourcing-Praxis. Seine Expertise liegt darin, Unternehmen durch IT-basierte Geschäftsmodelltransformationen zu führen, wobei er sein tiefes Verständnis für kontinuierliche Transformation, IT-Kompetenzen, nachhaltige Geschäftsstrategien und Change Management in einer Cloud-AI-getriebenen Geschäftslandschaft nutzt. Henkes ist bekannt für seine Beiträge als Keynote-Sprecher zum Thema digitale Innovation, in denen er Einblicke in die Nutzung von Technologie für Unternehmenswachstum und Transformation vermittelt.

IPL-Produktverantwortlicher



Jan Erik Aase

Partner und Global Head – ISG Provider Lens®

Herr Aase verfügt über umfangreiche Erfahrung bezüglich Implementierung und Research im Bereich Service- Integration und Management sowohl von IT- als auch von Geschäftsprozessen mit. Mit mehr als 35 Jahren Erfahrung ist er hochqualifiziert darin, Trends und Methoden der Vendor Governance zu analysieren, Ineffizienzen in aktuellen Prozessen zu identifizieren und als Berater tätig zu sein. Jan Erik hat Erfahrung auf allen vier Seiten des Sourcing- und Vendor-Governance- Lebenszyklus – als Kunde, als Branchenanalyst, als Dienstleister und als Berater.

Als Research Director, Principal Analyst und Global Leader des ISG Provider Lens® Programms ist er sehr gut in der Lage, den aktuellen Stand der Branche zu beurteilen und darüber zu berichten sowie Empfehlungen für Unternehmen und Service-Provider- Kunden auszusprechen.

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 finden hier eine Fülle von detaillierten Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Beschaffungspartner helfen. ISG-Berater nutzen die Berichte, um ihre eigenen Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG auszusprechen. 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 auch Marktforschung speziell über Anbieter für staatliche 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 Technologie-Segment mit Fokus auf KI. 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®

JUNI, 2026

BERICHT: CYBERSECURITY SERVICES AND SOLUTIONS