ISG Provider Lens™

# Cybersecurity – Solutions and Services

## Managed Security Services – SOC

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

Customized report courtesy of:

**QUADRANT REPORT | JULI 2024 | DEUTSCHLAND**

Inhaltsverzeichnis

*Autor des Berichts: Frank Heuer, Gowtham Sampath (SSE), und Dr. Maxime Martelli (XDR)*

**Künstliche Intelligenz und das Mittelstandssegment treiben den deutschen Cybersecurity-Markt**

Cyberbedrohungen nehmen für deutsche Unternehmen im Zuge immer raffinierterer, häufigerer, komplexerer und wandlungsfähigerer Cyberattacken zu. Durch den Mangel an qualifizierten Cybersecurity-Fachleute wird die Situation noch verschärft und die Nachfrage nach externen Dienstleistungen gefördert. Neue Technologien begünstigen Cyberbedrohungen, bieten zugleich aber auch neue Geschäftschancen für Dienstleister. Zusätzlich profitieren Serviceanbieter, wenn sie sich auf die Anforderungen verschiedener Zielgruppen verstehen.

Die Verantwortlichen in deutschen Unternehmen sind aktuell vor verschiedene Herausforderungen gestellt. Die verstärkten Cyberbedrohungen im Rahmen politischer Spannungen, wie des Ukraine-Kriegs, sowie der Trend zum Home Office – und selbstverständlich auch der langfristige Trend hin zur Digitalisierung – haben in Deutschland zu vergrößerten Angriffsflächen für Cyberattacken geführt, die entsprechender Gegenmaßnahmen bedürfen. Andererseits führt die schwache Konjunktur zu finanziellen Herausforderungen.

Geschäftsprozesse werden im Rahmen der Digitalisierung zunehmend in die IT verlagert. Auch geistiges Unternehmenseigentum wird immer mehr digital dargestellt. Folglich hat sich mit der steigenden Notwendigkeit, IT- und Kommunikationssysteme zu schützen, IT-Sicherheit zur Unternehmenssicherheit gewandelt. Die verstärkte Home-Office-Nutzung in Deutschland – und die dadurch bedingte externe Anbindung der Mitarbeiter – hat die IT-Systeme leichter angreifbar gemacht.

Neben der Digitalisierung und der vermehrten Remote-Arbeit hat die zunehmende Bereitstellung von Ressourcen aus der Cloud IT-Systeme angreifbarer gemacht und infolge zu einer steigenden Relevanz des Zero-Trust-Ansatzes und zum Bedeutungsverlust der

Der **Fachkräftemangel** fördert die Nachfrage nach externen Security-Dienstleistungen.

## Zusammenfassung

Perimetersicherheit geführt. Der Grundsatz „never trust, always verify" (nie vertrauen, immer überprüfen) bedeutet unter anderem gegenseitige Authentifizierung und kontinuierliche Überwachung des Netzwerks.

In immer kürzeren Abständen realisieren Cyberkriminelle neue, raffiniertere und komplexere Methoden, um die Cyberverteidigungssysteme von Unternehmen und Behörden zu überwinden. In der jüngsten Vergangenheit waren wieder einige spektakuläre Cyberattacken zu verzeichnen; aber auch nicht so prominente Angriffe – etwa durch Ransomware – machen Unternehmen zunehmend zu schaffen. Entsprechend müssen die Cybersecurity-Maßnahmen lückenlos auf dem neuesten Stand sein. Damit sind Unternehmen und Behörden nicht zuletzt durch den IT-Fachkräftemangel – speziell im Cybersecurity-Markt – immer mehr überfordert. Somit nehmen IT-Verantwortliche vermehrt externe Dienstleistungen, zum Beispiel Security Operations Center, in Anspruch. Diese Provider sowie auch viele IT-Security-Produktanbieter setzen, um selbst mit den Bedrohungen mithalten zu können, verstärkt auf proaktive statt reaktive Methoden, die zum Beispiel auf künstlicher Intelligenz basieren.

Nicht nur der Eigenschutz der Unternehmens, sondern auch gesetzliche Regelungen, wie die Datenschutz-Grundverordnung (DSGVO) in der EU, zwingen Unternehmen dazu, stärkere Sicherheitsmaßnahmen umzusetzen, um Cyberattacken vorzubeugen. Gerade für mittelständische Unternehmen stellt dies immer noch eine große Herausforderung dar.

Die mittelständischen Unternehmen sind andererseits aber auch in Deutschland ein interessantes Marktsegment für Cybersecurity-Anbieter. Mittelständler besitzen insgesamt gesehen weniger ausgereifte IT-Sicherheitssysteme als Großunternehmen, sind aber durch die oben beschriebenen Faktoren zu Nachrüstungen gezwungen. Dadurch haben sie einen großen Nachholbedarf und verzeichnen dementsprechend eine überdurchschnittlich stark wachsende Nachfrage nach Cybersecurity-Lösungen. Für Sicherheitsanbieter noch vorteilhafter ist eine ausgewogene Kundenstruktur aus Großunternehmen und Mittelstand, um auch von den umfangreichen Budgets der Large Accounts profitieren zu können. Die derzeit schwache Konjunktur in Deutschland lässt auch die Nachfrage nach Cybersecurity-Lösungen nicht unberührt, so dass der Mittelstand mit seiner überdurchschnittlich wachsenden Nachfrage zu einem immer attraktiveren Marktsegment wird, das aber auch adäquat adressiert werden will. Es reicht nicht aus, mittelständischen Kunden einfach einen Service für Großkunden anzubieten. Vielmehr muss der gesamte Go-to-Market-Ansatz – Produkte, Preise und Kommunikation – an diese Kunden angepasst werden. Kommunikation und kulturelle Aspekte sind besonders wichtig, um vom Mittelstand als Anbieter akzeptiert zu werden, der dieses Segment ernst nimmt.

IT-Verantwortliche kämpfen trotz der großen Bedeutung von Cybersicherheit wieder vermehrt mit der Aufgabe, Investitionen in Cybersicherheit gegenüber Stakeholdern des Unternehmens zu legitimieren, besonders gegenüber dem CFO. Die Rentabilität der Cybersecurity-Investitionen nachzuweisen ist anders als bei anderen IT-Projekten nicht immer möglich; auch Bedrohungsrisiken zu beziffern ist nicht einfach. Andererseits erkennen auch immer mehr Führungskräfte, dass Cyberattacken zu massiven – unter Umständen existenziellen – finanziellen und Imageschäden führen können. Demzufolge gewinnt die IT-Sicherheit in deutschen Unternehmen an Bedeutung, und die Führungsetage wird verstärkt in das Cyberrisikomanagement eingebunden.

Nach wie vor ist festzustellen, dass die Ursache für Cybersecurity-Vorfälle oft nicht (allein) auf der technischen Seite liegt. Vielmehr werden viele Angriffe durch unbedachtes Verhalten von Anwendern begünstigt, wie z.B. bei Phishing- und Trojaner-Angriffen. Neben einem zeitgemäßen IT-Sicherheitsequipment spielen daher Nutzerschulungen und Beratung weiterhin eine wichtige Rolle.

Beratung ist auch vermehrt hinsichtlich technischer Bedrohungen gefragt. Neben Cyberangriffen und -Lösungen auf Basis von künstlicher Intelligenz nimmt der Beratungsbedarf auch hinsichtlich quantum-basierender Angriffe zu. Diese stellen eine neue Qualität bei Angriffen auf die Verschlüsselung von vertraulichen Daten dar. Zwar spielen quantum-basierende Bedrohungen derzeit in

der Praxis noch keine Rolle, aber aufgrund der potenziell schwerwiegenden Folgen haben sich erste Dienstleister bereits mit ihrer Beratung darauf eingestellt. Diese Consulting-Angebote werden vor allem von Banken und Versicherungen in Anspruch genommen, da ihre Vermögenswerte aus virtuellen Assets bestehen und sie auf die neuen Bedrohungen frühzeitig vorbereitet sein wollen.

**Identity & Access Management (Produkte)**

Derzeit und auch in Zukunft ist IAM ein besonders wichtiges Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch vernetzte Maschinen (Industrie 4.0).

Zudem nimmt die Anzahl der Benutzer, Geräte und Dienste stetig zu und damit auch die Anzahl von digitalen Identitäten, die zu verwalten sind. Eine erhebliche Rolle spielt dabei die gestiegene Nutzung des Home Offices. Viele Mitarbeitende greifen remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden.

**Data Leakage/Loss Prevention & Data Security (Produkte)**

In Deutschland hat das Interesse an DLP-Lösungen in den letzten Jahren weiter deutlich zugenommen. Dazu tragen verschiedene Faktoren bei, welche die Sicherheit der Daten im Unternehmen berühren. So haben sich Daten und geistiges Eigentum zu immer wichtigeren und teilweise existenziell bedeutsamen Unternehmens-Assets entwickelt.

Darüber hinaus stellt die zunehmende geschäftliche Nutzung privater Endgeräte eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen.

**Strategic Security Services**

Deutsche Unternehmen sind angesichts der immer häufigeren, intensiveren wie auch raffinierteren Cyberattacken gefordert, ihre IT-Systeme vor Schaden zu bewahren. Schon lange sind hiervon nicht mehr nur die bekannten großen Unternehmen sowie Behörden betroffen, sondern zunehmend auch kleine und mittelgroße Firmen. Der Mangel an IT-Fachkräften erschwert zugleich diese Situation auch weiterhin.

Speziell mittelständische Unternehmen haben unter einem besonders starken Fachkräftemangel hinsichtlich Cybersecurity zu leiden. Sie stellen damit ein überdurchschnittlich wachsendes – und entsprechend zunehmend attraktives – Marktsegment dar.

**Technical Security Services**

Unternehmen und Behörden in Deutschland sind aufgrund immer raffinierterer Cyberangriffe und des drängenden Fachkräftemangels immer häufiger darauf angewiesen, externe Cybersecurity-Dienstleistungen in Anspruch zu nehmen, um ihre IT-Security-Systeme auf dem laufenden Stand zu halten.

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

**Managed Security Services – SOC**

Die immer anspruchsvolleren Cyberattacken fördern besonders auch die Nachfrage nach Managed Security Services von Security Operations Centers (SOCs). Der Mangel an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen machen diese Dienstleistungen zusätzlich für deutsche Unternehmen interessant.

Große und besonders auch mittelständische Kunden wissen SOCs mit deutschem oder EU-Standort aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen. Für beide Zielgruppen sind darüber hinaus auch integrierte Lösungen aus IT- und zugehörigen Security-Lösungen, End-to-End Security Services sowie eine hohe Innovationskraft 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.

Unternehmen setzen zunehmend auf Cloud-Anwendungen, Remote-Mitarbeitende und vernetzte Systeme, und im Zuge dieser Entwicklung haben Cyberbedrohungen an Komplexität und Raffinesse zugenommen. Solche dynamischen Umgebungen erfordern fortschrittliche Sicherheitsmaßnahmen, die über den traditionellen Perimeterschutz hinausgehen. Da Cyberbedrohungen immer raffinierter werden, ist die Einführung solcher hochmodernen Sicherheitsmaßnahmen für die Aufrechterhaltung einer starken Cybersicherheitslage unerlässlich.

Der Bedarf an hochentwickelten Cybersicherheitslösungen wie Extended Detection & Response (XDR) und Security Service Edge (SSE) wird durch die sich weiterentwickelnde Bedrohungslandschaft, die zunehmende Nutzung der Cloud und die erforderlichen umfassenden Sicherheits-Frameworks vorangetrieben. Diese innovativen Plattformen adressieren die kritischen Herausforderungen von Unternehmen und gewährleisten einen zuverlässigen und effizienten Schutz digitaler Ressourcen und Geschäftsabläufe.

Zu den bestehenden Herausforderungen zählen u.a. die folgenden:

**Komplexität der Sicherheitsarchitekturen:** Die Verwaltung unterschiedlicher Sicherheitstools und -lösungen kann zu Ineffizienzen und Schutzlücken führen; daher sind integrierte Plattformen wie XDR und SSE für einen optimierten Betrieb unerlässlich.

**Reaktive Erkennung von und Antwort auf Bedrohungen:** Herkömmliche Sicherheitsmaßnahmen bieten oft keine Transparenz und Reaktionsmöglichkeiten in Echtzeit. XDR arbeitet mit fortschrittlichen Analyse- und Automatisierungsfunktionen, um Bedrohungen an verschiedenen Endpunkten zu erkennen, zu untersuchen und darauf zu reagieren.

**Laxer Datenschutz und Governance:** Die Gewährleistung von Datenschutz und Governance in einer dezentralen IT-Umgebung ist eine Herausforderung. SSE bietet zentralisierte Sicherheitsrichtlinien und Governance Frameworks zur effektiven Verwaltung des Datenschutzes.

**Mangelnde Skalierbarkeit und Leistung:** Im Zuge des Unternehmenswachstums müssen Sicherheitslösungen entsprechend skalierbar sein, ohne die IT- oder Unternehmensleistung zu beeinträchtigen. XDR und SSE sollen skalierbare, leistungsstarke Sicherheit in umfangreichen und sich weiterentwickelnden IT-Landschaften bieten.

**Schlechte Nutzererfahrung:** Zuverlässige Sicherheit und eine nahtlose Benutzererfahrung müssen unbedingt in einem ausgewogenen Verhältnis stehen. Unternehmen benötigen innovative Lösungen, die so konzipiert sind, dass sie bei minimalen Störungen einen maximalen Schutz und Sicherheitsstatus bieten.

**Trends im Bereich Extended Detection & Response (XDR)**

Auf dem XDR-Markt sind diverse innovative Trends zur Verbesserung der Erkennung von Bedrohungen, der Reaktion darauf und der allgemeinen Sicherheitslage zu beobachten. XDR-Lösungen werden immer beliebter, denn sie können Daten über mehrere Sicherheitsebenen hinweg sammeln und korrelieren, u.a. E-Mails, Endpunkte, Server, Cloud-Workloads und Netzwerke, und so einen vielschichtigen Überblick über die Sicherheitslage des jeweiligen Unternehmens bieten.

Die wichtigsten Trends im XDR-Bereich sind nachstehend aufgeführt:

**Integration von KI und ML:** Einer der neuesten XDR-Trends ist die Integration von KI- und ML-Algorithmen, um die Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen zu verbessern. Dank dieser fortschrittlichen Technologien können XDR-Plattformen komplexe Bedrohungen erkennen, potenzielle Angriffe vorhersagen und Reaktionsmaßnahmen automatisieren; dadurch wird das Sicherheitsteam entlastet.

**Konvergenz mit anderen Sicherheitslösungen:** Ein weiterer neuer Trend ist die Konvergenz von XDR mit anderen Sicherheitslösungen wie Security Information & Event Management (SIEM) und Security Orchestration, Automation & Response (SOAR). Dadurch entsteht eine

einheitliche Sicherheitsarchitektur, die die Sichtbarkeit von Bedrohungen, deren Erkennung und die Reaktionszeiten verbessert und gleichzeitig die Sicherheitsabläufe effizienter gestaltet.

**Integration von Bedrohungsdaten (Threat Intelligence):** XDR-Plattformen werden zunehmend mit Bedrohungsdaten integriert, was die Erkennung von und Reaktion auf Bedrohungen verbessert. Durch die Kombination interner Sicherheitsdaten mit externen Bedrohungsdaten können XDR-Lösungen kontextbezogene Erkenntnisse über potenzielle Bedrohungen liefern. Dies hilft den Sicherheitsteams, fundierte Entscheidungen zu treffen und Prioritäten bezüglich ihrer Maßnahmen zu setzen.

**XDR für Cloud- und SaaS-Umgebungen:** Da Unternehmen immer häufiger Cloud- und SaaS-Anwendungen einsetzen, erweitern XDR-Lösungen ihre Abdeckung auf diese Umgebungen. Cloudnative XDR-Plattformen können Cloud-Workloads, Container und serverlose Anwendungen überwachen und sichern und bieten gleichzeitig einen Überblick über die Nutzung von SaaS-Anwendungen und potenzielle Risiken.

**Funktionen zur Erkennung von Bedrohungen und Gefahren (Threat & Compromise Detection):** XDR-Lösungen enthalten Funktionen zur Analyse des Benutzer- und Entitätsverhaltens (User & Entity Behavior Analysis, UEBA), um Insider-Bedrohungen und Account-Kompromittierungen zu erkennen. UEBA verwendet ML-Algorithmen zur Analyse von Benutzerverhaltensmustern und zur Identifizierung von Anomalien, die auf bösartige Aktivitäten hindeuten könnten, und hilft so Unternehmen, Bedrohungen zu erkennen und darauf zu reagieren, die andernfalls unbemerkt bleiben würden.

**XDR zur Verbesserung der Sicherheit von ICS- und OT-Umgebungen:** Da sich die Bedrohungslage für industrielle Kontrollsysteme (ICS) und OT-Umgebungen ständig weiterentwickelt, werden maßgeschneiderte XDR-Lösungen entwickelt, um die besonderen Sicherheitsanforderungen dieser Systeme zu erfüllen. XDR für ICS und OT kann Daten von speziellen industriellen Steuerungssystemen überwachen und analysieren, um Bedrohungen frühzeitig zu erkennen, eine schnelle Reaktion zu ermöglichen und so potenzielle Schäden zu minimieren.

**Unterstützung bei der Einhaltung von gesetzlichen Regelungen:** Angesichts der zunehmenden Bedeutung von Datenschutz- und Sicherheitsbestimmungen verbessern Unternehmen ihre XDR-Lösungen, um diese Compliance-Anforderungen zu erfüllen.

Unternehmen müssen sich in einer dynamischen Landschaft zurechtfinden, die durch die zunehmende Nutzung von Cloud-Umgebungen und sich neu entwickelnde Cyberbedrohungen gekennzeichnet ist und skalierbare, flexible und robuste Sicherheitslösungen erfordert. SSE-Lösungen gehen diese Herausforderungen an; sie bieten zentralisierte Transparenz, fortschrittliche Bedrohungserkennung durch KI und ML sowie eine nahtlose Durchsetzung von Richtlinien auf allen Endgeräten. Durch die Einführung von SSE können Unternehmen einen sicheren Zugriff auf Anwendungen und Daten von jedem beliebigen Standort aus gewährleisten, die Einhaltung gesetzlicher Vorschriften sicherstellen, sich gegen Datenschutzverletzungen und Insider-Bedrohungen absichern und so die Geschäftskontinuität und Resilienz angesichts einer sich ständig verändernden Bedrohungslandschaft unterstützen.

Die von SSE-Lösungen angegangenen Herausforderungen sind im Folgenden aufgeführt:

**Sicherheit von Cloud-Anwendungen:** Die zunehmende Verbreitung von Cloud-Diensten zieht komplexe Sicherheitsfragen nach sich. SSE zentralisiert Sicherheitsrichtlinien und erzwingt eine einheitliche Zugriffskontrolle für alle Cloud-Anwendungen.

**Sicherheit von Remote-Mitarbeitenden:** Mit der zunehmenden Zahl an Remote-Mitarbeitenden sind herkömmliche Sicherheitsmodelle auf Perimeterbasis nicht mehr so effektiv. SSE bietet sicheren und geräteunabhängigen Zugriff auf Cloud-Anwendungen von jedem Standort aus.

# Zusammenfassung

**Data Loss Prevention (DLP):** Datenschutzverletzungen und Datenlecks sind ein großes Problem. SSE setzt DLP-Richtlinien und Datenverschlüsselung über Cloud-Dienste hinweg durch und hilft so dabei, das Exfiltrieren sensibler Daten zu verhindern.

**Schatten-IT:** Mitarbeitende nutzen häufig nicht genehmigte Cloud-Anwendungen. SSE bietet Einblick in die Nutzung dieser Schatten-IT und ermöglicht eine sichere Zugriffskontrolle auch für nicht bewilligte Anwendungen.

**Komplexes Sicherheitsmanagement:** Die Verwaltung mehrerer Sicherheitslösungen kann komplex und zeitaufwendig sein. SSE bietet eine einheitliche Plattform für das Management von Sicherheitsrichtlinien über alle Cloud-Anwendungen hinweg.

Der SSE-Markt wächst gerade aufgrund der zunehmenden Nutzung von Cloud-Anwendungen und Remote-Arbeitskräften sowie des Bedarfs an einem konsolidierten Sicherheitsansatz beträchtlich.

Die wichtigsten Trends, die den Markt prägen, sind die folgenden:

**Cloudnative Architekturen:** Mit dem Umstieg auf Cloud-Umgebungen kommen cloudnative Sicherheitslösungen zum Einsatz, die mit den Workloads skalieren und dynamische, verteilte Konfigurationen unterstützen.

**Konvergenz von Sicherheit und Vernetzung:** Der Trend geht immer mehr in Richtung integrierter Netzwerk- und Sicherheitsfunktionen in einer einzigen Plattform, um den Betrieb zu optimieren und die Komplexität der Verwaltung von Sicherheit und Netzwerkleistung zu reduzieren.

**Integration von SWGs und CASBs:** Secure Web Gateways (SWGs) und Cloud Access Security Broker (CASBs) verschmelzen zu umfassenden SSE-Lösungen, die einheitlichen Bedrohungsschutz, DLP und Zugriffskontrolle für Cloud-Dienste bieten.

**Schwerpunkt auf Zero-Trust-Sicherheit:** SSE-Lösungen beinhalten zunehmend Zero-Trust-Prinzipien, d.h. die Gewährung von Zugang auf Basis der geringsten Rechte und einer kontinuierlichen Überprüfung; das minimiert die Angriffsfläche und die laterale Bewegung im Netzwerk und verbessert so die Sicherheit.

**SASE-Nutzung:** SSE ist ein Grundelement von Secure Access Service Edge (SASE)-Architekturen, die Netzwerksicherheit und Cloud-Zugangssicherheit in einen einheitlichen Cloud-Dienst integrieren.

**Integration von KI und ML:** SSE-Lösungen nutzen KI und ML, um die Erkennung von Bedrohungen zu automatisieren, die Identifizierung von Anomalien zu verbessern und Sicherheitsrichtlinien auf Basis des Benutzerverhaltens zu personalisieren.

**Fokus auf User Experience:** Es ist entscheidend, Sicherheit und User Experience (UX) in Balance zu halten. SSE-Lösungen sind so konzipiert, dass sie für die Benutzer transparent sind und ihre Arbeitsabläufe nur minimal stören, aber gleichzeitig die Sicherheit gewährleistet ist.

**Einheitliche Managementkonsolen:** Ein Trend geht hin zur Entwicklung einheitlicher Managementschnittstellen, die verschiedene Sicherheitsfunktionen in einem einzigen Dashboard konsolidieren, die Verwaltung vereinfachen und eine ganzheitliche Sicht auf die Sicherheitslandschaft bieten.

**Analyse des Benutzer- und Entitätsverhaltens (UEBA):** UEBA-Tools (User & Entity Behavior Analysis) analysieren das Verhalten von Benutzern und Entitäten, um so potenzielle Sicherheitsbedrohungen zu erkennen. UEBA legt Basiswerte fest, erkennt entsprechende Abweichungen und hilft so, anomale Aktivitäten zu identifizieren.

**Identitätsorientierte Sicherheit:** Das Identitäts- und Zugriffsmanagement (Identity & Access Management, IAM) entwickelt sich zum zentralen Bestandteil von Sicherheitsstrategien, um zu gewährleisten, dass nur authentifizierte und autorisierte Benutzer auf Ressourcen zugreifen können.

In dem Maße, in dem Unternehmen eine robuste Cybersicherheit in den Vordergrund stellen und sich in komplexen digitalen Umgebung zurechtfinden müssen, werden innovative Lösungen wie XDR und SSE zum Schutz der digitalen Unternehmenswerte besonders stark nachgefragt werden. Cyberbedrohungen werden immer raffinierter, und Unternehmen stützen sich zunehmend auf Cloud-Dienste; damit spielen XDR und SSE für die Unternehmenssicherheit eine Schlüsselrolle.

## Zusammenfassung

Künstliche Intelligenz und Quantumtechnologie bedeuten neue Bedrohungen für Anwender, aber auch neue Chancen für Cybersecurity-Dienstleister. Vorteile haben dabei Serviceanbieter, die sowohl die Großunternehmen mit ihren großen Budgets als auch die Mittelständler mit ihrer dynamisch wachsenden Nachfrage adressieren.

# Anbieterpositionierung

**Seite 1 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Absolute Software | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Accenture | Not In | Not In | Not In | Not In | Leader | Leader | Leader | Not In |
| Acronis | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Alice&Bob.Company | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In |
| All for One Group | Not In | Not In | Not In | Not In | Contender | Contender | Not In | Not In |
| Axians | Not In | Not In | Not In | Not In | Leader | Leader | Leader | Leader |
| BAYOOSOFT | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Bechtle | Not In | Not In | Not In | Not In | Leader | Market Challenger | Leader | Leader |
| Beta Systems | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| BeyondTrust | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

# Anbieterpositionierung

**Seite 2 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Bitdefender | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In |
| BlackBerry | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In |
| Brainloop | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Broadcom | Product Challenger | Leader | Leader | Product Challenger | Not In | Not In | Not In | Not In |
| CANCOM | Not In | Not In | Not In | Not In | Leader | Market Challenger | Leader | Leader |
| Capgemini | Not In | Not In | Not In | Not In | Leader | Leader | Leader | Not In |
| Cato Networks | Not In | Not In | Not In | Leader | Not In | Not In | Not In | Not In |
| CGI | Not In | Not In | Not In | Not In | Not In | Product Challenger | Contender | Contender |
| Check Point Software | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| Cisco | Not In | Not In | Market Challenger | Leader | Not In | Not In | Not In | Not In |

# Anbieterpositionierung

**Seite 3 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Cloudflare | Not In | Not In | Not In | Market Challenger | Not In | Not In | Not In | Not In |
| Computacenter | Not In | Not In | Not In | Not In | Leader | Leader | Product Challenger | Contender |
| Controlware | Not In | Not In | Not In | Not In | Leader | Market Challenger | Leader | Leader |
| CoSoSys (Netwrix) | Not In | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Cross Identity | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| CrowdStrike | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In |
| CyberArk | Rising Star ★ | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Cybereason | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| DATAGROUP | Not In | Not In | Not In | Not In | Not In | Not In | Market Challenger | Leader |
| Deloitte | Not In | Not In | Not In | Not In | Product Challenger | Leader | Product Challenger | Not In |

# Anbieterpositionierung

**Seite 4 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Deutsche Telekom | Not In | Not In | Not In | Not In | Leader | Leader | Leader | Leader |
| DIGITALL | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In |
| DriveLock | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| DXC Technology | Not In | Not In | Not In | Not In | Leader | Product Challenger | Contender | Not In |
| Ericom Software | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In |
| ESET | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In |
| Eviden | Leader | Not In | Not In | Not In | Leader | Leader | Leader | Not In |
| EY | Not In | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In |
| Fidelis Cybersecurity | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| Forcepoint | Not In | Leader | Not In | Leader | Not In | Not In | Not In | Not In |

# Anbieterpositionierung

**Seite 5 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Fortinet | Contender | Not In | Leader | Product Challenger | Not In | Not In | Not In | Not In |
| Fortra | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| GBS | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| glueckkanja | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger |
| Google | Not In | Contender | Not In | Not In | Not In | Not In | Not In | Not In |
| HCLTech | Not In | Not In | Not In | Not In | Rising Star ★ | Product Challenger | Leader | Product Challenger |
| HiSolutions | Not In | Not In | Not In | Not In | Not In | Product Challenger | Not In | Not In |
| HPE (Aruba) | Not In | Not In | Not In | Contender | Not In | Not In | Not In | Not In |
| IBM | Leader | Leader | Leader | Not In | Leader | Leader | Leader | Not In |
| iboss | Not In | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In |

# Anbieterpositionierung

**Seite 6 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| iC Consult | Not In | Not In | Not In | Not In | Contender | Not In | Not In | Not In |
| Imprivata | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| IN Groupe | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| indevis | Not In | Not In | Not In | Not In | Product Challenger | Not In | Contender | Market Challenger |
| InfoGuard | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger |
| Infosys | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Leader | Not In |
| itWatch | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Kaspersky | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| KPMG | Not In | Not In | Not In | Not In | Not In | Leader | Not In | Not In |
| Kyndryl | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Not In | Not In |

# Anbieterpositionierung

**Seite 7 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Logicalis | Not In | Not In | Not In | Not In | Contender | Contender | Product Challenger | Product Challenger |
| Lookout | Not In | Not In | Not In | Contender | Not In | Not In | Not In | Not In |
| LTIMindtree | Not In | Not In | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger |
| ManageEngine | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Materna Radar | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Rising Star ★ | Product Challenger |
| Matrix42 | Not In | Leader | Not In | Not In | Not In | Not In | Not In | Not In |
| Microsoft | Leader | Leader | Leader | Market Challenger | Not In | Not In | Not In | Not In |
| Netskope | Not In | Product Challenger | Not In | Leader | Not In | Not In | Not In | Not In |
| Nevis | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| NTT DATA | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Product Challenger | Product Challenger |

# Anbieterpositionierung



| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Okta | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Omada | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| One Identity (OneLogin) | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Open Systems | Not In | Not In | Not In | Contender | Not In | Not In | Not In | Not In |
| OpenText | Contender | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Oracle | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Orange Cyberdefense | Not In | Not In | Not In | Not In | Market Challenger | Product Challenger | Leader | Not In |
| Palo Alto Networks | Not In | Not In | Leader | Leader | Not In | Not In | Not In | Not In |
| pco | Not In | Not In | Not In | Not In | Not In | Not In | Not In | Contender |
| Perimeter 81 | Not In | Not In | Not In | Market Challenger | Not In | Not In | Not In | Not In |

# Anbieterpositionierung



| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Ping Identity | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Proofpoint | Not In | Market Challenger | Not In | Contender | Not In | Not In | Not In | Not In |
| Rapid7 | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| RSA | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| SailPoint | Leader | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| SAP | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Saviynt | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Secureworks | Not In | Not In | Product Challenger | Not In | Not In | Contender | Not In | Not In |
| SenseOn | Not In | Not In | Contender | Not In | Not In | Not In | Not In | Not In |
| SentinelOne | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In |

# Anbieterpositionierung

**Seite 10 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Skyhigh Security | Not In | Product Challenger | Not In | Rising Star ★ | Not In | Not In | Not In | Not In |
| SolarWinds | Contender | Not In | Not In | Not In | Not In | Not In | Not In | Not In |
| Sophos | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| Sopra Steria | Not In | Not In | Not In | Not In | Not In | Market Challenger | Market Challenger | Market Challenger |
| suresecure | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Product Challenger | Rising Star ★ |
| Syntax | Not In | Not In | Not In | Not In | Product Challenger | Not In | Product Challenger | Product Challenger |
| TCS | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Leader | Not In |
| Tech Mahindra | Not In | Not In | Not In | Not In | Product Challenger | Product Challenger | Product Challenger | Product Challenger |
| TEHTRIS | Not In | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In |
| Thales | Market Challenger | Not In | Not In | Not In | Not In | Not In | Not In | Not In |

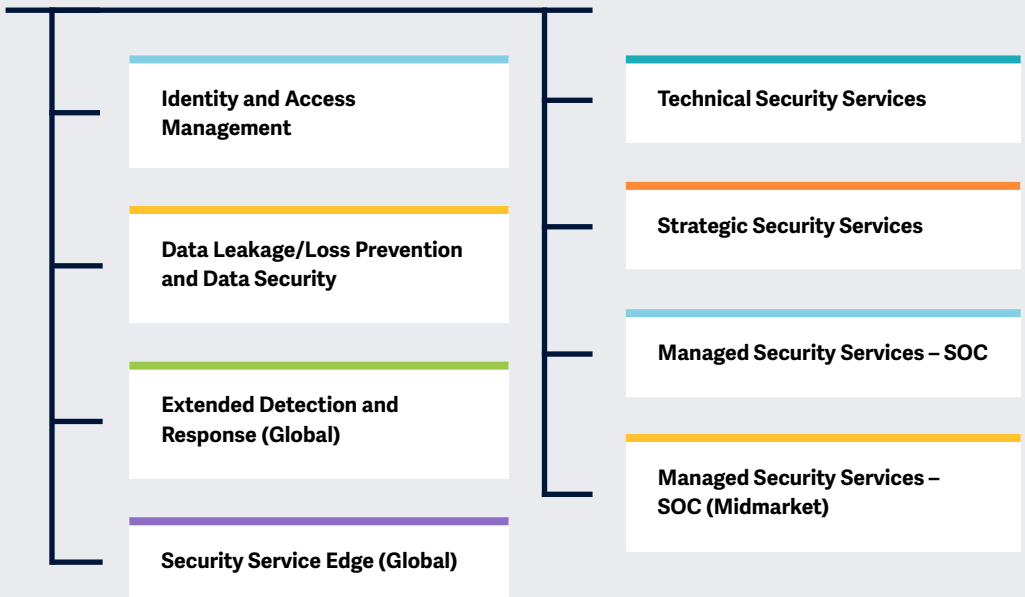
# Anbieterpositionierung

**Seite 11 von 11**

| | Identity and Access Management | Data Leakage/ Loss Prevention and Data Security | Extended Detection and Response (Global) | Security Service Edge (Global) | Technical Security Services | Strategic Security Services | Managed Security Services – SOC | Managed Security Services – SOC (Midmarket) |
|---|---|---|---|---|---|---|---|---|
| Trellix | Not In | Leader | Rising Star ★ | Not In | Not In | Not In | Not In | Not In |
| Trend Micro | Not In | Not In | Leader | Not In | Not In | Not In | Not In | Not In |
| Unisys | Not In | Not In | Not In | Not In | Market Challenger | Market Challenger | Market Challenger | Not In |
| Varonis | Not In | Product Challenger | Not In | Not In | Not In | Not In | Not In | Not In |
| Verizon Business | Not In | Not In | Not In | Not In | Not In | Contender | Product Challenger | Not In |
| Versa Networks | Not In | Not In | Not In | Leader | Not In | Not In | Not In | Not In |
| Wavestone | Not In | Not In | Not In | Not In | Not In | Rising Star ★ | Not In | Not In |
| Wipro | Not In | Not In | Not In | Not In | Product Challenger | Leader | Product Challenger | Not In |
| Zscaler | Not In | Rising Star ★ | Not In | Leader | Not In | Not In | Not In | Not In |

Untersuchte Schwer-punktthemen der Studie **„Cybersecurity – Solutions and Services 2024“**

Vereinfachte Illustration; Quelle: ISG 2024




**Definition**

**Cybersicherheit im Zeitalter der künstlichen Intelligenz**

Die aktuelle Cybersicherheitslandschaft erlebt im Zuge neuer Bedrohungen, technologischer Fortschritte und gesetzlicher Vorschriften 2024 eine rasche Weiterentwicklung.

Aus Cybersicherheitssicht kann man das Jahr 2023 angesichts deutlich raffinierterer und schwererer Angriffe als herausfordernd bezeichnen. Zahlreiche Unternehmen haben daraufhin ihre Investitionen in die Cybersicherheit erhöht und entsprechenden Initiativen zur Verhinderung von Angriffen und zur Verbesserung ihres Sicherheitsstatus eine hohe Priorität eingeräumt. Führungskräfte und Unternehmen aller Größen und Branchen haben aus den jüngsten Angriffen ihre Lektion gelernt und in entsprechende Maßnahmen zur Abwehr von Cyberbedrohungen investiert. Die Herausforderungen und Chancen, die mit künstlicher Intelligenz (KI) einhergehen, sind in diesem Zusammenhang besonders erwähnenswert.

Auf Unternehmensseite haben selbst kleinere Betriebe erkannt, dass sie anfällig für Cyberbedrohungen sind. Auch das erhöht die Nachfrage nach (gemanagten) Sicherheits- und Cyber-Resiliency-Lösungen. Dienstleister und Hersteller offerieren daher vermehrt Services und Lösungen zur Unterstützung der Wiederherstellung und der Aufrechterhaltung des Geschäftsbetriebes.

Security Service Provider helfen ihren Kunden, sich in der Cybersecurity-Landschaft zurechtzufinden. Es gilt vor allem, wachsam zu sein, um neue Bedrohungen zu erkennen und abzuschwächen, die transformativen Auswirkungen von Technologien wie KI zu verstehen und sich auf die neu entstehenden rechtlichen Rahmenbedingungen für den Datenschutz, wie NIS-2 in der Europäischen Union, einzustellen.

Cyberkriminelle nutzten großflächige Schwachstellen aus; mit beständigen Ransomware-Angriffen wurde versucht, Geschäftsaktivitäten zu stören, insbesondere im Gesundheitswesen, in der industriellen Lieferkette und im öffentlichen Dienst.

Unternehmen investierten infolgedessen in Funktionen wie Identitäts- und Zugriffsmanagement (IAM), Data Loss Prevention (DLP), Managed Detection & Response (MDR) und die Absicherung der Cloud und der Endpunkte. Der Markt verlagert sich hin zu integrierten Lösungen wie Security Service Edge (SSE) und Extended Detection & Response (XDR). Anhand der besten Tools, mit Experten und ergänzender verhaltens- und kontextbezogener Intelligenz und Automatisierung soll der Sicherheitsstand verbessert werden.

**Betrachtungsumfang der Studie**

Dieser ISG Provider Lens™-Quadrantenbericht deckt die folgenden 8 Quadranten für Dienstleistungen/Lösungen ab:

Identity & Access Management, Data Leakage/Loss Prevention & Data Security, Technical Security Services, Strategic Security Services, Managed Security Services – SOC, Managed Security Services – SOC (Midmarket). Die Anbieter von Security Service Edge (SSE)-Lösungen sowie von Extended Detection & Response (XDR) werden in dieser Studie in diesem Jahr aus einer globalen Perspektive analysiert und positioniert, nicht aus der Perspektive einzelner Länder und Regionen, da sich diese Märkte derzeit noch im Anfangsstadium und Reifungsprozess befinden.

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

- Transparenz über die Stärken und Schwächen der relevanten Dienstleister 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 von IT-Dienstleistern 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 Millionen 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 Stars 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.

# Managed Security Services – SOC

**Wer sollte dieses Kapitel lesen**

Dieser Bericht ist relevant für deutsche Unternehmen, um sich über den Markt für Managed Security Services (MSS) zu informieren, damit sie fundierte Entscheidungen bei der Auswahl von MSS-Anbietern treffen können, die ihren individuellen Sicherheitsanforderungen gerecht werden.

Der ISG-Bericht bietet Einblicke in kritische Marktherausforderungen und geht darauf ein, wie die einzelnen Anbieter diese angehen, so dass Unternehmen die Fähigkeiten der MSS-Anbieter bei der Erfüllung ihrer Sicherheitsanforderungen bewerten können.

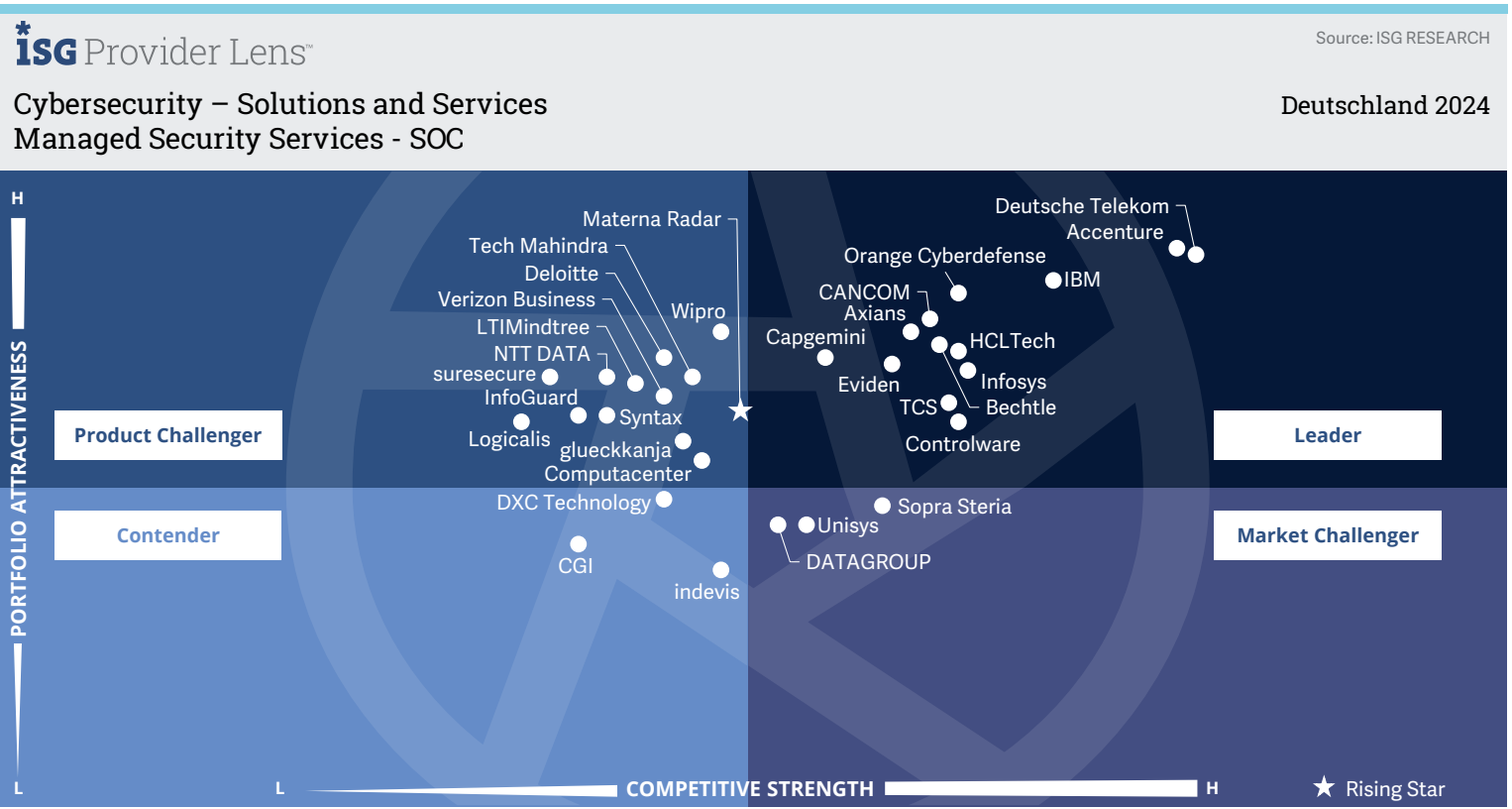
Deutsche Unternehmen wünschen sich robuste Sicherheitslösungen, um der zunehmenden Zahl von Cyberbedrohungen zu begegnen, insbesondere im Hinblick auf Remote-Arbeit und cloudbasierte Dienste. Sie benötigen kontinuierliche Überwachung, Funktionen zur Erkennung von hochkomplexen Bedrohungen sowie Unterstützung bei der Reaktion auf Vorfälle und bei der Behebung von Problemen, um die Geschäftskontinuität sicherzustellen und ihre wertvollen Daten und Systeme vor Ransomware-Angriffen zu schützen.

Die Dienstleistungen der MSS-Provider auf dem deutschen Markt sind auf diese Bedürfnisse zugeschnitten; sie umfassen u.a. Managed Detection & Response (MDR), fortschrittliche Analysen, KI, ML und Deep Learning-Techniken für verhaltensbasierte Bedrohungsanalysen sowie Threat Intelligence as a Service. MSS-Anbieter adressieren die wachsende Nachfrage nach Zero-Trust und SASE Frameworks und stellen sicher, dass Unternehmen Zugang zu den neuesten Sicherheitstechnologien und Fachkenntnissen haben, um ihren Geschäftsbetrieb vor den sich entwickelnden Bedrohungen zu schützen.

**Chief Information Security Officers** sollten diesen Bericht lesen, um einen Einblick in die aktuelle Marktlandschaft der MSS-Anbieter zu erhalten und so fundierte Entscheidungen treffen zu können.

**Chief Technology Officers** können anhand dieses Berichts die potenziellen Auswirkungen von MSS auf die technologische Infrastruktur ihres Unternehmens bewerten.

**Risiko- und Compliance-Verantwortliche** gewinnen aus diesem Bericht Einblicke in aktuelle Sicherheitstrends und -vorschriften und können so sicherstellen, dass die Sicherheitsvorkehrungen ihres Unternehmens die Branchenstandards und gesetzlichen Anforderungen erfüllen.




In diesem Quadranten geht es um die **relevantesten** Anbieter von **Managed Security Services aus SOCs** auf dem deutschen Markt, ohne Dienstleister, die ihre Leistungen nur auf eigene Produkte beziehen. Bedrohungslage und Fachkräftemangel **treiben** den Markt.

*Frank Heuer*

**Definition**

Die im Managed Security Services – SOC- (MSS-SOC-) Quadranten bewerteten Anbieter offerieren Leistungen für die kontinuierliche Überwachung von IT- und OT-Sicherheitsinfrastrukturen sowie das Management der IT- und OT-Infrastruktur für einen oder mehrere Kunden durch ein Security Operations Center (SOC). **Dieser Quadrant untersucht Dienstleister, die sich nicht ausschließlich auf proprietäre Produkte fokussieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können.** Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Lösung von Problemen.

Die Nachfrage nach Anbietern, die Unternehmen dabei unterstützen, ihre IT-Sicherheit insgesamt zu verbessern und die Wirksamkeit ihrer Sicherheitsprogramme durch kontinuierliche Verbesserungen langfristig zu maximieren, steigt. MSS-SOC Provider müssen traditionelle Managed Security Services mit Innovationen zusammenführen, um die Sicherheit ihrer Kunden mit einem integrierten Cyber-Abwehrmechanismus stärken zu können. Sie sollten in der Lage sein, Managed-Detection-&-Response-Dienste (MDR) zu erbringen, und über die neuesten Technologien und Infrastrukturen verfügen. Auch Fachwissen in den Bereichen Threat Hunting und Incident Management muss vorhanden sein, um Unternehmen bei der aktiven Erkennung von und Reaktion auf Bedrohungen durch Abwehr und Eindämmung zu unterstützen. Um die steigenden Kundenerwartungen in Bezug auf die proaktives Threat Hunting erfüllen zu können, bauen die Anbieter ihre SOC-Umgebungen mit Sicherheitsintelligenz aus und tätigen erhebliche Investitionen in Technologien wie Automatisierung, Big Data, Analytik, KI und Machine Learning. Diese hochmodernen SOCs unterstützen von Experten gesteuerte Reaktionen auf Sicherheitsinformationen und bieten den Kunden gleichzeitig einen ganzheitlichen und einheitlichen Ansatz für Sicherheit auf hohem Niveau.

Auswahlkriterien

1. Typische Leistungen wie **Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests** und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen
2. Angebot von Sicherheitsdiensten wie **Vorbeugung und Erkennung, Security Information & Event Management (SIEM)** sowie Sicherheitsberatung und Audits, entweder remote oder vor Ort beim Kunden
3. **Akkreditierungen** von Anbietern von Security Tools
4. Management eigener SOCs
5. **Zertifizierte Mitarbeiter**, z.B. mit Zertifizierungen wie Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)
6. Verfügbarkeit verschiedener Preismodelle

**Observations**

Die Nachfrage nach Managed Security Services durch Security Operations Centers (SOCs) wird durch immer raffiniertere, häufigere, komplexere und wandlungsfähigere Cyberattacken gefördert. Der Mangel an qualifizierter Fachleuten und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich 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. In dieser Zielgruppe werden zudem häufig individuell zugeschnittene Lösungen für die speziellen Anforderungen erwartet.

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

Generell wird zudem von den Anbietern eine hohe Innovationskraft erwartet, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Erweiterung der SOCs in Richtung Cyber Defense Centers, wobei den immer komplexeren Bedrohungen auch mit künstlicher Intelligenz und Automatisierung begegnet wird. Neben reaktiven Maßnahmen gewinnen zudem proaktive Leistungen zur Vorbeugung an Bedeutung. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen zunehmend interessant.

Von den 85 Anbietern, die in dieser Studie bewertet wurden, konnten sich 32 für diesen Quadranten qualifizieren. Dabei erreichten dreizehn eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

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 Managed Security/SOC Services.

axians

Mit umfangreichen, kundenorientierten Leistungen ist **Axians IT Security** im deutschen Markt für Managed Security/SOC Services zunehmend erfolgreich.

BECHTLE

**Bechtle** überzeugt seine Kunden mit umfangreichen, zertifizierten sowie modular anpassungsfähigen Managed Security/SOC Services und positioniert sich so als Leader in Deutschland.

CANCOM

Mit einem wachsenden Angebot an Managed Security, das ein breites Spektrum an gemanagten Technologien abdeckt, und SOC Services made in Germany profiliert sich **CANCOM** als Leader im deutschen Markt.

Capgemini

**Capgeminis** Erfolg im deutschen Markt für Managed Security/SOC 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 Managed Security/SOC Services bei.

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

**Eviden (an Atos Business)** punktet mit einem umfangreichen Angebot, innovativen Ansätzen und mit der globalen Verfügbarkeit seiner Managed Security/SOC Services.

Für **HCLTech** zahlt sich das starke Engagement im deutschen Markt für Managed Security/SOC Services aus. Unter anderem werden mehrere dedizierte Security Operations Centers hierzulande betrieben.

**IBM** kombiniert die eigene leistungsstarke Technologie mit umfassenden, global verfügbaren Managed Security/SOC Services zum Vorteil international aktiver Großkunden.

**Infosys** hat umfangreiche Ressourcen, entwickelt seine Managed Security/SOC Services kontinuierlich zum Vorteil seiner Großkunden weiter und positioniert sich damit als Leader für diese Dienstleistungen.

**Orange Cyberdefense** punktet mit europäischer Herkunft, globaler und lokaler Präsenz sowie kontinuierlich optimierten Managed Security/SOC Services.

Kosteneffiziente Lösungen, weltweite Präsenz und umfangreiche Technologieabdeckung, inklusive OT-Sicherheit, machen **TCS** zu einem Leader im deutschen Markt für Managed Security/SOC Services.

**Materna Radar** ist der neue „Rising Star" für Managed Security/SOC Services in Deutschland. Dazu trugen die geschickte Erweiterung des Geschäftes von Materna und auf europäischer Technologie basierende Dienste bei.

Leader

„Mit ihren umfassenden Managed Security/SOC Services, ihrem großen qualifizierten Team und dem Betrieb in Deutschland überzeugt die Deutsche Telekom als führender Anbieter."

*Frank Heuer*

# Deutsche Telekom

**Übersicht**

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 204.200 Mitarbeitende in über 87 Niederlassungen in mehr als 50 Ländern. Im Geschäftsjahr 2023 erwirtschaftete das Unternehmen einen Umsatz von 112,0 Milliarden €. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom") innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security rund 1.700 Mitarbeitende. Das SOC kombiniert auf maschinellem Lernen basierende künstliche Intelligenz, Verhaltensanalysen und Threat Hunting.

**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 Deutsche 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 besonders von vielen Mittelstandskunden geschätzt und auch allgemein 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.

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

**Herausforderungen**

Im Gegensatz zu vielen Wettbewerbern kann die Deutsche Telekom spezielle Kompetenzen hinsichtlich des Mittelstandes vorweisen. Dennoch liegt der Schwerpunkt der Managed Security/SOC Services weiterhin noch auf Großkunden, weniger auf dem Segment der Mittelstandskunden, dessen Nachfrage überdurchschnittlich wächst. Ein Ausbau in dieser Zielgruppe könnte lohnenswert sein.

# Star of Excellence

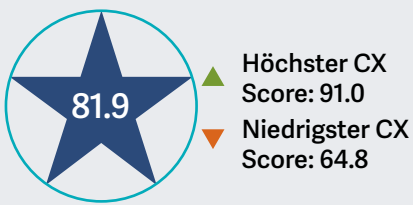
Ein von ISG entwickeltes Programm zur Sammlung von Kundenfeedback über den Erfolg von Anbietern bei der Demonstration höchster Standards im Bereich der Kundenbetreuung und Kundenorientierung.

Quelle: ISG Star of Excellence™ Research-Programm, Insights bis June 2024

Im Rahmen der ISG Star of Excellence™-Marktforschung zur Kundenerfahrung (Customer Experience, CX) in Unternehmen haben Kunden Feedback zu ihren Erfahrungen mit Dienstleistern für ihre **Cybersecurity Solutions and Services** gegeben.

Auf Basis des direkten Feedbacks von Unternehmenskunden werden im Folgenden die wichtigsten Punkte genannt:

### Durchschnittlicher CX-Wert der Branche




▲ Höchster CX Score: 91.0

▼ Niedrigster CX Score: 64.8

*CX Score: 100 am zufriedensten, 0 am wenigsten zufrieden. Antworten insgesamt (N) = 419*

### Kundenrolle im Unternehmen

▲ **Am zufriedensten**
Information Technology

▼ **Am wenigsten zufrieden**
Human Resources

### Region

▲ **Am zufriedensten**
Africa

▼ **Am wenigsten zufrieden**
Eastern Europe

### Branche

▲ **Am zufriedensten**
Chemicals

▼ **Am wenigsten zufrieden**
Public sector

### Wichtigste CX-Säule

**Execution and Delivery**

| Service Delivery Modelle | % der geleisteten Arbeit im Durchschnitt |
|---|---|
| Onsite | 53.6% |
| Nearshore | 21.6% |
| Offshore | 24.8% |

# Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2024 – Cybersecurity – Solutions and Services" analysiert die entsprechenden Softwareanbieter/Dienstleister im deutschen Markt auf Basis eines mehrstufigen Marktforschungs- und Analyseprozesses und positioniert diese Anbieter auf Basis der ISG Research-Methodik.

**Sponsor der Studie:**
Heiko Henkes

**Federführender Autor:**
Frank Heuer, Gowtham Sampath, und Dr. Maxime Martelli

**Editorin:**
Maria Müller-de Haen

**Forschungsanalysten:**
Monica K

**Datenanalyst:**
Rajesh Chillappagari und Laxmi Sahebrao

**Beratende Berater:**
Roger Albrecht

**Projektleiter:**
Shreemadhu Rai B

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

Die in diesem Bericht vorgestellten Marktforschungs- und Analysedaten umfassen Research-Informationen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit.

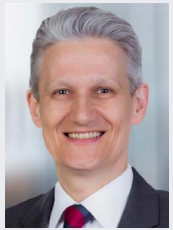
ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. Die für diesen Bericht erhobenen Daten und Informationen, entsprechen nach Ansicht von ISG sowohl für Anbieter, die aktiv teilgenommen haben, als auch für Anbieter, die nicht teilgenommen haben, dem aktuellen Stand vom Mai 2024. Zwischenzeitliche Fusionen und Akquisitionen und die damit zusammenhängenden Veränderungen sind in diesem Bericht nicht berücksichtigt.

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

Dabei wurde die Studie in folgende Schritte gegliedert:

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. Nutzung der Star of Excellence CX-Daten
6. Detaillierte Analyse und Evaluierung von Services und entsprechenden Dokumentationen auf Basis der von den Anbietern zur Verfügung gestellten Daten und Zahlen sowie anderer Quellen
7. Auswertung auf Basis der folgenden Kriterien:
   * Strategie & Vision
   * Technologische Innovationen
   * Markenbekanntheitsgrad und Marktpräsenz
   * Vertriebs- und Partnerlandschaft
   * Breite und Tiefe des Service-Angebots
   * CX und Empfehlung

*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.

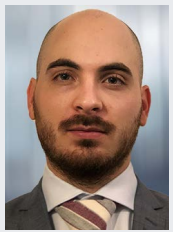
Zu seinen Aufgabengebieten gehört vor allem die Beratung von ICT-Anbietern zum strategischen und operativen Marketing sowie Vertrieb. Herr Heuer ist als Sprecher bei Konferenzen und Webcasts zu seinen Themenschwerpunkten im Einsatz und Mitglied des IDG-Expertennetzwerks. Herr Heuer ist seit 1999 als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

*Autor (SSE)*

## Gowtham Kumar Sampath
**Assistant Director & Lead Analyst**

Gowtham Sampath ist Assistant Director bei ISG Research und verantwortlich für die Erstellung seiner ISG Provider Lens™ Quadrantenberichte für die Bereiche Banking Technology/Platforms, Digital Banking Services, Cybersecurity sowie Analytics Solutions & Services. Gowtham verfügt über 15 Jahre Marktforschungserfahrung; seine Analysen sollen die Lücke zwischen Datenanalyseanbietern und Unternehmen schließen und gehen auf Marktchancen und Best Practices ein.

In dieser Funktion arbeitet er auch mit Beratern zusammen, um branchenübergreifend Ad-Hoc-Anfragen von Unternehmenskunden im Bereich der IT-Services zu adressieren. Darüber hinaus verfasst er Thought Leadership Researcharbeiten, Whitepapers und Artikel über neue Technologien im Bankwesen zu den Themen Automatisierung, Digital und User Experience (DX bzw. UX) sowie über die Auswirkungen der Datenanalyse in diversen Branchen.



*Autor (XDR)*

## Dr. Maxime Martelli

**Consulting Manager und Sicherheitsanalyst**

Maxime zählt zu ISGs “Cybersecurity” -Einheit für multinationale Unternehmen und den öffentlichen Sektor, und wendet sein Fachwissen im Bereich Informationssicherheit und Cloud-Sicherheitsprojektean. Als Autor, Lehrer und Dozent auf dem Gebiet der IT, begeistert sich Maxime leidenschaftlich für Technologie und wendet sein Wissen über Prozesse, digitale Strategie und IT-Organisationan, um die Anforderungen seiner Kunden zu erfüllen.

Als Sicherheitsberater führt er Transformations- und Strategieprojekte für alle Art von Sicherheitsprodukten und -lösungen durch und leitet das SASE/ SSE-Thema bei der Cybersecurity-Einheit bei ISG EMEA.

*Unternehmenskontext und globaler Überblick*

## Monica K

**Assistant Manager, Lead Research Specialist**

Monica K. ist Assistant Manager und Lead Research Specialist und eine Digitalexpertin bei ISG. Sie hat Inhalte für die Provider Lens™-Studien sowie Inhalte aus der Unternehmensperspektive erstellt und ist die Autorin des globalen zusammenfassenden Berichts für den Cybersecurity-, ESG- und Nachhaltigkeitsmarkt. Monica K. verfügt über mehr als ein Jahrzehnt an Erfahrung und Fachwissen in den Bereichen Technologie, Wirtschaft und Marktforschung für ISG-Kunden. Zuvor war sie bei einem Forschungsunternehmen tätig, wo sie sich auf aufkommende Technologien wie IoT und Produktentwicklung, Anbieterprofile und Talent Intelligence spezialisierte. Zu ihrem Aufgabenbereich gehörte das Management umfassender Forschungsprojekte und die Zusammenarbeit mit internen Stakeholdern bei verschiedenen Beratungsinitiativen.

*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 globaler Leiter – ISG Provider Lens™**

Herr Aase verfügt über umfangreiche Erfahrungen bei der Implementierung und Erforschung der Dienstleistungsintegration und des Managements von IT- und Geschäftsprozessen. Mit mehr als 35 Jahren Erfahrung ist er hochqualifiziert in der Analyse von Trends und Methoden der Vendor Governance, der Identifizierung von Ineffizienzen in aktuellen Prozessen und der Beratung der Branche. Jan Erik hat Erfahrungen auf allen vier Seiten des Sourcing- und Vendor-Governance-Lebenszyklus - als Kunde, Branchenanalyst, Dienstleister und Berater.

Als Partner und globaler Leiter von ISG Provider Lens™ ist er nun sehr gut positioniert, um den Zustand der Branche zu bewerten, darüber zu berichten und Empfehlungen sowohl für Unternehmen als auch für Kunden von Dienstleistern 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 ISGBeraterteam. Unternehmen erhalten eine Fülle detaillierter Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Sourcing- Partner helfen; die ISG-Berater wiederum nutzen die Berichte, um ihre Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG abzugeben. Die Studien decken derzeit Provider mit Angeboten in mehreren Regionen weltweit ab. Weitere Informationen über die ISG Provider Lens Studien finden Sie auf dieser Webseite.

## ISG Research™

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

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

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

## ISG

ISG (Information Services Group) (Nasdaq: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 900 Kunden, darunter über 75 der 100 weltweit größten Unternehmen, unterstützt ISG Unternehmen, öffentliche Organisationen sowie Service- und Technologie-Anbieter dabei, Operational Excellence und schnelleres Wachstum zu erzielen. Der Fokus des Unternehmens liegt auf Services im Kontext der digitalin Transformation, inclusive AI und Automatisierung, Cloud und Daten- Analytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzwerkbetrieb, Strategie- und - Betriebs-Design, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.600 mit der Digitalisierung vertraute Experten und ist in mehr als 20 Ländern tätig. Das globale Team von ISG ist bekannt für sein innovatives Denken, seine geschätzte Stimme im Markt, tiefgehende Branchenund Technologie-Expertise sowie weltweit führende Marktforschungsund Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren.

Weitere Informationen unter isg-one.com.

ISG Provider Lens™

**JULI, 2024**

# REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES