ISG Provider Lens™

Cybersecurity – Solutions and Services

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

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.

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

	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

	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

	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

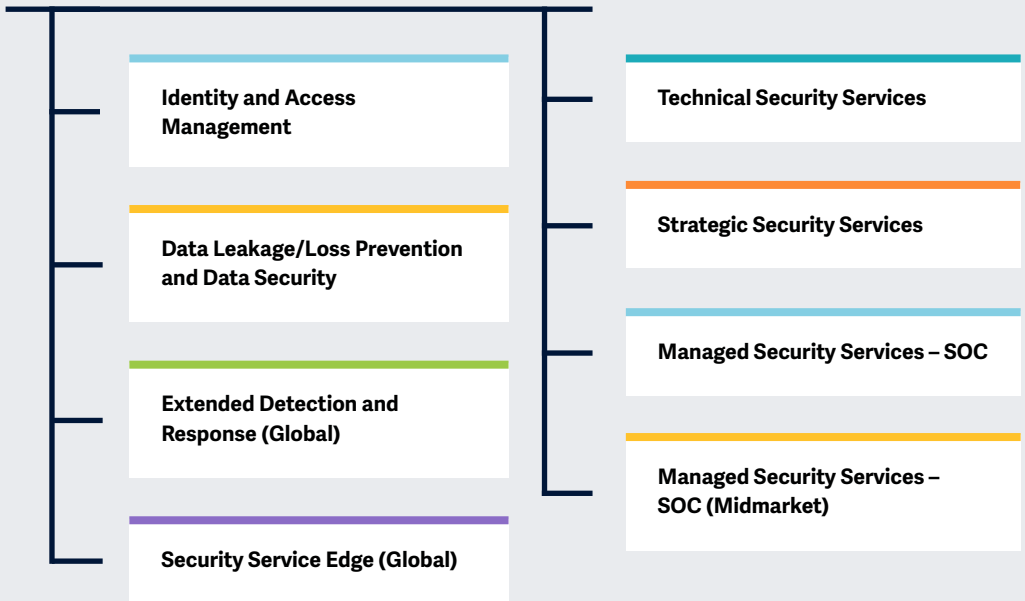
Anbieterpositionierung

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.

Identity and Access Management

Wer sollte dieses Kapitel lesen

Diese Bewertung von IAM-Lösungsanbietern ist für Unternehmen in Deutschland relevant, die ihre Cybersicherheit verbessern und ihre Zugriffsmanagementprozesse optimieren wollen. Dieser ISG-Bericht richtet sich an Unternehmen, die mit der komplexen Verwaltung von Benutzeridentitäten, Zugriffsrechten und privilegiertem Zugang zu wichtigen Ressourcen zu kämpfen haben.

In Deutschland soll durch den Einsatz von IAM-Lösungen die Sicherheit erhöhen, den Benutzerzugang optimiert und die Einhaltung von Vorschriften wie der GDPR gewährleistet werden. Unternehmen wünschen sich Lösungen, die eine robuste Benutzerauthentifizierung, Autorisierung und zentralisierte Zugangskontrolle bieten.

Unternehmen wollen IAM-Lösungen mit Funktionen wie Single Sign-on (SSO), Multifaktor-Authentifizierung (MFA) und Privileged Access Management (PAM) einsetzen, um kritische Ressourcen zu schützen.

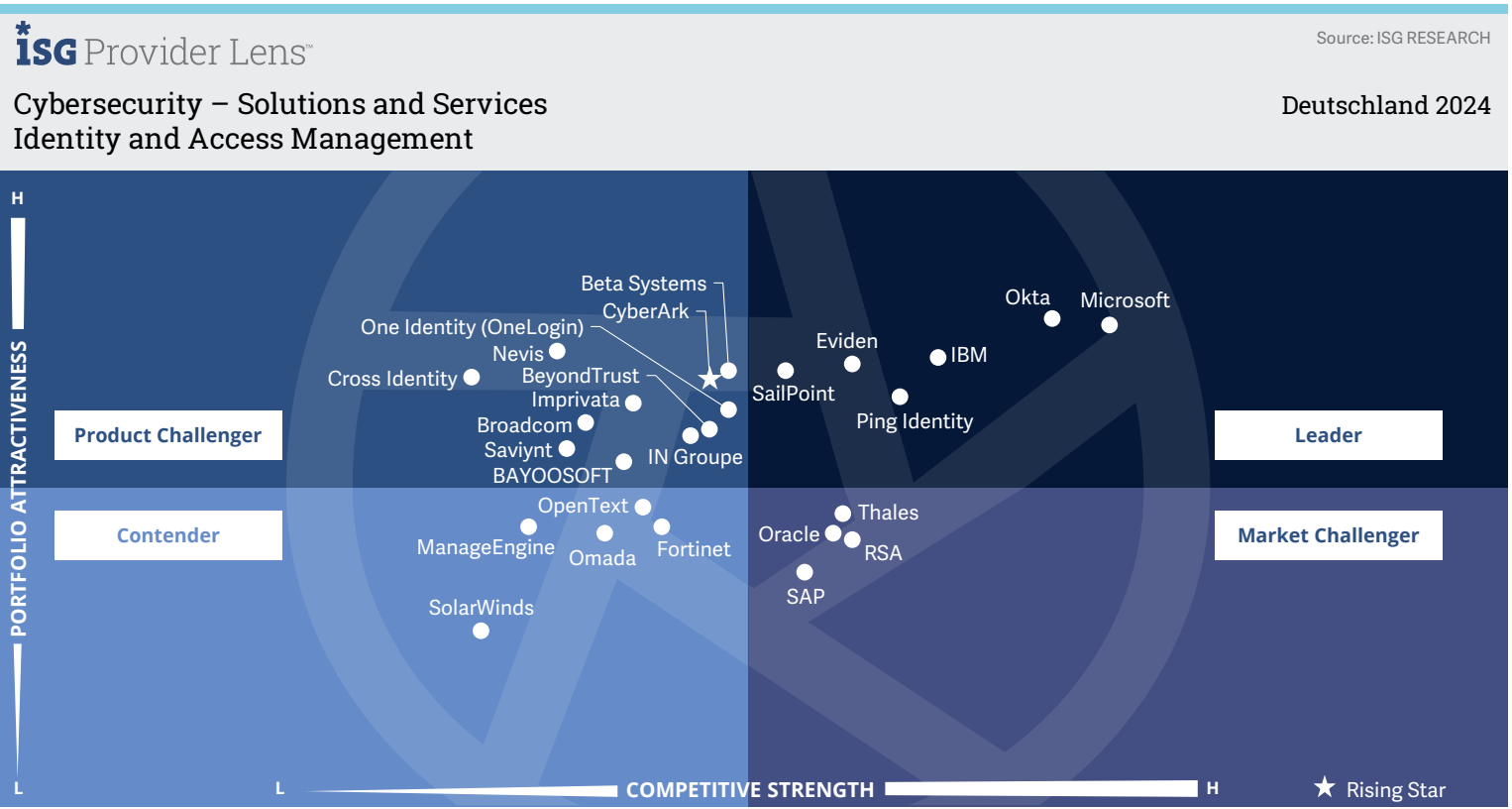
Die IAM-Lösungen der Anbieter umfassen User Provisioning, rollenbasierte Zugriffskontrolle und Identity Governance, um die verschiedenen Unternehmensanforderungen zu erfüllen. Auch Beratungsdienste für die Entwicklung von IAM-Strategien, Implementierung und kontinuierlicher Support werden offeriert.

Deutsche Unternehmen erhalten mit diesem Bericht Bewertungen von IAM-Lösungsanbietern; sie spielen eine entscheidende Rolle bei der Sicherung digitaler Assets. Unternehmen verlassen sich zunehmend auf digitale Infrastrukturen, und deshalb wird IAM für die Verwaltung von Benutzeridentitäten und Zugriffsrechten zu einem unerlässlichen Werkzeug.

IT-Sicherheitsexperten erhalten mit diesem Bericht Einblicke in die Fähigkeiten und Leistungen der verschiedenen IAM-Lösungsanbieter und erfahren, wie sie die Unternehmensdaten und -infrastruktur schützen können.

Entscheidungsträgern hilft dieser Bericht, IAM-Lösungen auszuwählen und zu implementieren sowie fundierte Entscheidungen zu treffen.

Compliance-Verantwortliche erfahren aus diesem Bericht, inwieweit IAM-Lösungen die gesetzlichen Compliance-Anforderungen erfüllen.



Im Rahmen des Quadranten werden die **relevantesten** IAM-Anbieter in Deutschland, die eigenerstellte Software anbieten bzw. betreiben, bewertet. Wichtige Themen sind **SSO** und **MFA. Passwortlose** Authentifizierung und **KI-Unterstützung** werden immer wichtiger.

Frank Heuer

Definition

Die im Rahmen dieses Quadranten bewerteten IAM-Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die Verwaltung von Benutzeridentitäten und -geräten in Unternehmen Dieser Quadrant umfasst auch SaaS-Angebote auf Basis von proprietärer Software. **Reine Dienstleister, die keine IAM-Produkte (On-Premises oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht berücksichtigt.** Entsprechend den individuellen Unternehmensanforderungen können diese Angebote auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in vom Kunden verwalteten Clouds, auf Basis eines as-a-Service-Modells oder in Form einer kombinierten Lösung.

IAM-Lösungen dienen dem Management (Erfassung, Aufzeichnung und Verwaltung) von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets auf Basis von Privileged Access Management (PAM), d.h. des Zugriffs anhand von definierten Policies. Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungs-Suites im Rahmen von Management Suites zunehmend in sichere Mechanismen, Frameworks und Automatisierung (z.B. der Risikobewertung) eingebunden, um Nutzer- und Attacken-Profiling in Echtzeit durchführen zu können. Von den Lösungsanbietern werden zudem weitere Funktionalitäten für Social Media und mobile Anwendungen erwartet, um deren spezifische Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Dieser Quadrant umfasst auch Machine Identity Management.

Auswahlkriterien

1. Einsatz der Lösung **vor Ort, in der Cloud, als Identity as a Service (IDaaS)** und auf Basis eines verwalteten Modells eines Drittanbieters
2. Die angebotenen Lösungen sollten die **Authentifizierung** anhand einer Kombination von **Single Sign-on (SSO), Multifaktor-Authentifizierung (MFA)**, risiko- und kontextbasierten Modellen unterstützen
3. Unterstützung von **rollenbasiertem Zugriff** und PAM
4. **Zugriffsmanagement** für eine oder mehrere Unternehmensanforderungen wie **Cloud, Endpunkte, mobile Geräte, APIs und Webanwendungen**
5. **Unterstützung von einem oder mehreren älteren und neuen IAM-Standards**, einschließlich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM
6. Sicherer Zugriff durch eine oder mehrere der folgenden Möglichkeiten: Directory-**Lösungen, Dashboard- oder Self-Service-Management** und Lifecycle Management (Migration, Synchronisierung und Replizierung)

Beobachtungen

IAM ist nach wie vor ein besonders relevantes Cybersecurity-Thema. Die zunehmende Digitalisierung aller Bereiche ist ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen. Diese Entwicklung trägt dazu bei, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern z.B. auch vernetzte Fertigungsmaschinen (Industrie 4.0).

Zudem nimmt die auch Anzahl zu verwaltender „natürlicher" digitaler Identitäten stetig zu. Ein wichtiger Faktor dabei ist nach wie vor der Umzug vieler Mitarbeitender in das Home Office. Durch vermehrte Remote- und mobile Zugriffe auf die Unternehmensressourcen wird die Regulierung und Zugriffskontrolle zunehmend wichtig. Dies resultiert auch in nochmals höheren Sicherheits- bei gleichzeitig höheren Komfortanforderungen. Daher gewinnen Themen wie Multi-Faktor-Authentifizierung (MFA), Single Sign-on (SSO), intuitive Schnittstellen, passwortlose Authentifizierung sowie der Einsatz von Biometrie und künstlicher Intelligenz an Bedeutung.

Wie im Softwaremarkt insgesamt ist auch bei IAM-Lösungen eine Verschiebung vom On-Premise-Betrieb in die Cloud festzustellen. Die meisten Anbieter haben sich darauf eingestellt und bieten sowohl den On-Premise- als auch den Cloudbetrieb an. Auch reine Cloudanbieter treten immer häufiger auf, allen voran Okta.

Anbieterseitig ist zudem zu erwähnen, dass Ping Identity den Wettbewerber ForgeRock übernommen und integriert hat, der infolgedessen in unserer Analyse nicht mehr dediziert aufgeführt ist. Neuer Rising Star ist CyberArk. ManageEngine ist neu im Quadranten vertreten.

Von den 85 Anbietern, die in dieser Studie bewertet wurden, konnten sich 26 für diesen Quadranten qualifizieren. Dabei erreichten sechs eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Eviden (an Atos Business) profiliert sich als europäischer Anbieter im deutschen IAM-Markt mit einem vielseitigen Portfolio und baut sein Offering weiter aus.

IBM punktet mit seiner großen Marktpräsenz und bietet ein leistungsfähiges Portfolio für Identity & Access-Management-Lösungen an, das sich besonders gut in die IBM-Technologielandschaft integrieren lässt.

Microsoft

Microsoft setzt sich im deutschen IAM-Markt aufgrund des versierten Marketings, aber auch mit technologischen Verbesserungen, immer stärker durch.

Okta

Mit rein cloudbasierten IAM-Lösungen ist **Okta** weiterhin erfolgreich in Deutschland – insbesondere bei Anwendern, die Wert auf eine schnelle und einfache Umsetzung legen.

Mit einer optimierten Balance von Sicherheit und Endbenutzerkomfort sowie vielseitiger Nutzbarkeit ist **Ping Identity** auch im deutschen Markt zunehmend erfolgreich.

SailPoint

SailPoint punktet mit Risikominimierung durch künstliche Intelligenz und mit erleichterter IAM-Verwaltung von Multicloud-Umgebungen.

CyberArk

CyberArk ist der „Rising Star" unter den Anbietern von Identity- & Access-Management-Lösungen in Deutschland. Dazu tragen die umfassenden und ausgefeilten PAM-Lösungen von CyberArk bei.

Data Leakage/Loss Prevention and Data Security

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für deutsche Unternehmen aller Branchen relevant, um Anbieter von DLP- und Datensicherheitsdiensten zu evaluieren. Es werden Dienstleister bewertet, die Unternehmen bei der Identifizierung und Überwachung sensibler Daten unterstützen, und zwar indem nur autorisierten Benutzern Zugang gewährt und Datenverluste bzw. -lecks verhindert werden.

In Deutschland finden deutliche Verschiebungen in den DLP-Strategien statt, was die dynamische Cybersicherheitslandschaft widerspiegelt. Deutsche Unternehmen setzen vorrangig auf DLP-Tools, um sensible Daten zu schützen und strenge Datenschutzvorschriften wie die DSGVO einzuhalten. Sie erwarten skalierbare und effiziente DLP-Lösungen, damit die mit Datenschutzverletzungen und Insider-Bedrohungen verbundenen Risiken minimiert werden können.

Cloudnative DLP-Lösungen sind im Zuge der weiter fortschreitenden Nutzung von Cloud-Technologien auf dem Vormarsch.

Die Integration von DLP mit Collaboration Tools wird immer wichtiger, um den sicheren Datenaustausch und die Zusammenarbeit im Rahmen von Remote-Arbeitsumgebungen zu erleichtern. Diese Integration stellt sicher, dass vertrauliche Informationen unabhängig vom Standort oder dem für den Zugriff verwendeten Gerät geschützt bleiben.

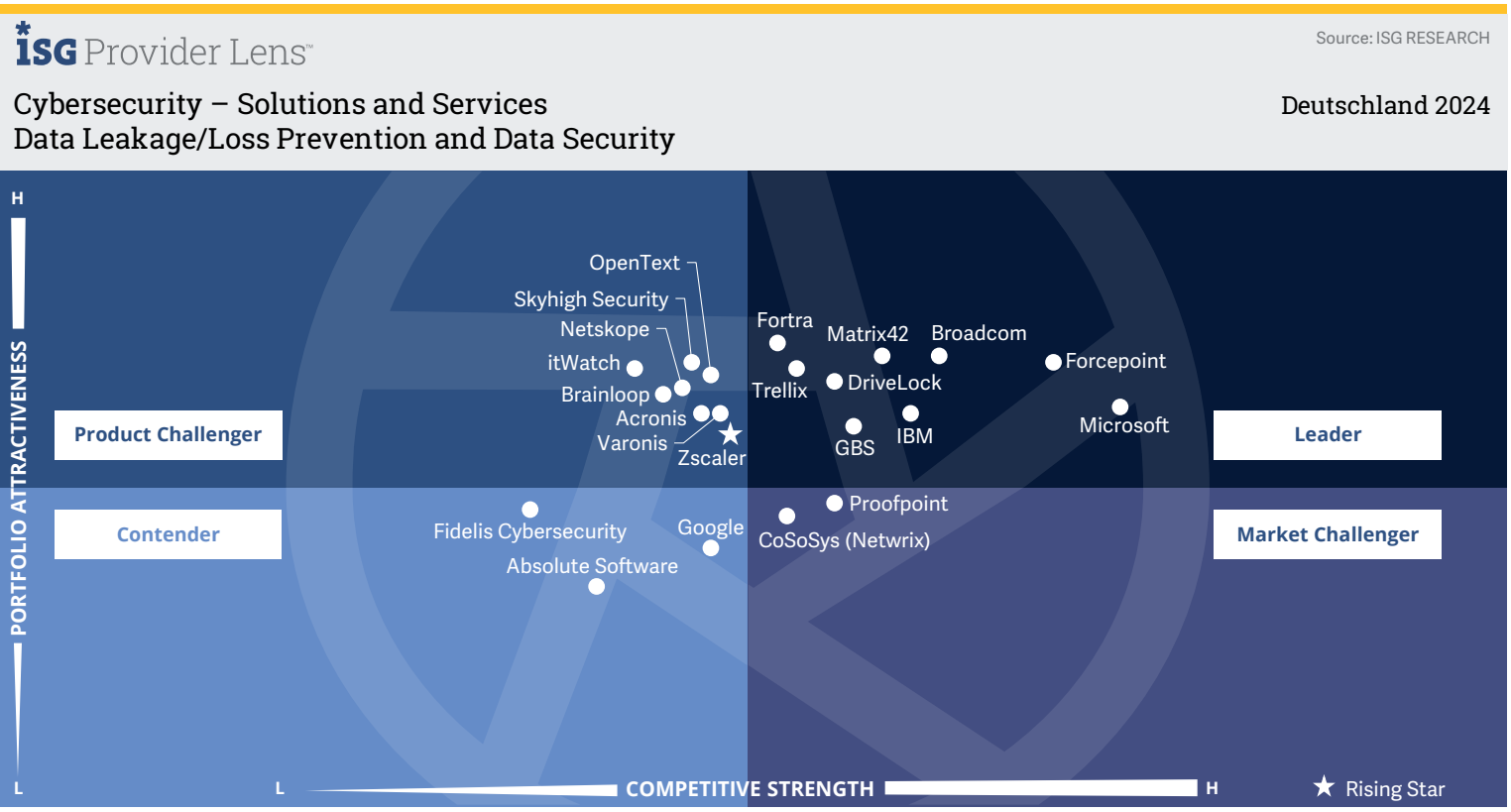
Die steigende Zahl von Mitarbeitenden an Remote-Standorten unterstreicht, wie notwendig DLP-Lösungen sind, die Insider-Bedrohungen wirksam abwehren und sensible Daten, auf die von verschiedenen Standorten aus zugegriffen wird, schützen können.

DLP-Anbieter reagieren auf diese Trends mit innovativen Features, wie z.B. umfangreichen Funktionen zur Dateiverfolgung, ML-gestütztes DLP zur Priorisierung der Datenüberwachung und API-gesteuerte Lösungen zur nahtlosen Integration in bestehende Systeme. Diese Fortschritte entsprechen den sich entwickelnden Anforderungen deutscher Unternehmen, die skalierbare, flexible und auf die Einhaltung von Vorschriften ausgerichtete DLP-Lösungen suchen, um die Komplexität moderner Cybersicherheitslandschaften zu bewältigen.

IT-Sicherheitsexperten informiert dieser Bericht über neue Trends, innovative Funktionalitäten und Best Practices in diesem Bereich.

Chief Information Security Officers erhalten durch diesen Bericht einen Einblick in die sich entwickelnde Landschaft der DLP-Strategien und -Lösungen, so dass sie fundierte Entscheidungen über Investitionen in Cybersicherheitstechnologien treffen können.

Compliance-Beauftragte, die für die Einhaltung von Datenschutzbestimmungen verantwortlich sind, erfahren aus diesem Bericht, wie DLP-Lösungen ihren Unternehmen helfen können, Vorschriften einzuhalten.



Im Rahmen dieses Quadranten werden die **relevantesten** DLP-Anbieter in Deutschland, die eigenerstellte Software anbieten bzw. betreiben, bewertet. Drängende **Datenschutzbelange** und die Sicherung geistigen Eigentums tragen zur Bedeutung des Marktes bei.

Frank Heuer

Definition

Die im Rahmen dieses Quadranten bewerteten DLP-Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen, u.a. auch SaaS-Lösungen. **Reine Dienstanbieter, die kein DLP-Produkt (On-Premises oder in der Cloud) anbieten, das auf eigenentwickelter Software basiert, werden in diesem Quadranten nicht berücksichtigt.** DLP-Lösungen können sensible Daten identifizieren und überwachen, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste/-lecks verhindern. Die Lösungen der Anbieter in diesem Markt bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf diversen Geräten ermöglichen.

Diese Lösungen gewinnen zunehmend an Bedeutung, denn es wird für Unternehmen immer schwieriger, Datenbewegungen und -übertragungen zu kontrollieren; über ein Drittel der Datenverletzungen haben ihren Ursprung innerhalb des Unternehmens. Die Anzahl der Geräte, u.a. mobiler Geräte, die zur Datenspeicherung verwendet werden, verstärkt dieses Problem zusätzlich. Dank Internetkonnektivität können diese Geräte Daten austauschen, ohne ein zentrales Gateway zu passieren. Datensicherheitslösungen schützen Daten vor unbefugtem Zugriff, Offenlegung oder Diebstahl durch die Priorisierung, Klassifizierung und Überwachung von Daten (im Ruhezustand und bei der Übertragung); sie ermöglichen ein Security Reporting und helfen, die Sicherheit der gefährdeten Daten zu verbessern.

Auswahlkriterien

1. DLP-Lösungen auf Basis von **eigenentwickelter Software** und nicht auf Basis von Software von Drittanbietern
2. DLP-Unterstützung über eine **beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt**
3. Nachweislicher Schutz von **sensiblen Daten**, egal ob es sich dabei um **strukturierte oder unstrukturierte Daten**, Text- oder Binärdaten handelt
4. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
5. Fähigkeit der Lösung, **sensible Daten zu erkennen, Richtlinien durchzusetzen**, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern.

Beobachtungen

Nicht nur bei (Finanz-) Dienstleistern haben sich Daten und geistiges Eigentum zu immer wichtigeren, teilweise existenziell bedeutsamen Assets entwickelt. Gerade auch Industrieunternehmen sind im internationalen Wettbewerb auf den zuverlässigen Schutz von Firmengeheimnissen angewiesen. Dies trägt zum gestiegenen Interesse an DLP-Lösungen bei. Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung dar, da sie sich oftmals der betrieblichen Administration entziehen und teilweise auch aus rechtlichen Gründen nicht umfassend betrieblich überwacht werden dürfen. DLP-Lösungen müssen diese Einschränkungen bei der Kontrolle berücksichtigen, ohne betriebliche Sicherheitslücken zuzulassen. Mit der Datenschutz-Grundverordnung hat die Bedeutung des Datenschutzes in Unternehmen auch von Rechts wegen weiter zugenommen.

Die enorme Zunahme an Unternehmensdaten erfordert leistungsfähige DLP-Lösungen, die die Daten schnell aufspüren, klassifizieren und entsprechend ihrem Schutzbedarf vor unerlaubten Aktionen schützen. 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. Aber nicht nur ungewollt können Daten durch das Verschulden von internen Akteuren abfließen; auch vor ungetreuem Verhalten interner Beteiligter müssen sich Unternehmen schützen können.

KI hilft zunehmend bei der Bewältigung der Herausforderungen.

Zscaler ist der neue Rising Star. Trend Micro ist nicht mehr im Markt vertreten.

Von den 85 Anbietern, die in dieser Studie bewertet wurden, konnten sich 22 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 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 unterstützt wird.

MATRIX42

Matrix42 profiliert sich zunehmend im Security-Markt und überzeugt mit umfassenden, effizienten DLP-Funktionen und kundenorientiertem Service. Mit geringen Beeinträchtigungen wird eine hohe Akzeptanz bei den Endanwendern erreicht.

Microsoft

Mit geschicktem Marketing – z.B. Integration und Bundling – und verbesserten Lösungen baut **Microsoft** seine Leader-Position im deutschen DLP-Markt aus.

Trellix

Eine umfangreiche Lösung, Cloudbetrieb in Deutschland und eine große lokale Präsenz durch eine umfassende Partnerlandschaft machen **Trellix** zum Leader im deutschen DLP-Markt.

zscaler

Zscaler ist der neue Rising Star für Data Loss/Leakage Prevention in Deutschland. Dazu tragen zum Beispiel eine leistungsfähige Lösung und höhere Marktpräsenz bei.

Extended Detection and Response (Global)

Wer sollte dieses Kapitel lesen

Dieser Quadrant ist für Unternehmen weltweit relevant, um Anbieter von Extended Detection & Response (XDR) Lösungen zu evaluieren. Es wird bewertet, wie die einzelnen Anbieter Unternehmen dabei helfen, die Transparenz über alle Telemetriequellen hinweg zu erhöhen und eine einheitliche Sicht auf die Erkennung von und Reaktion auf Bedrohungen zu erhalten. ISG bietet eine Analyse der aktuellen Positionierung von globalen XDR-Akteuren, inklusive eines umfassenden Überblicks über das Wettbewerbsumfeld in diesem Markt.

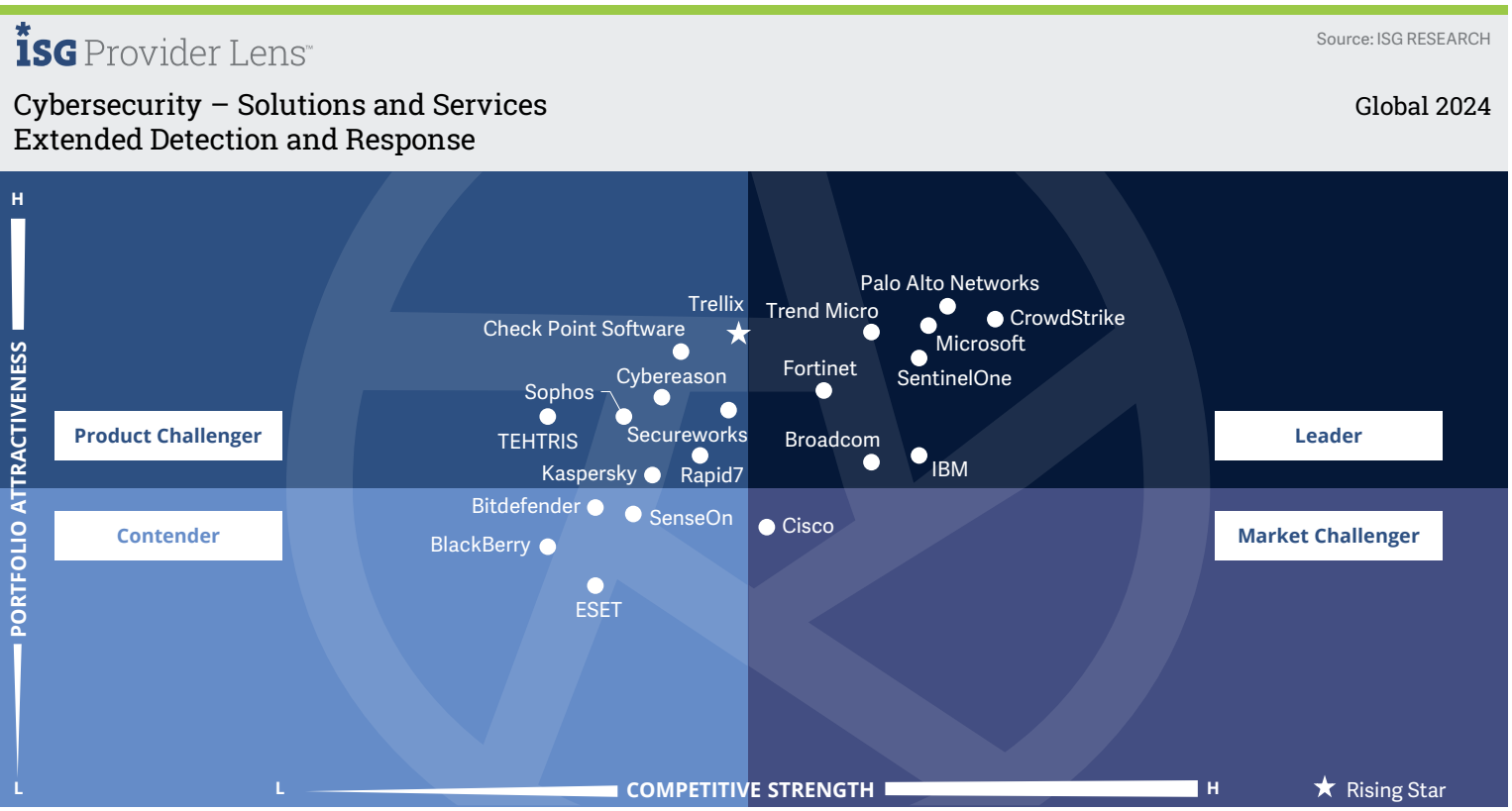
Unternehmen erkennen die Notwendigkeit eines proaktiven Ansatzes zur Erkennung von und Reaktion auf Bedrohungen, der sich auf Data-Science-Techniken und dynamisch aktualisierte Bedrohungsdaten stützt. XDR ermöglicht es Unternehmen jeder Größe und jedes Sicherheitsniveaus, robuste Fähigkeiten zur Erkennung und Reaktion auf Bedrohungen zu entwickeln, auch bei begrenztem Sicherheitspersonal, Fachwissen oder Budget für ein dediziertes Security Operations Center (SOC). Eine gut aufgebaute XDR-Lösung ist ein SOC-Enabler, der eine anschauliche Sicht auf Bedrohungen bietet und die initialen Triage-Aufgaben automatisiert.

Unter Einsatz des MITRE ATT&CK Frameworks und von Open-Source-Informationen erkennen XDR-Modelle Anomalien, klassifizieren Angriffe auf Basis spezifischer Taktiken und Techniken und liefern so verwertbare Erkenntnisse für SOC-Analysten. Warnungen werden mit Kontext angereichert und Ereignisse in Korrelation gesetzt, um den wahren Schweregrad der Bedrohung und die Beteiligung an der Angriffskette zu ermitteln. Das reduziert Fehlalarme und spart wertvolle Ermittlungszeit. Fortschrittliche XDR-Lösungen priorisieren Warnungen auf Grundlage von Risikobewertungen und Geschäftsauswirkungen und unterstützen so die Planung der Reaktion auf Vorfälle (Incident Response). Darüber hinaus sollten XDR-Lösungen über robuste APIs verfügen, über die Workflow-Funktionen auf andere externe Systeme ausgeweitet werden können, um Maßnahmen zur Eindämmung von Ereignissen effektiver zu gestalten.

Cybersecurity-Experten bietet dieser Bericht wertvolle Einblicke in XDR-Lösungen für eine bessere Sichtbarkeit über Endpunkte hinweg, um eine einheitliche Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

Strategie-Experten vermittelt dieser Bericht ein besseres Verständnis der Fähigkeiten von XDR-Anbietern, die Unternehmen dabei helfen, Sicherheitsrisiken effektiv zu verwalten und fundierte Entscheidungen über ihre Sicherheitsstrategie zu treffen.

Technologie-Experten werden in diesem Bericht über die Integrationsmöglichkeiten von XDR-Anbietern informiert und erfahren, wie sie zu einer besseren Erkennung und schnelleren Reaktion auf Bedrohungen beitragen können.



Im Rahmen des Quadranten „Extended Detection & Response“ wird die Fähigkeit von Sicherheitsanbietern bewertet, **integrierte Leistungen zur Erkennung, Untersuchung und Reaktion** auf Bedrohungen über mehrere Endpunkte, Netzwerke und Cloud-Umgebungen hinweg zu erbringen.

Dr. Maxime Martelli

Definition

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich durch eine Plattform aus, die Daten und Warnungen aus verschiedenen Komponenten zur Bedrohungsabwehr, -erkennung und -reaktion integriert, korreliert und kontextualisiert. XDR ist eine aus der Cloud bereitgestellte Technologie, die Multipoint-Lösungen umfasst und anhand von fortschrittlichen Analysen Warnmeldungen aus mehreren Quellen, unter anderem auch von schwachen Einzelsignalen, mit Vorfällen korreliert, um so die Erkennung zu präzisieren. XDR-Lösungen konsolidieren und integrieren mehrere Produkte und bieten umfassende Sicherheit für Arbeitsbereiche, Netzwerke und Workloads; sie sollen für eine erheblich höhere Transparenz und ein besseres kontextbasiertes Verständnis der im Unternehmen aufgedeckten Bedrohungen sorgen. Sie umfassen u.a. Telemetrie und kontextbezogene Datenanalysen zur Erkennung von und Reaktion auf solche Risiken. XDR-Lösungen umfassen mehrere Produkte; sie sind in einer einzigen Konsole mit ausgefeilten Funktionen für das Sichten, Erkennen und Reagieren auf Bedrohungen zusammengeführt. Ihr hoher Automatisierungsgrad und die kontextbezogene Analyse bieten maßgeschneiderte Reaktionsmöglichkeiten für betroffene Systeme; Warnmeldungen werden nach Schweregrad im Vergleich zu bekannten Referenz-Frameworks priorisiert. **Reine Dienstleister , die keine auf proprietärer Software basierende XDR-Lösung anbieten, werden in diesem Quadranten nicht berücksichtigt.** XDR-Lösungen zielen darauf ab, die Produktvielfalt, Alarmmüdigkeit, Integrationsprobleme und Betriebskosten zu verringern. Sie eignen sich besonders für Sicherheitsteams, die mit der Verwaltung verschiedenster Lösungsportfolios zu kämpfen haben oder den Wert von SIEM- (Security Information and Event Management) oder SOAR-Lösungen (Security Orchestration, Automation & Response) steigern wollen.

Auswahlkriterien

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

Beobachtungen

Im Jahr 2024 erfährt der XDR-Markt mit mehreren neuen Trends und Verbesserungen eine Weiterentwicklung. XDR-Lösungen integrieren fortschrittliche KI- und ML-Funktionen, verbessern so die Verhaltensanalyse und automatisieren Reaktionsmaßnahmen auf Basis erlernter Muster.

Die Anbieter legen zudem verstärkten Wert auf Cloud-Sicherheit und sorgen für umfassende Transparenz und Schutz in hybriden und Multicloud-Umgebungen. Die XDR-Plattformen sind eng auf das MITRE ATT&CK Framework abgestimmt und ermöglichen fundiertere Strategien für die Bedrohungsjagd und -bekämpfung.

XDR-Anbieter erweitern ihre Leistungen um robuste Managed Detection & Response Services (MDR) und begegnen damit dem Fachkräftemangel. Darüber hinaus nutzen XDR-Lösungen fortschrittliche UEBA zur proaktiven Erkennung von und Reaktion auf Bedrohungen. Die Automatisierungs- und Orchestrierungsfunktionen innerhalb der XDR-Plattformen werden immer ausgereifter; das optimiert die Prozesse zur Reaktion auf Vorfälle und reduziert manuelle Aufgaben. XDR orientiert sich außerdem an den Zero-Trust-Prinzipien, die eine kontinuierliche Überprüfung und strenge Zugriffskontrollen vorsehen, und enthält Funktionen zur Einhaltung gesetzlicher Vorschriften.

Diese Fortschritte unterstreichen die Rolle von XDR bei der Bereitstellung hochentwickelter Funktionalitäten für die Erkennung von und Reaktion auf Bedrohungen sowie die Einhaltung von Vorschriften im Zuge sich weiterentwickelnder Cyberbedrohungen.

21 Anbieter haben sich für diesen Quadranten qualifiziert; acht dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Broadcom

XDR von **Broadcom** beinhaltet umfassende Transparenz, fortschrittliche Analysen, automatische Reaktionen und eine vereinfachte Managementkonsole, über die digitale Unternehmensressourcen effektiv gegen sich entwickelnde Bedrohungen geschützt werden können.

CrowdStrike

CrowdStrikes Falcon® Insight XDR deckt mit seinem Falcon-Tool die steigende Marktnachfrage nach einer einzigen, vereinfachten Managementkonsole mit dem Ziel, die Widerstandsfähigkeit durch die Unterstützung von Standards und Frameworks wie CrowdXDR Alliance zu erhöhen.

Fortinet

Fortinet FortiXDR kann nahtlos in Fortinet Security Fabric und andere Sicherheitsprodukte von Fortinet integriert werden; so wird die Reaktion auf Vorfälle mit automatisierten Workflows und Playbooks optimiert. Diese Integration ermöglicht eine schnelle Eindämmung und Beseitigung von Bedrohungen.

IBM

IBMs Security QRadar XDR verfolgt einen proaktiven und koordinierten Ansatz zur Erkennung von und Reaktion auf Bedrohungen mit mehreren Modulen und der Integration über Netzwerke, Clouds, Endpunkte und andere Workloads hinweg.

Microsoft

Microsofts großer Kundenstamm und der hohe Bekanntheitsgrad der Marke haben dazu beigetragen, dass das Unternehmen eine herausragende Position im XDR-Markt einnimmt. Sein XDR integriert Defender Advanced Threat Protection (ATP), um Bedrohungen zu erkennen und darauf zu reagieren.

Palo Alto Networks

Die starke Marktpräsenz von **Palo Alto Networks**, das Engagement für Innovation und der Fokus auf Secure Access Service Edge/ Security Service Edge (SASE/SSE)-Lösungen machen Cortex XDR zu einem robusten Produkt und Palo Alto Networks zu einem Leader im XDR-Quadranten.

SentinelOne

SentinelOne behauptet seine Stellung als einer der führenden XDR-Anbieter dank patentierter verhaltensbasierter KI-Algorithmen zur Erkennung und Klassifizierung bösartiger Aktivitäten. Alle Sicherheitsfunktionen sind in einem einzigen Agenten gebündelt, so dass nicht mehrere Sicherheitsprodukte erforderlich sind.

Trend Micro

Trend Micro hat seine EDR-Funktionen (Endpoint Detection & Response) zu einem XDR-Produkt der nächsten Generation ausgebaut, das auf das MITRE ATT&CK Framework abgestimmt ist und dynamische Risikobewertungen bietet. Die Automatisierungsfunktionen liefern fortschrittliches XDR.

Trellix

XDR von **Trellix** (Rising Star) verfügt über ein anpassungsfähiges und interoperables Framework, das sich nahtlos mit einer Vielzahl externer Sicherheitslösungen verbinden lässt und so eine einheitliche Cybersicherheitsstrategie in Kombination mit einem ausgefeilten Mechanismus zur Erkennung von Bedrohungen fördert.

Security Service Edge (Global)

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Unternehmen weltweit relevant, um Anbieter von Security Service Edge (SSE) Lösungen zu evaluieren. Er bewertet die wichtigsten Funktionen von SSE-Lösungen, wie Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB) und Secure Web Gateways (SWGs). Darüber hinaus wird evaluiert, wie die einzelnen Anbieter Unternehmen bei der Gewährleistung der Sicherheit in hybriden und Multicloud-Ökosystemen unterstützen.

ISG gibt einen umfassenden Überblick über das Wettbewerbsumfeld in diesem Markt und stellt die aktuelle Positionierung dieser SSE Provider dar.

Im Zuge der schnellen Verlagerung zu hybriden Arbeitsmodellen suchen Unternehmen nach Lösungen, die Mitarbeitern, Partnern, Lieferanten und Kunden den Zugriff auf interne Anwendungen, das Internet und SaaS-Anwendungen ermöglichen. Sie wünschen sich SSE-Lösungen, die die Einführung und Umsetzung von Sicherheitsrichtlinien vereinfachen. Ein rationalisierter Ansatz reduziert die Komplexität und beschleunigt die Umsetzung. Von SSE-Plattformen wird erwartet, dass sie die Benutzeraktivitäten im gesamten Netzwerk überwachen und verfolgen. Außerdem müssen SSE-Anbieter alle Nutzer vor Ransomware und anderen hochentwickelten Malware-Bedrohungen schützen.

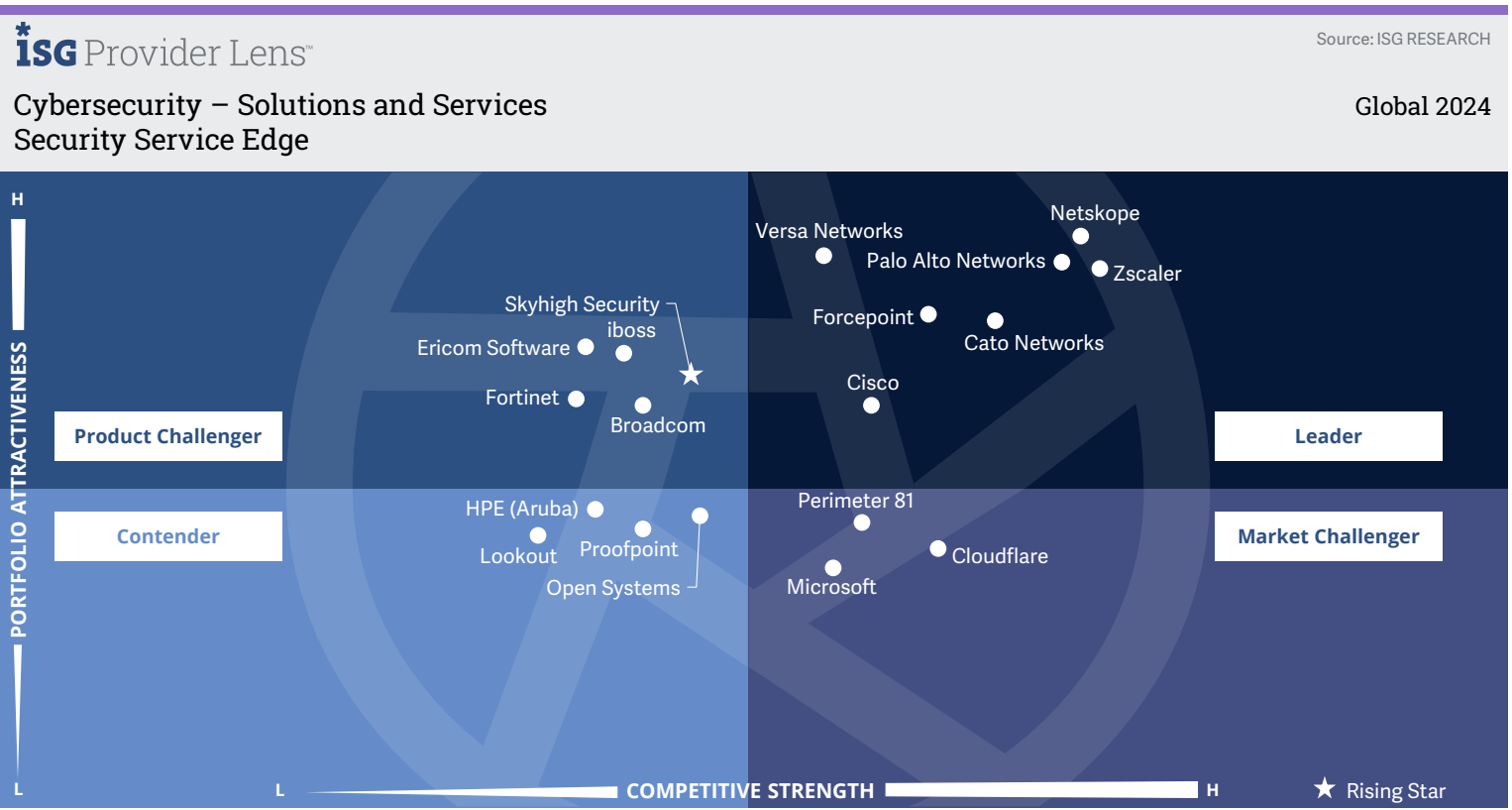
SSE wird eingesetzt, um moderne Sicherheitsherausforderungen zu bewältigen, den Zugang zu vereinfachen und die digitalen Erfahrungen zu verbessern. Von den Anbietern wird gewünscht, dass sie rationalisierte Lösungen, robusten Schutz und Flexibilität in einer sich schnell entwickelnden Landschaft bieten.

Der benötigte einheitliche, sichere Zugang für eine hybride Belegschaft treibt die Einführung von SSE voran. Unternehmen erwarten von SSE-Anbietern eine vereinfachte Bereitstellung, VPN-Umgehung und einen zuverlässigen Schutz vor Malware. Um erfolgreich zu sein, sollten die Anbieter innovativ sein, sich anpassen, die Benutzerfreundlichkeit in den Vordergrund stellen und ihre globale Reichweite ausbauen.

Datenmanagement-Experten sollten diesen Bericht lesen, um zu verstehen, wie SSE-Anbieter Unternehmen dabei helfen, die Herausforderungen zu meistern, die sich aus der Datenregulierung ergeben, und zwar durch bessere Richtlinienkontrolle und Berichterstattung.

Strategie-Experten gewinnen Einblicke in die kritischen Fähigkeiten von SSE-Anbietern und ihren Fokus auf die Nutzerorientierung durch Sicherheit für Endnutzer am Edge oder auf Geräten über die Cloud.

Technologie-Experten gewinnen durch diesen Bericht ein besseres Verständnis dahingehend, wie SSE-Anbieter Unternehmen bei der Einführung eines unternehmensweiten Zero-Trust-Frameworks unterstützen, um ihre Sicherheitslage zu verbessern.



Dieser Quadrant bewertet SSE-Anbieter von **cloud-zentrierten Lösungen**, welche Einzellösungen integrieren, um einen **sicheren Zugang zu Cloud-Diensten**, SaaS-Anwendungen, Webdiensten und privaten Anwendungen zu schaffen; dabei wird ein **starker Fokus auf die UX** gelegt.

Gowtham Sampath

Definition

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

Die Anbieter demonstrieren ihre Erfahrung mit der Einhaltung lokaler, regionaler und nationaler Gesetze (z.B. hinsichtlich Datensouveränität) für globale Kunden.

Die Netzwerkkomponenten von Secure Access Service Edge (SASE), wie SD-WAN, die in der ISG Provider Lens™ Studie „Network – Software-Defined Solutions & Services 2024" abgedeckt werden, **sind hier nicht berücksichtigt.**

SSE-Lösungen sind stark nutzerorientiert; sie bieten den Endanwendern Edge- oder Gerätesicherheit über die Cloud, anstatt ihnen den zentralen Zugriff auf Unternehmensanwendungen und Datenbanken über dedizierte Netzwerke zu gewähren. ZTNA (Zero Trust Network Access) stellt eine exklusive Verbindung zwischen Benutzern und Anwendungen her und nutzt kontextbasierte Verhaltensanalysen für die Zugriffskontrolle. CASB (Cloud Access Security Broker) bietet Transparenz, setzt Sicherheitsrichtlinien und Compliance durch und kontrolliert die Cloud-Nutzung durch die Schatten-IT; FWaaS (Firewall as a Service) und SWG (Secure Web Gateway) wehren bösartige Bedrohungen und den Zugriff auf infizierte Websites und Anwendungen ab. Typischerweise verfügt eine SSE-Lösung über eine einheitliche Konsole für die Gewährleistung der Transparenz und Governance und fortschrittliche Automatisierungsfunktionen zur Auswertung der Benutzererfahrung.

Auswahlkriterien

1. SSE als **integrierte Lösung** und mit folgenden entscheidenden Komponenten: **Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateways (SWG) und Firewall as a Service (FWaaS)**
2. Bereitstellung von Lösungen **überwiegend auf Basis von proprietärer** Software, **evtl. in Teilen auch basierend auf Partnerlösungen,** aber **nicht vollständig** auf Basis von Software **von Drittanbietern**
3. **Weltweite POPs** für die Bereitstellung dieser Lösungen
4. Erbringung von **SSE sowohl für Cloud- als auch für On-Premises-Umgebungen** (einschließlich hybrider Umgebungen)
5. **Kontextbezogene und verhaltensbezogene Auswertungen und Analysen** (Nutzeridentitäts- und Verhaltensanalysen bzw. User Entity and Behavior Analytics/ UEBA) zur Aufdeckung und Verhinderung bösartiger bzw. verdächtiger Absichten
6. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
7. Sicherstellung der **globalen Verfügbarkeit der Lösung**

Beobachtungen

Der Security Service Edge-Markt erlebt derzeit durch den zunehmenden Einsatz von Cloud-Anwendungen, die wachsende Zahl von Remote-Mitarbeitenden und die sich entwickelnde Cyberbedrohungslandschaft ein schnelles Wachstum. Die Analyse von ISG zeigt mehrere Herausforderungen für Unternehmen auf, die den Einsatz von SSE erforderlich machen:

Unternehmen setzen zunehmend eine Mischung aus verschiedenen Cloud-Plattformen ein (öffentlich, privat und hybrid), da herkömmliche Sicherheitslösungen keine konsistente Sicherheit in diesen unterschiedlichen Umgebungen gewährleisten können.

Mit der Zunahme der Remote-Arbeit wird der sichere Zugriff auf Cloud-Anwendungen von verschiedenen Standorten und Geräten aus immer wichtiger.

Die Verwaltung eines komplexen Sicherheits-Ökosystems mit mehreren Punktlösungen kann eine Herausforderung darstellen.

Strenge Vorschriften wie der Health Insurance Portability & Accountability Act (HIPAA), der California Consumer Privacy Act (CCPA) und die DSGVO erfordern robuste Datensicherheitsmaßnahmen.

Anbieterauswahl: Differenzierung im SSE-Markt:

Unternehmen bevorzugen SSE-Anbieter, die ihre branchenspezifischen Compliance-Vorschriften und Datensicherheitsanforderungen erfüllen.

Sie wünschen sich Anbieter, die offene Standards und vorgefertigte Integrationen mit bestehenden Sicherheitstools und Cloud-Plattformen anbieten, um einen Vendor Lock-in zu vermeiden und die Bereitstellung zu vereinfachen.

SSE-Lösungen müssen effektiv skalierbar sein, um die zunehmende Nutzung von Cloud-Anwendungen und die steigende Zahl an Nutzern adressieren zu können. Zudem müssen sie niedrige Latenzzeiten und eine zuverlässige Leistung aufweisen; das ist für die Gewährleistung einer positiven Benutzererfahrung für geografisch verteilte Arbeitskräfte unerlässlich.

Unternehmen bevorzugen Anbieter mit soliden Threat Intelligence-Funktionen und einer nachgewiesenen Erfolgsbilanz in Sachen Sicherheit.

Eine transparente Preisgestaltung und ein klares Verständnis der Gesamtbetriebskosten, einschließlich der Integrationskosten, sind für Unternehmen bei der Auswahl eines SSE-Anbieters von entscheidender Bedeutung.

19 Anbieter haben sich für diesen Quadranten qualifiziert; sieben dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Cato Networks

Cato Networks kümmert sich insbesondere um die Verbesserung der Integration und Leistung seiner SSE-Lösungen; zu diesem Zweck werden die ZTNA-Fähigkeiten innerhalb der Secure Connect-Plattform und die Partnerschaften mit Cloud-Anbietern ausgebaut.

Cisco

Cisco setzt auf die Integration seiner SSE-Lösung Secure Access mit anderen Cisco-Sicherheitsprodukten, um einen einheitlichen Ansatz verfolgen zu können. Der Anbieter baut außerdem die Partnerschaften mit Cloud-Anbietern wie Microsoft aus, um die Funktionen von Secure Access zu erweitern.

Forcepoint

Forcepoint legt den Fokus auf Integrationen mit weiteren Cloud-Plattformen, um mit seinem Forcepoint Cloud Security Gateway, einer SSE-Plattform, eine höhere Abdeckung zu erzielen. Dieser strategische Schritt steht im Einklang mit der zunehmenden Verbreitung von Multicloud-Umgebungen.

Netskope

Netskope erweitert sein globales Rechenzentrumsnetzwerk mit dem Ziel, niedrigere Latenzzeiten sowie eine höhere Leistung und Nutzerreichweite zu bieten. Der Anbieter fokussiert sich zudem auf Partnerschaften mit SIEM-Anbietern, um eine bessere Erkennung und Untersuchung von Bedrohungen innerhalb seiner SSE-Plattform zu ermöglichen.

Palo Alto Networks

Palo Alto Networks hat die Benutzerfreundlichkeit seiner Prisma SASE-Plattform verbessert und die Tools zur Richtlinienverwaltung optimiert. Außerdem wurden die Partnerschaften mit Cloud-Anbietern wie AWS ausgebaut, um vorkonfigurierte Sicherheitsrichtlinien anbieten zu können.

Versa Networks

Versa Networks hat in seine Versa SASE-Plattform erweiterte Funktionen zum Schutz von Cloud Workloads eingeführt und Partnerschaften mit Threat-Intelligence-Anbietern abgeschlossen, um die Fähigkeiten zur Erkennung von Bedrohungen zu verbessern und so einen umfassenden Schutz für Kunden zu gewährleisten.

zscaler

Zscaler hat sein globales Rechenzentrumsnetzwerk erweitert, um die Leistung seiner Zscaler ZSSP-Plattform zu verbessern. Außerdem wurde der Fokus auf Partnerschaften mit SASE-Framework-Anbietern für einen sicheren Zugang nach Industriestandard gestärkt, um ein einheitliches und sicheres Cloud-Sicherheitsökosystem zu fördern.

Skyhigh Security

Skyhigh Security (Rising Star) bietet inzwischen die Integration der Cloud Workload Protection Platform (CWPP) an, um neben der SSE-Kernplattform umfassende Cloud-Sicherheit bieten zu können. Dieses Angebot geht über die grundlegenden SSE-Funktionen hinaus und bietet zusätzlichen Schutz für Cloud Workloads.

Technical Security Services

Wer sollte dieses Kapitel lesen

Anhand dieses umfassenden Berichts können Unternehmen aller Branchen TSS-Anbieter einer Evaluierung unterziehen. Er geht über die bloße Bewertung der proprietären Angebote dieser Anbieter hinaus und hebt deren Fähigkeiten zur Integration verschiedener Sicherheitsprodukte und -lösungen unterschiedlicher Vendoren hervor. Der Fokus liegt auf der aktuellen Marktlandschaft; der Bericht evaluiert die derzeitige Marktpositionierung von TSS-Anbietern und erläutert ihre Strategien zur Bewältigung kritischer Sicherheitsherausforderungen.

Deutsche Unternehmen können aus diesem Bericht wertvolle Erkenntnisse gewinnen, insbesondere um sich in der sich ständig weiterentwickelnden Cybersicherheitslandschaft zurechtzufinden. Zero-Trust-Prinzipien setzen sich immer mehr durch, und deshalb ist es sehr wichtig zu verstehen, wie TSS-Anbieter Zero-Trust-Implementierungen angehen, um die Sicherheitsstrategien an die sich entwickelnde Bedrohungslandschaft anpassen zu können. Dieser Bericht bietet wertvolle Einblicke in cloudnative Sicherheitslösungen, u.a. Secure Access Service Edge (SASE) und Security Service Edge (SSE), die für den Übergang von On-Premises-Rechenzentren zu öffentlichen Cloud-Umgebungen unerlässlich sind.

Auch der Trend hin zur Konsolidierung von Sicherheitstechnologien wird untersucht, die darauf abzielt, die Sicherheitsinfrastruktur effektiver zu gestalten und die Komplexität zu verringern. Wenn deutsche Unternehmen die Vorteile der Anbieterkonsolidierung erkennen und integrierte Sicherheitsplattformen einsetzen, können sie ihre Sicherheitsinvestitionen effektiv optimieren. Wenn Unternehmen mit den Branchentrends Schritt halten und sich innovative Sicherheitstechnologien zunutze machen, können sie ihre Cybersicherheitslage verbessern, neue Bedrohungen wirksam abwehren und ihre Vermögenswerte und Daten schützen.

Strategieexperten hilft dieser Bericht, sich über die aktuelle Marktlandschaft zu informieren und fundierte Entscheidungen über Sicherheitsstrategien, Anbieterauswahl und Technologieinvestitionen zu treffen.

Cybersicherheitsexperten informiert dieser Bericht über die Leistungen und die Marktpositionierung von TSS-Anbietern, die einen Beitrag zur Verbesserung der Sicherheitslage ihres Unternehmen leisten.

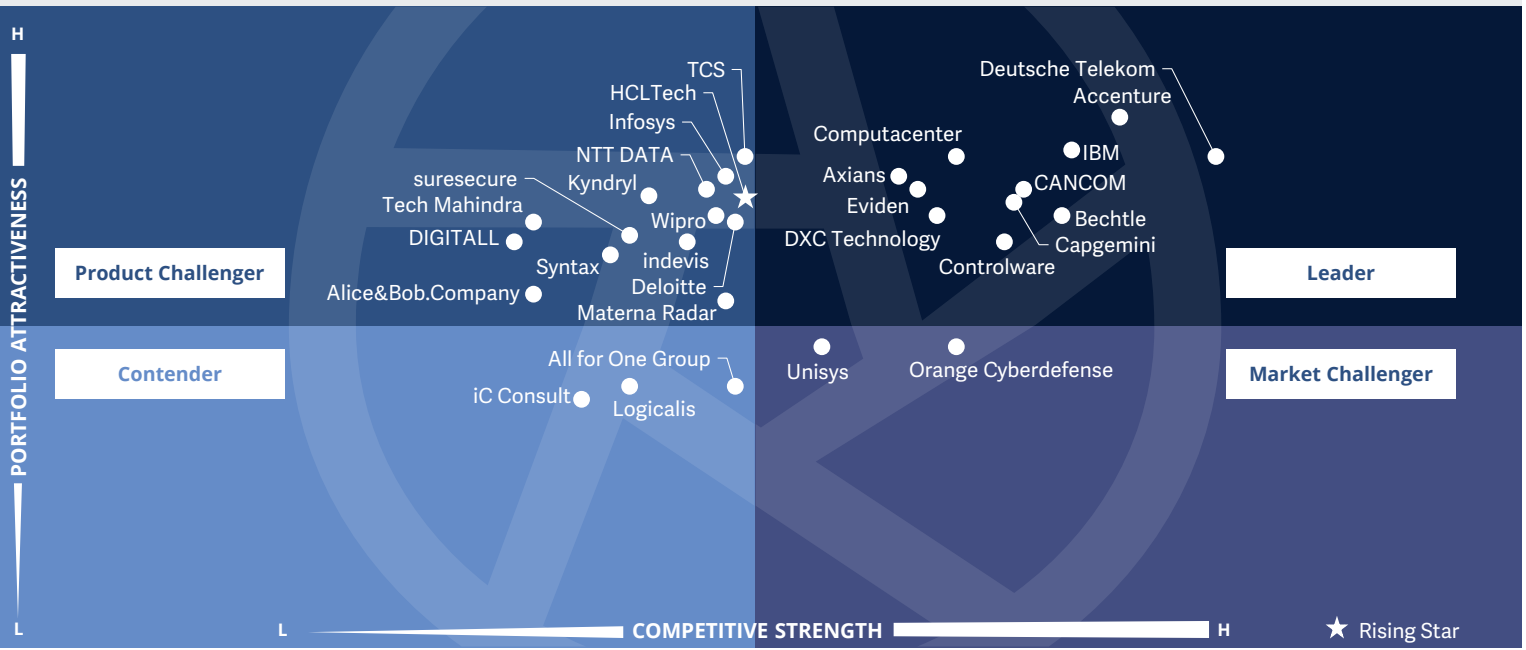
Auf Cybersicherheit und IT-Strategie spezialisierte **Berater und Advisors** unterstützt dieser Bericht dabei, die Wettbewerbslandschaft zu bewerten und geeignete TSS-Anbieter für spezifische Kundenbedürfnisse zu identifizieren.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Technical Security Services

Deutschland 2024



In diesem Quadranten geht es um die **relevantesten** Anbieter von technischen Security Services in Deutschland, deren Leistungen nicht nur die eigenen Produkte abdecken. Externe Provider spielen aufgrund des Fachkräftemangels **eine immer wichtigere Rolle**.

Frank Heuer

Definition

Die in diesem Quadranten bewerteten Anbieter von TSS offerieren Integrations-, Wartungs- und Supportleistungen für IT- und OT-Sicherheitsprodukte oder -lösungen. Diese Dienste decken alle Sicherheitsprodukte ab, u.a. Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, Unified Threat Management (UTM), OT Security, SASE und weitere Angebote.

TSS Provider bieten standardisierte Playbooks und Roadmaps an, die dabei helfen, eine bestehende Sicherheitsumgebung mit den besten Tools und Technologien umzugestalten, den Sicherheitsstatus zu verbessern und die Auswirkungen von Bedrohungen zu reduzieren. Ihre Portfolios sollen u.a. die vollständige oder individuelle Transformation bestehender Sicherheitsarchitekturen in Bereichen wie Netzwerken, Cloud, Arbeitsplatz, OT, IAM, Datenschutz und -sicherheit, Risiko- und Compliance-Management und SASE ermöglichen. Die Angebote beinhalten zudem die Identifizierung von Produkten oder Lösungen, Bewertung, Design und Entwicklung, Implementierung, Validierung, Penetrationstests, Integration und Bereitstellung.

TSS Provider investieren in den Aufbau von Partnerschaften mit Anbietern von Sicherheitslösungen und -technologien, um spezialisierte Akkreditierungen zu erlangen und ihr Portfolio zu erweitern. Dieser Quadrant umfasst auch klassische Managed Security Services, die ohne ein Security Operations Center (SOC) erbracht werden.

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf ihre eigenen Produkte fokussieren, sondern auch in der Lage sind, Lösungen anderer Anbieter zu implementieren und zu integrieren.

Auswahlkriterien

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

Beobachtungen

Für Unternehmen in Deutschland sind die immer intensiveren wie auch raffinierteren, komplexeren und ständig neuen Cyberattacken weiterhin eine Herausforderung. Dies wird erschwert durch den Mangel an Cybersecurity-Experten. Daher benötigen Firmen immer häufiger die Unterstützung externer Dienstleister. Vorteile besitzen dabei Provider, die aktuelle Technologien wie auch die Ansprache verschiedener Zielgruppen beherrschen.

Mittelständler zeigen besonderen Nachholbedarf, da sie besonders häufig unter Problemen wie dem IT-Fachkräftemangel leiden. Zunehmende, komplexere Sicherheitsbedrohungen und verschärfte gesetzliche Regelungen bewegen diese Firmen immer häufiger dazu, externe Unterstützung in Anspruch zu nehmen. Mittelständler schätzen dabei häufig die lokale Präsenz der Dienstleister für kurze Wege und unkomplizierte, schnelle Unterstützung.

Um auch im anspruchsvollen Großkundenmarkt erfolgreich zu sein, müssen die Anbieter große, auch internationale Erfahrung und Teams präsentieren können. 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.

IT-Security-Projekte sind häufig anspruchsvoll und vielfältig angelegt. Daher sind Provider im Vorteil, die umfangreiche Technical Security Services aus einer Hand bieten. Dabei können auch Dienstleister profitieren, die mit renommierten Technologieanbietern kooperieren und deren Mitarbeitende zahlreiche hochwertige Zertifizierungen vorweisen können.

Zudem sind Dienstleister im Vorteil, die ihren Kunden End-to-End-Sicherheitsdienstleistungen und auch zugehörige IT-Lösungen aus einem Guss anbieten können.

Von den 85 Anbietern, die in dieser Studie bewertet wurden, konnten sich 30 für diesen Quadranten qualifizieren. Dabei erreichten elf eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Umfangreiche Leistungen und kosteneffiziente Lösungen auf Basis von Robotic Process Automation machen **Accenture** zu einem führenden Anbieter von 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.

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

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

Mit seinen zielgerichteten und modularen technischen Cybersecurity-Dienstleistungen sowie seinen deutschen Wurzeln versteht es **Controlware**, im wachstumsstarken Mittelstandssegment erfolgreich zu sein.

Basierend auf einem großen, hoch qualifizierten Team sowie einem lückenlosen End-to-End-Service-Angebot made in Germany ist **Deutsche Telekom Security** Leader für Technical Security Services in Deutschland.

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

Eviden (an Atos Business) hat sich als führender Anbieter von Technical Security Services in Deutschland etabliert, unter anderem durch einen ganzheitlichen Cybersecurity-Ansatz, der auch die Geschäftsrelevanz betont.

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

HCLTech ist zunehmend erfolgreich und somit der Rising Star für Technical Security Services in Deutschland. Der Anbieter überzeugt mit internationaler Erfahrung, einem umfassenden Angebot und hochwertigen Technologiepartnerschaften.

Leader

„Basierend auf einem großen hoch qualifizierten Team und End-to-End-Services made in Germany ist Deutsche Telekom Security Leader für Technical Security Services in Deutschland."

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. 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.

Sehr großes, qualifiziertes Team: Die Nähe zum Kunden ist möglich durch die große Manpower – 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 Mitarbeiter geführt haben.

End-to-End-Lösungen für Cybersecurity: Die Deutsche Telekom bietet ihren Kunden lückenlose Technical Security Services, die ein komplettes Spektrum an Themen abdecken. Neben Technical Security Services werden auch Strategic Security Services und Managed Security Services aus einer Hand angeboten, so dass der gesamte Lifecycle eines Security-Projektes aus einem Guss möglich ist. Darüber hinaus ermöglicht die Deutsche Telekom aufgrund der generellen IT-Kompetenz auch IT-Lösungen mit damit verbundener Cybersecurity. Dabei ist insbesondere auch die spezielle Kompetenz der Deutschen Telekom hinsichtlich der Kombination von IT-Security und TK-Security hervorzuheben.

Herausforderungen

Ein weiterer Ausbau der globalen Präsenz könnte erwägenswert sein. 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.

Strategic Security Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für deutsche Unternehmen relevant, die Anbieter von strategischen Sicherheits-Services (SSS) evaluieren und sich über die Wettbewerbslandschaft informieren möchten. Anhand dieser Informationen können Unternehmen Anbieter auswählen, die in der Lage sind, die Sicherheitsreife zu bewerten, maßgeschneiderte Cybersicherheitsstrategien zu definieren und Risiken wirksam zu mindern.

Deutsche Unternehmen setzen auf Trends wie die Konsolidierung von Technologien für eine optimierte Sicherheitsinfrastruktur und die Einführung von Zero-Trust-Sicherheitsprinzipien, um ihre Cybersicherheit zu verbessern. Sicherheitstechnologien werden zudem verstärkt mit Firewalls, CASBs (Cloud Access Security Broker) und Threat-Intelligence-Plattformen integriert, um die Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen in Echtzeit zu verbessern.

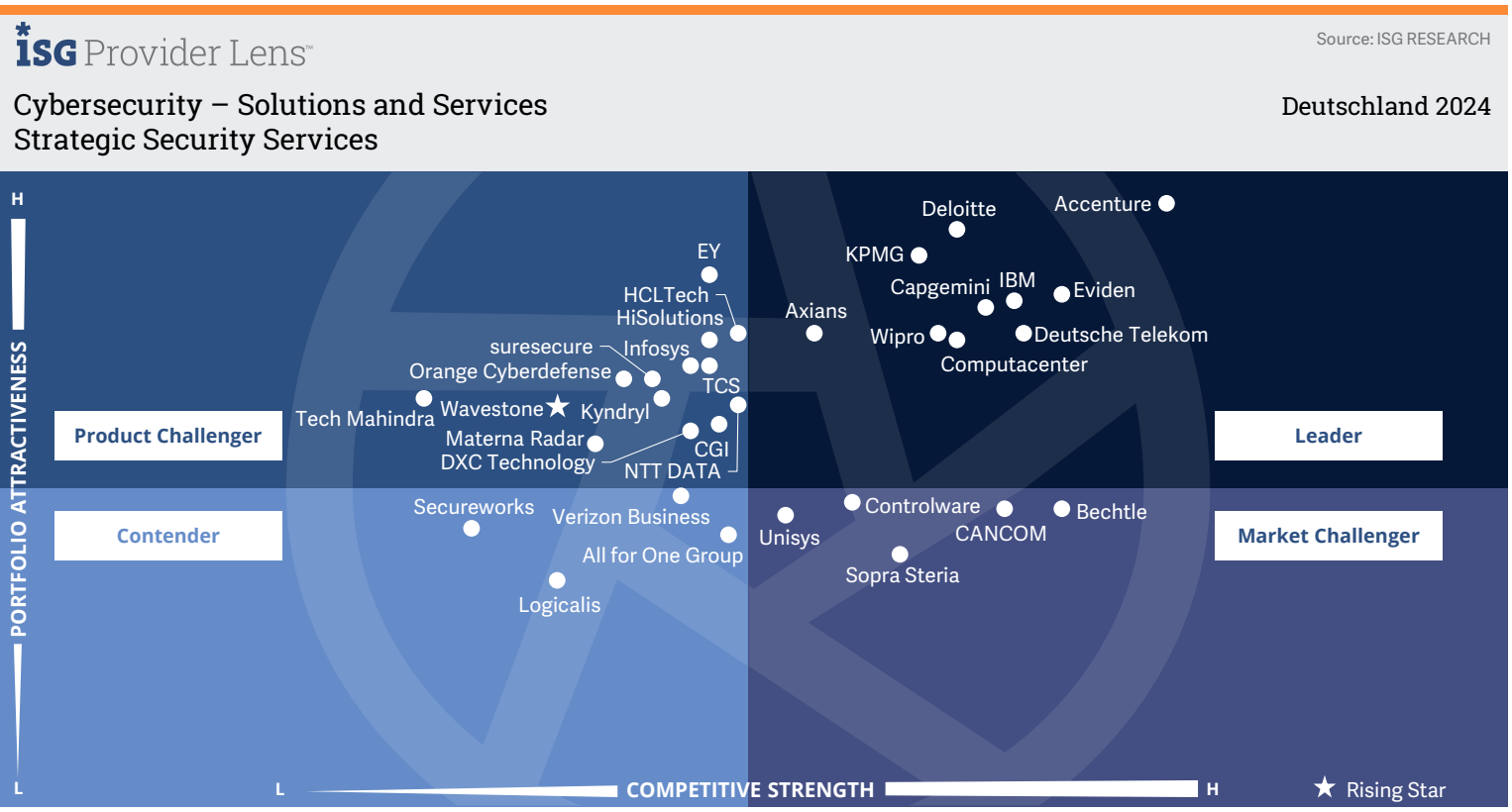
Die Dienstleister auf dem deutschen Markt bieten eine Reihe von Lösungen an, darunter die Absicherung von Edge Computing, die Implementierung von sicheren Internet-Gateway-Systemen und die Verbesserung von Zero-Trust-Philosophien durch kontextbezogene Zugangskontrollen. Darüber hinaus offerieren sie cloudbasierte Bereitstellungsmodelle, KI- und ML-gestützte Sicherheitskontrollen und konsistente Sicherheit in Multicloud-Umgebungen, um sich ändernde Kundenanforderungen zu erfüllen.

Dieser ISG-Bericht bietet wertvolle Einblicke in die Landschaft der SSS Provider und Branchentrends. Deutsche Unternehmen können so bei der Auswahl eines Dienstleisters fundierte Entscheidungen treffen; die Dienstleister wiederum können sich über Marktentwicklungen auf dem Laufenden halten und ihre Angebote an die sich wandelnden Sicherheitsanforderungen anpassen.

IT-Sicherheitsexperten erhalten mit diesem Bericht einen Einblick in die aktuelle Positionierung von SSS-Anbietern und können so deren Fähigkeiten bei der Bewertung des Sicherheitsreifegrads und der Definition maßgeschneiderter Cybersicherheitsstrategien besser evaluieren.

IT-Leiter gewinnen aus diesem Bericht ein besseres Verständnis der Marktlandschaft und der Trends im Bereich der Sicherheitsdienste, so dass sie fundierte Entscheidungen bei der Auswahl von Dienstleistern treffen können.

Compliance-Beauftragte sollten diesen Bericht lesen, um die Einhaltung von Sicherheitsstandards und -vorschriften gewährleisten und die darin enthaltenen Informationen zur Verbesserung der Sicherheitslage nutzen zu können.



In diesem Quadranten geht es um die **relevantesten** Cybersecurity-Berater in Deutschland, die Leistungen nicht nur für die eigenen Produkte offerieren. Im Zuge steigender Cyberbedrohungen und neuer Technologien sind ihre Services **zunehmend gefragt**.

Frank Heuer

Definition

Die in diesem Quadranten bewerteten Provider von Strategic Security Services bieten Beratung für IT- und OT-Sicherheit an. Die abgedeckten Leistungen umfassen Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zu Sicherheitslösungen sowie Sensibilisierungstrainings und Schulungen. Die Anbieter helfen auch bei der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition einer auf den individuellen Anforderungen basierenden Cybersecurity-Strategie für Unternehmen.

Diese Provider sollten Sicherheitsberater beschäftigen, die über umfassende Erfahrung mit der Planung, Entwicklung und Verwaltung von umfassenden Sicherheitsprogrammen für Unternehmen verfügen. Angesichts des wachsenden Bedarfs an solchen Diensten bei KMUs und des Fachkräftemangels sollten diese Experten auch auf Abruf durch vCISO (Virtual Chief Information Security Officer) Services zur Verfügung gestellt werden. Angesichts der zunehmenden Bedeutung der Cyber-Resilienz sollten SSS-Anbieter in der Lage sein, Business Continuity Roadmaps zu formulieren und geschäftskritische Anwendungen für die Wiederherstellung zu priorisieren. Außerdem sollten sie regelmäßig so genannte Tabletop Exercises und Cyber Drills für Vorstandsmitglieder, wichtige Führungskräfte und Mitarbeiter durchführen, um sie besser mit Cybersecurity-Themen vertraut zu machen und Best Practices einzuführen, damit sie besser auf tatsächliche Bedrohungen und Cyber-Angriffe reagieren können. Sie sollten zudem mit den auf dem Markt erhältlichen Sicherheitstechnologien und -produkten vertraut sein und Unternehmen bei der Auswahl des besten Produkts und Anbieters für die spezifischen Anforderungen entsprechend beraten.

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf eigene Produkte oder Lösungen fokussieren. Die hier analysierten Dienste decken alle Sicherheitstechnologien ab, u.a. auch OT-Sicherheit und SASE.

Auswahlkriterien

1. Nachweisliche Leistungen in SSS-Bereichen wie **Evaluierung, Assessments, Anbieterauswahl, Architekturberatung und Risikoberatung**
2. **Angebot von mindestens einem der oben genannten** Strategic Security Services im jeweiligen Land
3. Erbringung von **Sicherheitsberatungsdiensten unter Verwendung von Frameworks** ist von Vorteil
4. **Kein ausschließlicher Fokus auf proprietäre Produkte** bzw. Lösungen

Beobachtungen

Die Cybersecurity-Gefährdungssituation eskaliert weiterhin. Der Ukraine-Krieg ist dabei nur das herausragendste Beispiel für das Anfachen von Bedrohungen. Zusammen mit mangelnden Ressourcen bewirkt dies ein zunehmendes Bedürfnis nach Orientierung hinsichtlich Cybersicherheit. Für die nächste Zukunft zeichnen sich zudem neue, technisch ausgefeilte Bedrohungen ab.

Angesichts immer intensiverer und raffinierterer Cyberattacken – auch im Zuge von geopolitischen Konflikten – sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Davon sind schon lange nicht mehr nur bekannte Großunternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelgroße Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin; darunter leidet besonders der Mittelstand. Diese Faktoren bewirken, dass Unternehmen zunehmend externe Unterstützung benötigen. Am Anfang steht hierbei häufig die Beratung.

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

Des Weiteren sind Dienstleister, die ihren Kunden neben Sicherheitsberatung auch -Umsetzung und -Betrieb anbieten können, damit die Strategie bruchlos in die Tat umgesetzt werden kann, im Vorteil; ebenso wie Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen – gegebenenfalls auch zugehörige neugestaltete Geschäftsprozesse – aus einem Guss anbieten können. Erste Berater stellen sich auf die Abwehr von quantum-basierenden Cyberattacken ein.

Secureworks und Zensar sind nicht mehr im Quadranten vertreten.

Von den 85 Anbietern, die in dieser Studie bewertet wurden, konnten sich 33 für diesen Quadranten qualifizieren. Dabei erreichten zehn eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

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

axians

Mit seinem pragmatischen, zielgerichteten Ansatz in der Cybersecurity-Beratung entspricht **Axians IT Security** den Bedürfnissen der mittelständischen Zielgruppe. Zudem wird das Portfolio dynamisch weiterentwickelt.

Capgemini

Capgemini überzeugt seine deutschen Kunden im Cybersecurity Consulting 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.

Deloitte.

Deloitte hat 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 Berater zu Cybersecurity in Deutschland.

Eviden (an Atos Business) hat sich als neuer Anbieter mit ganzheitlichem Ansatz und zahlreichen Zertifizierungen im deutschen Markt für Cybersecurity-Beratung als Leader etabliert.

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

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

Wipro überzeugt seine Kunden in Deutschland mit umfassendem technischem Know-how und umfangreichen Services sowie einem kundenorientierten Preismodell für Cybersecurity-Beratung.

Wavestone

Mit der aufsehenerregenden Vereinigung mit Q_PERIOR erhöht **Wavestone** schlagartig seine Präsenz im deutschen Markt und positioniert sich auf Anhieb als der Rising Star für Cybersecurity-Beratung.

Leader

„Mit großer Erfahrung in anspruchsvollen Umgebungen überzeugt die Deutsche Telekom als Berater zu Cybersecurity in Deutschland."

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. Der Hauptsitz befindet sich in Bonn. 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 Mitarbeiter 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.

Integrierte 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.

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.

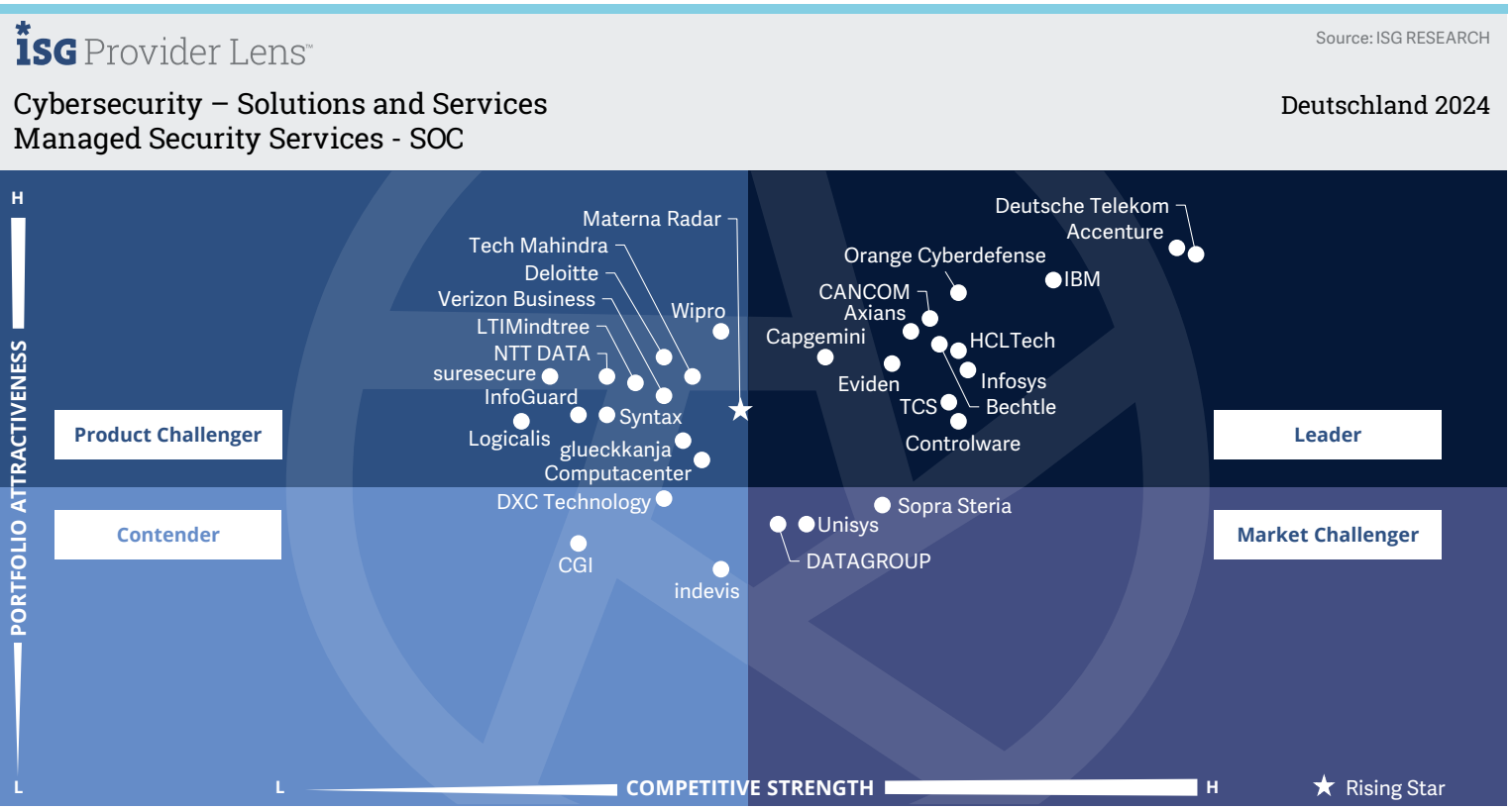
Deutsche Unternehmen wünschen sich robuste Sicherheitslösungen, um der zunehmenden Zahl von Cyberbedrohungen zu begegnen, insbesondere im Hinblick auf Remote-Arbeit und cloudbasierte Dienste. Sie benötigen kontinuierliche Überwachung, Funktionen zur Erkennung von hochkomplexen Bedrohungen sowie Unterstützung 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.

Managed Security Services – SOC (Midmarket)

Wer sollte dieses Kapitel lesen

Dieser Bericht ist relevant für mittelständische Unternehmen in Deutschland, um sich über den Markt für Managed Security Services (MSS) zu informiert, 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..

Mittelständler in Deutschland 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.

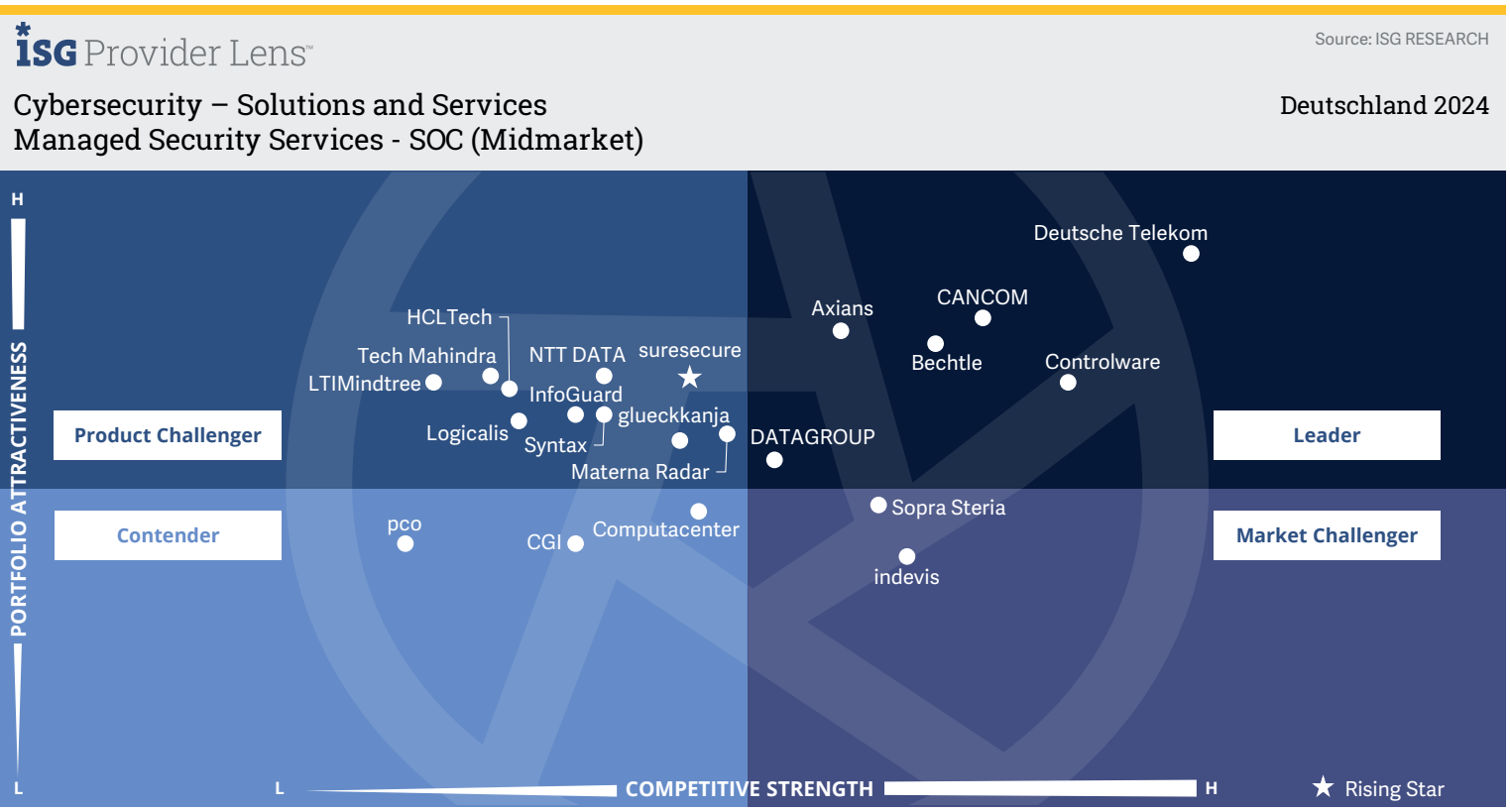
Diese Unternehmen setzen vor allem auf IT-Investitionen, um technologisch auf dem neuesten Stand zu bleiben, und nutzen Technologien wie Cloud Computing, Big Data und IoT, um die betriebliche Effizienz zu steigern und das Umsatzwachstum zu fördern.

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 zudem die wachsende Nachfrage nach Zero-Trust und SASE Frameworks und stellen sicher, dass Unternehmen Zugang zu den neuesten Sicherheitstechnologien und Fachkenntnissen haben, um ihren Betrieb vor den sich entwickelnden Bedrohungen zu schützen.

IT-Sicherheitsverantwortliche erhalten durch diesen Bericht Einblicke in die aktuelle Marktlandschaft der MSS-Anbieter und die neuesten Trends in Bezug auf Sicherheitstechnologien und -dienste.

Chief Technology Officers können sich mit diesem Bericht über die neuesten Trends und Technologien auf dem MSS-Markt informieren und so fundierte Entscheidungen treffen.

Chief Information Officers erfahren aus diesem Bericht, wie MSS-Anbieter kritische Marktherausforderungen angehen, und können die potenziellen Auswirkungen auf die IT-Strategie und den IT-Betrieb ihres Unternehmens evaluieren.



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Managed Security Services aus SOCs** für deutsche Mittelständler, ohne Provider, die nur eigene Produkte betreuen. Der **Fachkräftemangel** bewirkt eine zunehmende Nachfrage.

Frank Heuer

Definition

Die im Managed Security Services – SOC- (MSS-SOC-) Quadranten (Midmarket) 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 aus dem Segment der mittelständischen Unternehmen 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. Das gilt insbesondere für das Segment der mittelständischen Firmen, die immer mehr in das Blickfeld von Cyberkriminellen geraten und gleichzeitig noch mehr als die großen Unternehmen unter dem IT-Fachkräftemangel leiden. 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. Speziell für mittelständische Firmen sind auch kostenattraktive und bedarfsgerechte (modulare) Lösungen interessant.

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. **Optimal sind bedarfsgerechte**, modulare Leistungs- und Preismodelle

Beobachtungen

Mittelständische Unternehmen in Deutschland sind noch stärker als Großunternehmen vom Cybersecurity-Fachkräftemangel betroffen. Gleichzeitig sind auch sie mit immer mehr, immer neuen und immer komplexeren Sicherheitsherausforderungen konfrontiert und geraten öfter ins Visier von Cyberkriminellen, die in dieser Zielgruppe leichte Opfer vermuten. Daher sind auch mittelgroße Unternehmen verstärkt auf externe Dienstleistungen wie z.B. durch Security Operations Centers angewiesen. SOCs verfügen über das erforderliche stets aktuelle Spezialistenwissen und die Ausrüstung für eine laufende Überwachung der Kundensysteme.

Für das Mittelstandssegment sind SOCs in Deutschland aus Gründen des Vertrauens und des Datenschutzes ein Pluspunkt. Zudem wissen die Entscheider in mittelständischen Unternehmen die räumliche Nähe zu Dienstleistern zu schätzen. Auch deutschsprachige Ansprechpartner spielen für diese Kundengruppe eine wichtige Rolle. Viele Mittelständler bieten ihren eigenen Kunden pragmatische, schnelle Lösungen – und erwarten daher oft auch von ihren Dienstleistern eine unkomplizierte, rasche Umsetzung, auch ein rasches Onboarding bei SOC Services.

Auch Mittelständler erwarten von SOC-Dienstleistern eine hohe Innovationskraft, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählen unter anderem die Nutzung von künstlicher Intelligenz und Automatisierung, um auch komplexere Bedrohungen zu meistern. 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 21 für diesen Quadranten qualifizieren. Dabei erreichten sechs eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

axians

Mit umfangreichen und bedarfsgerechten SOC 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 SOC Services für den deutschen Mittelstand.

CANCOM

CANCOM baut seine SOC Services aus und kann so seine Position als führender Dienstleister für den deutschen Mittelstand stärken.

controlware

Controlware ist mit flexiblen, kundenorientierten Services ein Leader im Markt für SOC Services für den deutschen Mittelstand.

DATAGROUP

DATAGROUP gelingt mit hochwertigen, integrierten Services der Sprung unter die führenden Anbieter von Managed-Security-/SOC-Dienstleistungen für den deutschen Mittelstand.

Deutsche Telekom Security ist mit einem großen Team und einem umfangreichen Angebot der führende Anbieter von Managed-Security-/SOC-Dienstleistungen für den deutschen Mittelstand.

sure[secure]

suresecure ist mit der Konzentration auf die dynamisch wachsende Zielgruppe und einer innovativen Technologieplattform der Rising Star für Managed-Security-/SOC-Dienstleistungen für den deutschen Mittelstand.

Leader

„Die Deutsche Telekom ist der führende Anbieter von Managed-Security-/SOC-Dienstleistungen für den deutschen Mittelstand."

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. Der Hauptsitz befindet sich in Bonn. Das SOC kombiniert auf maschinellem Lernen basierende künstliche Intelligenz, Verhaltensanalysen und Threat Hunting.

Stärken

Services aus Deutschland: Die Deutsche Telekom bietet „Security made in Germany" und betreibt ihre Managed Security Services unter anderem in Deutschland, was besonders von vielen Mittelstandskunden geschätzt wird. Der Anbieter betreibt hochmoderne Cyber Defense & Security Operations Center und generiert als globaler Carrier umfangreiche Threat Intelligence. Mit „Security made in Germany" kann die Deutsche Telekom speziell angesichts der Datenschutzdiskussion – und besonders in der Zielgruppe des Mittelstandes – punkten.

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. Der Anbieter ist zudem in der Lage, ein speziell für den Mittelstand angepasstes Portfolio (MDR Pro) anzubieten.

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 Komplexität des Schutzes eines globalen Unternehmenskunden und verfügen über das nötige Wissen und die Erfahrung, um Kunden mit dem gleichen hohen Standard schützen zu können.

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.

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.

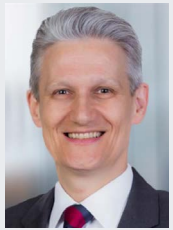
ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. Die für diesen Bericht erhobenen Daten und Informationen, entsprechen nach Ansicht von ISG sowohl für Anbieter, die aktiv teilgenommen haben, als auch für Anbieter, die 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.

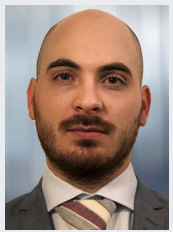
Zu seinen Aufgabengebieten gehört vor allem die Beratung von ICT-Anbietern zum strategischen und operativen Marketing sowie Vertrieb. Herr Heuer ist als Sprecher bei Konferenzen und Webcasts zu seinen Themenschwerpunkten im Einsatz und Mitglied des IDG-Expertennetzwerks. Herr Heuer ist seit 1999 als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