ISG Provider Lens™

Cybersecurity – Services and Solutions

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

Customized report courtesy of:

controlware

QUADRANT REPORT | JULI 2025 | DEUTSCHLAND, GLOBAL

Inhaltsverzeichnis

Seite 1 von 2

Autor des Berichts: Frank Heuer

Technologische Revolution und Fachkräftemangel treiben den deutschen Cybersecurity-Markt

Unter zunehmend herausfordernden Umständen nehmen die Cyberbedrohungen für deutsche Unternehmen im Zuge immer raffinierterer, häufigerer, komplexerer und wandlungsfähigerer Cyberattacken zu. Durch den Mangel an qualifizierten Cybersecurity-Fachleuten wird die Situation noch verschärft und die Nachfrage nach externen Dienstleistungen gefördert. Neue Technologien begünstigen Cyberbedrohungen, bieten zugleich aber auch neue Geschäftschancen für Dienstleister. Service Provider, die sich auf die Anforderungen verschiedener Zielgruppen verstehen und neben technischen auch geschäftliche und regulatorische Aspekte beherrschen, können hier zusätzlich profitieren.

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 vermehrt 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-

Multiple Herausforderungen fördern die Nachfrage nach externen Security-Dienstleistungen

Zusammenfassung

Ansatzes und zum Bedeutungsverlust der 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, und IT-Verantwortliche verstärkt 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, immer häufiger auf proaktive statt reaktive Methoden, die zum Beispiel auf künstlicher Intelligenz basieren.

Nicht nur der Eigenschutz der Unternehmen, 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 nach wie vor eine große Herausforderung dar. Aktuell steht zudem vielen Mittelständlern aus bestimmten Branchen die Einstufung als besonders zu schützende Infrastruktur bevor. Daraus werden unter anderem forcierte Schutzerfordernisse und -maßnahmen hinsichtlich der Cybersecurity abgeleitet. Die zugrundeliegende EU-Richtlinie NIS-2 wird voraussichtlich 2025 in nationales Recht umgesetzt.

Die mittelständischen Unternehmen sind 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, die inzwischen deutlich drängender geworden ist. Während bisher davon ausgegangen wurde, dass im Zuge der technischen Entwicklung noch bis Ende des Jahrzehnts Zeit für konkrete Gegenmaßnahmen bliebe, hat sich dies durch neue kriminelle Strategien geändert. Mit dem „Harvest now – decrypt later"-Ansatz wurde inzwischen klar, dass der Schutz von Daten in Form der Verschlüsselung dringender als bisher angenommen überprüft und gegebenenfalls verstärkt werden muss. Demzufolge hat sich die Zahl der Dienstleister, die sich mit ihrer Beratung auf diese neue Art der Bedrohung eingestellt und ein neues Geschäftsfeld erschlossen haben, in den letzten zwei Jahren stark erhöht. Diese Consulting-Angebote werden derzeit noch vor allem von Banken und Versicherungen in Anspruch genommen, da ihre Vermögenswerte aus virtuellen Assets bestehen und sie somit potenziell besonders gefährdet sind. Aufgrund der oben geschilderten dynamischen Entwicklung steigt die Nachfrage auch in anderen Wirtschaftszweigen stark an.

Data Leakage/Loss Prevention & Data Security (Produkte)

Das Interesse an DLP-Lösungen hat in Deutschland in den letzten Jahren wieder 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. Ein weiterer Treiber für die DLP-Nutzung sind zunehmende regulatorische Vorgaben. Künstliche Intelligenz unterstützt Hersteller beim Angebot leistungsfähiger Lösungen.

Technical Security Services

Aufgrund immer raffinierterer Cyberangriffe und des drängenden Fachkräftemangels sind Unternehmen und Behörden in Deutschland 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.

Strategic Security Services

Deutsche Unternehmen sind angesichts der immer häufigeren, intensiveren und 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 diese Situation auch weiterhin.

Unter anderem sind Dienstleister im Vorteil, die ihren Kunden bruchlose End-to-End Services und die Integration von IT- und Security-Lösung aus einer Hand bieten können. Darüber hinaus ist die tiefe Kenntnis regulatorischer Regelungen immer stärker gefragt, und die Beratung zu Post-Quantum Encryption gewinnt schneller als bisher erwartet an Bedeutung.

Next-Gen SOC/MDR Services

Die immer anspruchsvolleren Cyberattacken fördern besonders auch die Nachfrage nach Diensten von Security Operations Centers (SOCs) sowie Managed Detection & Response (MDR) Services. 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 (digitale Souveränität)

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.

Quantumtechnologie wird schneller als erwartet zu einer Bedrohung für Anwender, bietet aber wie künstliche Intelligenz auch neue Chancen für Cybersecurity-Dienstleister. Vorteile haben dabei Service-Anbieter, die eine ausgewogene Zielgruppe adressieren und sowohl technische als auch regulatorische Aspekte beherrschen.

Autor des Berichts:
Bhuvaneshwari Mohan (Global- IAM)

KI-gesteuerte Funktionen, Zero Trust und eine nahtlose UX sind integraler Bestandteile von IAM

Die Notwendigkeit eines robusten Identity & Access Managements (IAM) bzw. Identitäts- und Zugriffsmanagements spielt aufgrund der zunehmenden Cyberbedrohungen, der stärkeren Nutzung hybrider Arbeitsmodelle und der weit verbreiteten Einführung von Cloud-Technologien eine entscheidende Rolle. IAM bildet für Unternehmen die Grundlage für einen sicheren Betrieb, um innovativ zu sein und gleichzeitig strenge gesetzliche Auflagen zu erfüllen.

Strategische Bedeutung von IAM für Unternehmen: IAM ist die Grundlage für den Aufbau einer stabilen Sicherheitsstruktur, die sich an neu entstehende Bedrohungen und Geschäftsanforderungen anpasst und die Sicherheit durch ein geringeres Risiko von unbefugten Zugriffen und Datenverletzungen erheblich verbessert. Wichtige Sicherheitsmaßnahmen wie adaptive und kontextabhängige Zugangskontrollen, kontinuierliche Identitätsrisikobewertungen und Zero-Trust-Architekturen bilden das Rückgrat solcher Bestrebungen. Adaptive Zugangskontrollen mit Echtzeit-Analysen erkennen ungewöhnliches Verhalten und gehen wirksam dagegen vor. Zero-Trust Frameworks in IAM-Systemen entwickeln sich zum Standard für die Sicherung des Zugriffs, unabhängig von Standort oder Gerät des Benutzers. Der Eckpfeiler von Zero Trust ist eine strenge Identitätsüberprüfung und Zugangskontrolle; daher benötigen Unternehmen robuste Authentifizierungsmechanismen.

IAM verbessert nicht nur die Sicherheit, sondern erleichtert auch die Einhaltung gesetzlicher Vorschriften wie DSGVO, HIPAA, CCPA, SOX und PCI DSS durch Echtzeit-Audit-Trails und die automatische Bereitstellung von Benutzerzugängen. Diese Funktionen gewährleisten Einblick in die Benutzeraktivitäten und schützen sensible Daten; so wird unbefugter Zugriff verhindert.

Da ein identitätszentrierter Ansatz in den **Mittelpunkt rückt**, ist IAM zu einer **strategischen Notwendigkeit** geworden.

IAM vereinfacht auch die Einhaltung komplexer Vorschriften, so dass sich Unternehmen auf ihr Kerngeschäft konzentrieren können.

Die IAM-Landschaft befindet sich im Umbruch, angetrieben durch den Bedarf an sicheren, nahtlosen Identitätslösungen und die sich verändernden organisatorischen Anforderungen. Nachstehend werden die wichtigsten IAM-bezogenen Trends aufgeführt, die ISG beobachtet hat:

Dezentrale Identitäten: Eine der vielversprechendsten Entwicklungen sind dezentrale Identitätsmodelle, die unter Einsatz der Blockchain-Technologie den Nutzern die Kontrolle über ihre digitalen Identitäten geben und zustimmungsbasierte Authentifizierung und Datenschutz ermöglichen. Sowohl überprüfbare Berechtigungsnachweise als auch dezentralisierte Identifikatoren sind wichtige Standards für dezentralisierte Identitäten. Das Customer Identity & Access Management (CIAM) gewinnt mit dem Aufkommen dezentraler Identitäten zunehmend an Bedeutung, da der Datenschutz, die Sicherheit und die nutzerzentrierte Kontrolle über persönliche Daten immer mehr in den Vordergrund rücken.

Zunahme von Identity as a Service (IDaaS): Die hohen Wachstumsraten von IDaaS unterstreichen den Wechsel hin zu Cloud-First-Architekturen. IAM-Anbieter verbessern ihre IDaaS-Plattformen, um sie nahtlos in SaaS-Anwendungen und Multicloud- und Hybrid-Cloud-Infrastrukturen integrieren zu können. Dieser Trend ermöglicht mehr Flexibilität, Skalierbarkeit und Sicherheit und auch eine schnelle Anpassung an die dynamischen Anforderungen von Unternehmen und Mitarbeitenden.

Marktkonsolidierung und strategische Übernahmen: Die anhaltende Konsolidierung auf dem IAM-Markt spiegelt die strategischen Bemühungen der Anbieter wider, fortschrittliche Technologien zu integrieren und ihre Produktmöglichkeiten zu erweitern. Zum Beispiel verändern die anhaltenden Investitionen von Microsoft in diesem Bereich die Wettbewerbslandschaft. Diese Entwicklungen treiben zwar Innovationen voran, erhöhen aber auch die Abhängigkeit von einigen wenigen marktbeherrschenden Akteuren.

Einführung der biometrischen Authentifizierung und des passwortlosen Zugangs: Unternehmen setzen zunehmend auf biometrische Authentifizierung und passwortlosen Zugang, um die Sicherheit und Benutzerfreundlichkeit zu verbessern. Diese Methoden, u.a. Gesichtserkennung, Fingerabdruck-Scanning und FIDO2-basierte Schlüssel, reduzieren die Abhängigkeit von Passwörtern, verringern das Phishing-Risiko und entsprechen den Zero-Trust-Prinzipien für eine starke Identitätssicherung.

Branchenspezifische IAM-Lösungen: Die individuellen Anforderungen der verschiedenen Branchen erfordern maßgeschneiderte IAM-Lösungen. Organisationen des Gesundheitswesens müssen die HIPAA-Vorgaben einhalten und elektronische Gesundheitsakten (EHRs) schützen; dafür kommen granulare Zugangskontrollen und sichere Telemedizinplattformen zum Einsatz. Finanzdienstleister müssen die SOX- und PCI DSS-Standards einhalten und deshalb robuste Maßnahmen wie Verhaltensanalysen und Multifaktor-Authentifizierung (MFA) implementieren, um Betrug zu verhindern und die Datenintegrität zu gewährleisten. Einzelhändler benötigen skalierbare IAM-Lösungen zum Schutz der Kundendaten und für die effiziente Verwaltung des Zugriffs durch Mitarbeitende in Stoßzeiten.

Technologischer Fortschritt und Produktinnovationen: Der IAM-Markt entwickelt sich weiter; zu den Innovationen zählen KI-gesteuerte Identitätsanalysen, kontextbezogene Authentifizierung und tiefe Integrationen mit Cloud-Plattformen. KI und ML spielen in IAM-Lösungen eine wichtige Rolle; sie analysieren und erkennen ungewöhnliches Nutzerverhalten und passen die Zugriffskontrollen automatisch auf Basis von Echtzeitinformationen an. Durch diese Weiterentwicklungen werden IAM-Systeme besser darin, Anomalien zu erkennen, Zugriffsentscheidungen dynamisch anzupassen und hybride Cloud- und Multicloud-Umgebungen zu unterstützen. Identitäts- und Bedrohungserkennungs- und Reaktionslösungen (Identity & Threat Detection & Response, ITDR) entwickeln sich zu einem wichtigen Aspekt von IAM,

da sie sich auf die proaktive Erkennung von Bedrohungen, die Echtzeitüberwachung und die Erkennung von Anomalien fokussieren, um identitätsbezogene Angriffe wirksam bekämpfen zu können.

Herausforderungen bei der Implementierung von IAM

Die Abstimmung von IAM auf Legacy-Systeme, Cloud-Plattformen und Anwendungen von Drittanbietern bringt für Unternehmen oft komplexe Integrationsprobleme mit sich. Diese technischen Hürden erfordern häufig spezielles Know-how gehen mit längeren Implementierungszeiten einher. Die sich schnell entwickelnde Bedrohungslandschaft und die erforderliche höhere Benutzerfreundlichkeit ohne Beeinträchtigung der Sicherheit erschweren die IAM-Implementierung zusätzlich.

Unternehmen müssen Kriterien wie eine nahtlose Integration, verbesserte Benutzererfahrung, Produkteffektivität und verbesserte Kosten- und Lizenzmodelle gründlich auf den Prüfstand stellen, damit der ausgewählte IAM-Anbieter ihren Sicherheitsanforderungen, Geschäftszielen und Compliance-Anforderungen auch wirklich gerecht wird.

Die zunehmende Integration von KI in die Identitätssicherheit birgt auch viele Gefahren, wie KI-Modellvergiftung, Modelldiebstahl und synthetische Identitäten. Daher sollten KI-gestützte IAM-Systeme die Einhaltung der Zero-Trust-Prinzipien, die Stärkung von IAM-Konfigurationen, die regelmäßige Überprüfung und das Testen von KI-Modellen sowie einen hybriden Ansatz berücksichtigen, bei dem KI zur Unterstützung eingesetzt wird, die menschliche Aufsicht bei der Entscheidungsfindung aber erhalten bleibt.

Der IAM-Markt ist im Zuge der zunehmenden Cyberbedrohungen, des regulatorischen Drucks und der digitalen Transformation auf Wachstumskurs. Investitionen in dezentrale Identitätsmodelle, IDaaS und KI-gesteuerte Lösungen werden wahrscheinlich zunehmen. Chancen liegen in der Entwicklung branchenspezifischer Lösungen, die den besonderen rechtlichen und betrieblichen Anforderungen gerecht werden. Neue adaptive Echtzeit-Sicherheitsmaßnahmen, Identity Governance und Compliance Management werden die UX in den Vordergrund stellen.

IAM dient als strategischer Wegbereiter, der die Compliance unterstützt, Innovationen fördert und die Benutzererfahrung verbessert. Mit der Weiterentwicklung der digitalen Landschaft spielen Investitionen in fortschrittliche IAM-Lösungen für Unternehmen, die ihre Abläufe sichern und in einer vernetzten Welt wachsen wollen, eine entscheidende Rolle.

Dieser Bericht untersucht die strategische Bedeutung von IAM für Unternehmen aller Größenordnungen, geht auf die wichtigsten IAM-Anbieter und ihre Fähigkeiten aus einer globalen Perspektive ein und bietet einen detaillierten Überblick über die Marktlandschaft. Identitätslösungen von Hyperscalern wie AWS und Google (Cloud) werden nicht bewertet, da sie in erster Linie für die Sicherung der eigenen Cloud-Ökosysteme konzipiert sind und nicht als eigenständige Angebote verkauft werden.

Im Mittelpunkt von Zero Trust stehen eine strenge Identitätsüberprüfung und eine strikte Zugangskontrolle; der Schwerpunkt liegt dabei auf einer kontinuierlichen, risikobasierten Authentifizierung. Unternehmen müssen über die traditionellen Methoden hinausgehen und passwortlose Lösungen, biometrische Authentifizierung und Verhaltensanalysen einsetzen. Kontextbezogene Risikobewertungen in Echtzeit sorgen für einen dynamischen Zugriff und proaktive statt reaktiver Identitätssicherheit, was in der heutigen, sich ständig weiterentwickelnden Bedrohungslandschaft von entscheidender Bedeutung ist.

Autor des Berichts:
Gowtham Sampath (Global-XDR)

XDR adressiert komplexe IT-Umgebungen und den Fachkräftemangel mit verbesserter Transparenz und Automatisierung

Der Markt für erweiterte Erkennung und Reaktion (Extended Detection & Response, XDR) gewinnt im Zuge der Nachfrage nach konsolidierten, erkenntnisgestützten Sicherheitsabläufen schnell an Reife. In Reaktion auf die zunehmend komplexen Cyberbedrohungen gehen Unternehmen von isolierten Erkennungstools zu einheitlichen Plattformen über, die umfassende Transparenz, Automatisierung und kontextbezogene Analysen für Endgeräte, Netzwerke, Cloud Workloads und Identitäten bieten. XDR hat sich von einem ergänzenden Nischenprodukt für EDR (Endpoint Detection & Response) zu einer Kernkomponente moderner Security Operations Center-Strategien entwickelt und ermöglicht eine proaktive Bedrohungssuche, eine schnelle Eindämmung und eine koordinierte Reaktion über die gesamte Angriffsfläche hinweg.

Den Kern dieser Transformation bildet die umfassende Einführung von KI, ML und Verhaltensanalysen, die inzwischen hinter vielen Erkennungs-, Korrelations- und Priorisierungs-Engines innerhalb der XDR-Plattformen stehen. Diese Technologien reduzieren Fehlalarme und ermöglichen eine frühzeitige Erkennung von Anomalien sowie eine fortschrittliche Bedrohungsmodellierung. Die zunehmende Integration von cloud-nativer Sicherheit und Zero-Trust Frameworks spiegelt die Erkenntnis des Marktes wider, dass Sicherheitsperimeter dynamisch und identitätsgesteuert sind. XDR-Plattformen sind zunehmend auf MITRE ATT&CK abgestimmt und unterstützen Continuous Threat Exposure Management (CTEM) und automatisierungsfokussierte Reaktions-Modelle.

Wichtige Trends und Entwicklungen

- **Agentenbasierte KI:** Die Integration von agentenbasierter KI (autonome, zielorientierte Systeme) revolutioniert XDR-Plattformen. Diese KI-Agenten können selbstständig Bedrohungen erkennen, untersuchen und auf sie reagieren, wodurch die Abhängigkeit von menschlichen

Die Weiterentwicklung von XDR **vereinheitlicht die Verteidigungsmaßnahmen** und fördert eine proaktive, intelligente **Cyberresilienz**.

Eingriffen verringert und die Reaktionszeiten verkürzt werden.

- **Verlagerung hin zu offenen und modularen Architekturen:** Unternehmen wünschen sich XDR-Lösungen mit offenen Architekturen, die eine nahtlose Integration mit bestehenden Sicherheitstools und Anwendungen von Drittanbietern ermöglichen. Dieser modulare Ansatz erhöht die Flexibilität und gewährleistet einen umfassenden Überblick über Bedrohungen in verschiedenen Umgebungen.
- **Integration von Verhaltensanalysen zur Erkennung von internen Bedrohungen:** Fortschrittliche Verhaltensanalysen verfolgen Abweichungen vom typischen Benutzerverhalten und können so interne Bedrohungen aufdecken. Dieser proaktive Ansatz ermöglicht die frühzeitige Erkennung potenzieller Sicherheitsverletzungen, die innerhalb des Unternehmens passieren.
- **Continuous Threat Exposure Management (CTEM):** XDR-Plattformen integrieren CTEM, um Echtzeitbewertungen der Sicherheitslage eines Unternehmens zu ermöglichen. Unternehmen können durch die Bewertung von Schwachstellen und potenziellen Angriffsvektoren Prioritäten für die Behebung von Problemen setzen.
- **Einbeziehung der Betriebstechnologie (Operational Technolog, OT):** XDR-Lösungen weiten ihre Fähigkeiten auf die Absicherung von OT-Umgebungen aus und stellen sich den besonderen Herausforderungen von Industriesystemen und kritischen Infrastrukturen. Diese Erweiterung gewährleistet einen umfassenden Schutz für IT- und OT-Bereiche.
- **Integration von Wissensgraphen:** XDR-Plattformen nutzen Wissensgraphen zur Abbildung der Beziehungen zwischen verschiedenen Einheiten innerhalb einer Organisation. Diese Integration liefert kontextbezogene Bedrohungsdaten, wodurch sich Bedrohungen genauer erkennen und Reaktionsstrategien verbessern lassen.
- **KI-gesteuertes Insider-Risikomanagement (IRM):** Fortschrittliche IRM-Systeme auf Basis von KI werden in XDR-Plattformen integriert, um interne Bedrohungen proaktiv zu erkennen und abzuschwächen. Diese Systeme nutzen eine adaptive Bewertung und die Durchsetzung von Richtlinien in Echtzeit, um die organisatorische Sicherheit zu verbessern.
- **Fokus auf proaktive Abwehrmechanismen:** Auf dem XDR-Markt vollzieht sich eine Verlagerung von reaktiven zu proaktiven Verteidigungsstrategien. Durch die Vorhersage von potenziellen Bedrohungen und Schwachstellen können Unternehmen Maßnahmen ergreifen, um Sicherheitsvorfälle zu verhindern, bevor sie auftreten.

Diese Trends unterstreichen die dynamische Entwicklung der XDR-Landschaft und zeigen, wie wichtig Anpassungsfähigkeit, Integration und proaktive Strategien in modernen Cybersicherheits-Frameworks sind.

Für die zweite Hälfte des Jahres 2025 ist davon auszugehen, dass XDR-Anbieter ihren Fokus auf offene Architekturen, die Integration von Drittanbietern und die KI-Unterstützung von Analysten verstärken werden. Künftige XDR-Plattformen werden bereits bekannte Bedrohungen erkennen, darauf reagieren und als entscheidungsunterstützende Maschinen fungieren, die in der Lage sind, autonome Untersuchungen durchzuführen, Risiken in Echtzeit zu bewerten und Richtlinien adaptiv durchzusetzen. Da Cyberangriffe zunehmend dynamisch und mehrstufig ablaufen, wird sich XDR wohl zum operativen Nervenzentrum der Cybersicherheit von Unternehmen entwickeln.

XDR verlagert sich von reaktiver zu proaktiver Sicherheit und verändert damit die Cyberabwehr von Grund auf. Diese tiefgreifende Entwicklung stützt sich auf fortschrittliche künstliche Intelligenz und ML; Prognosefunktionen können Angriffe antizipieren und blockieren, bevor sie eskalieren. XDR geht über die reine Erkennung hinaus und beugt durch die Integration von Identitätsdaten und umfassenden Bedrohungsdaten Verstößen vor.

Autor des Berichts:
Yash Jethani (Global-SSE)

Die Zero-Trust-SSE-Architektur entwickelt sich auf Basis von KI weiter und wartet mit kontinuierlicher Authentifizierung und strengen Zugangskontrollen auf.

Warum Zero-Trust-Prinzipien nötig sind

In der heutigen digitalen Landschaft sind herkömmliche Sicherheitsvorkehrungen obsolet. Die Zero-Trust-Architektur bietet kontinuierliche Authentifizierung und strenge Zugriffskontrollen, die für sichere Remote-Arbeit und Cloud-Umgebungen unerlässlich sind. Jeder Benutzer und jedes Gerät wird verifiziert, bevor Zugriff gewährt wird; so können Unternehmen das Risiko von Sicherheitsverletzungen erheblich reduzieren und sensible Daten vor externen Angreifern und internen Bedrohungen schützen.

Die Zero-Trust-Architektur arbeitet nach dem Prinzip „never trust, always verify" und erfordert eine kontinuierliche Authentifizierung unabhängig vom Standort.

Moderne Cybersicherheitsmaßnahmen verstärken diesen Ansatz durch folgende Schritte:

- **Integration von KI und ML:** Verbessert Zero Trust durch kontinuierliche Überwachung von Benutzerverhaltensmustern und die automatische Erkennung von Anomalien, die auf kompromittierte Anmeldedaten hindeuten
- **Ransomware-Abwehr:** Unterstützt Zero Trust durch das Isolieren potenzieller Bedrohungen und Verhindern von lateralen Bewegungen innerhalb von Netzwerken, was den Schadensumfang begrenzt
- **Cloud Security:** Weitet Zero-Trust-Prinzipien durch CASB-Tools, die einheitliche Zugriffsrichtlinien für alle Anwendungen durchsetzen, auf verteilte Umgebungen aus
- **IoT-Schutz:** Wendet Zero-Trust-Mikrosegmentierung auf angeschlossene Geräte an und verhindert so den Zugriff über kompromittierte Geräte auf kritische Systeme

Die Anbieter stimmen SSE auf die Unternehmens-bedürfnisse, nämlich **Agilität, Integration und einheitliches SASE**, ab.

- **Sicherheit kritischer Infrastrukturen:** Implementiert Zero-Trust-Maßnahmen zur Schaffung sicherer Betriebszonen mit strenger Verifizierung des Zugangs zu Kontrollsystemen
- **Datenschutz:** Ist auf die Zero-Trust-Zugriffskontrollen basierend auf dem „Least-Privilege"-Ansatz abgestimmt, um die Einhaltung gesetzlicher Vorschriften zu gewährleisten und sensible Informationen zu schützen
- **Neue Technologien:** Stärken die Zero-Trust-Authentifizierung durch quantenresistente Verschlüsselung und Blockchain-verifiziertes Identitätsmanagement

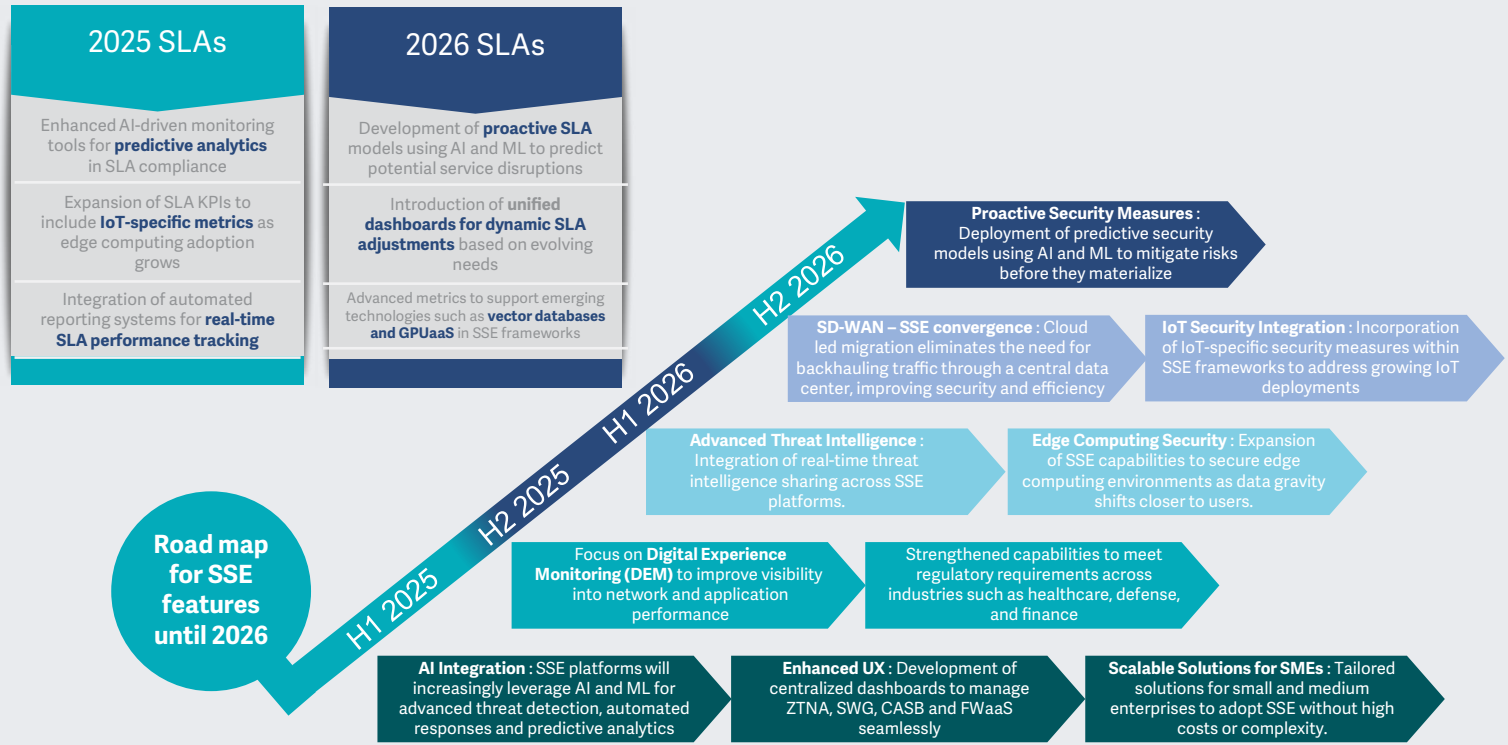
Eine fundierte Cybersicherheitsstrategie integriert diese Elemente in ein Zero-Trust Framework und schafft so mehrere Verifizierungsebenen, die vor komplexen Bedrohungen schützen.

Security Service Edge (SSE) ist eine grundlegende Komponente, die Zero-Trust-Prinzipien in modernen Netzumgebungen ermöglicht. SSE bietet cloud-basierte Sicherheitsfunktionen, die Zero Trust durch folgende Maßnahmen durchsetzen:

- **Identitätsbasierte Zugangskontrolle:** SSE validiert die Identität des Benutzers, bevor Zugriff auf Anwendungen gewährt wird, was dem Zero-Trust-Prinzip "never trust, always verify" entspricht.
- **Kontinuierliche Verifizierung:** SSE überwacht Sitzungen nach der ersten Authentifizierung kontinuierlich und erkennt Verhaltensanomalien, die auf eine Sicherheitsgefährdung hindeuten könnten.
- **Policy Enforcement Point:** SSE dient als cloudbasierter Kontrollpunkt, an dem Zero-Trust-Richtlinien konsistent auf alle Benutzer, Standorte und Geräte angewendet werden. Der Ersatz von Legacy-VPNs reduziert die Angriffsfläche durch eine sicherere Fernzugriffslösung.
- **Kontrollen auf Anwendungsebene:** Anstatt Netzwerksegmente zu sichern, sichert SSE den Zugang zu bestimmten Anwendungen ab und unterstützt damit den Fokus von Zero Trust auf den Schutz von Ressourcen und nicht von Netzwerken. ZTNA bietet Zero-Trust-Zugang zu privaten Anwendungen und ersetzt damit VPNs; CASB dagegen sichert die Konnektivität zu SaaS-Anwendungen und verhindert so Datenverluste und Cyberangriffe, und eine sichere Zusammenarbeit ermöglicht den sicheren Austausch vertraulicher Informationen.
- **Inspektion und Gefahrenabwehr:** SSE bietet eine fundierte Inspektion des verschlüsselten Datenverkehrs und erkennt und blockiert Bedrohungen, die vertrauenswürdige Verbindungen ausnutzen könnten. Das Secure Web Gateway (SWG) ermöglicht einen sicheren Internetzugang mit fortschrittlichem Schutz vor Bedrohungen; DEM wiederum überwacht die Geräte-, Anwendungs- und Netzwerkleistung für eine schnelle Problemlösung.
- **Integrierter Datenschutz:** SSE umfasst Data Loss Prevention (DLP) und Cloud Access Security Broker (CASB) Funktionen, um das Ausschleusen sensibler Daten zu verhindern und die Zero-Trust-Anforderungen für die Datensicherheit zu erfüllen. GenAI DLP verhindert den Austausch sensibler Daten mit GenAI; KI-fähiges DLP arbeitet mit intelligenten Richtlinien zur Kontrolle und zum Schutz sensibler Daten.
- **Sensitive Information Management (SIM):** SSE entdeckt, bewertet und schützt sensible Daten in Echtzeit; kontinuierlicher Zero-Trust-Zugriff sorgt für eine konsequente Autorisierung des Benutzer- und Gerätezugriffs.

SSE liefert den Cloud-Sicherheits-Stack für die skalierbare Implementierung der Zero-Trust-Prinzipien in verteilten Umgebungen und ersetzt die herkömmliche Perimetersicherheit durch einen flexiblen, identitätszentrierten Ansatz zur Absicherung der Remote-Arbeit, Cloud-Nutzung und mobiler Zugriffsszenarien, ohne dass der Schutz oder die Transparenz beeinträchtigt werden.

SSE adressiert ein breites Spektrum von Kunden geeignet, u.a. Anwenderunternehmen, Cloud Service Provider (CSP), Network Service Provider (NSP) für die Netzwerkkonnektivität und Managed Service Provider (MSP), die ausgelagerte IT und Sicherheit anbieten.



Source: ISG, 2025

Großunternehmen mit umfangreichen IT-Teams und -Infrastrukturen, aber auch kleine und mittelständische Unternehmen (KMU), die oft nur über begrenzte Ressourcen verfügen, sind wichtige Kundensegmente. Das Verständnis dieser unterschiedlichen Profile ist sowohl für SSE-Anbieter als auch für Unternehmen im Hinblick auf maßgeschneiderte Lösungen und Einführungsstrategien von entscheidender Bedeutung.

Komponenten und Funktionen von SSE, erweiterte SLA Compliance und Roadmap für 2025 und 2026:

Die SSE-Komponenten lassen sich in vier große Bereiche unterteilen:

- CNAPP (Cloud-Native Application Protection Platform): Kombiniert Cloud-Sicherheitstools (CSPM, CIEM, CWP) für optimierten, skalierbaren Cloud-Schutz – ein wichtiger Teil von SSE
- Digital Ecosystem Exposure Management: Identifizierung und Abschwächung von Risiken bei vernetzten digitalen Assets (Cloud, IoT, BYOD), was für den Ausbau des digitalen Fußabdrucks und als Alleinstellungsmerkmal für SSE-Anbietern entscheidend ist
- Deep Packet Inspection (DPI) der nächsten Generation: Nutzt fortschrittliche Techniken wie ML zur Analyse von verschlüsseltem Datenverkehr und zur Erkennung von ausgefeilte Bedrohungen in Cloud-Umgebungen, wodurch die Sichtbarkeit für CASB, SWG und ZTNA innerhalb von SSE verbessert wird
- UEBA (User & Entity Behavior Analytics): Setzt Analysen und ML ein, um anormales Benutzer- und Entitätsverhalten zu erkennen, das auf interne Bedrohungen oder Angriffe hindeutet, und wird zunehmend in SSE für Advanced Threat Detection Zwecke integriert

Immer mehr SSE-Anbieter offerieren Plattformen, die mehrere Funktionen und Komponenten integrieren. Diese Plattformen bieten auf Basis einer einzigen Architektur umfassende cloud-native Sicherheit sowie die Möglichkeit, verschlüsselten Datenverkehr in großem Umfang zu prüfen; sie verfügen über einen Inline Proxy für Cloud- und Web-Datenverkehr. Zu den wichtigsten Sicherheitsfunktionen gehören eine Full-Port Firewall mit Intrusion Protection (FWaaS), API-basierte Datensicherheit für Cloud-Services (CASB) und die kontinuierliche Sicherheitsbewertung für Public-Cloud-Infrastrukturen (CSPM). Ein erweiterter Schutz vor Datenverlusten ist in der Regel für Daten bei der Übertragung und im Ruhezustand enthalten, ebenso ein Schutz vor komplexen Bedrohungen (Advanced Threat Protection, ATP) unter Einsatz von KI und ML, UEBA und Sandboxing. Eine solche Plattform integriert Bedrohungsdaten mit anderen Sicherheitstools (EPP/EDR, SIEM, SOAR), verhindert Datenverluste aus GenAI-Systemen, bietet Zero Trust Network Access (ZTNA), was herkömmliche VPNs ersetzt, und ermöglicht letztendlich eine sichere Zusammenarbeit über E-Mail und Collaboration Tools. Sie verfügt eventuell auch über einen softwaredefinierten Perimeter mit Zero-Trust-Zugang (SD-WAN/SDP) und eine globale, skalierbare Netzwerkinfrastruktur mit Optimierungen für die SaaS-Leistung.

Wie in der obigen Abbildung dargestellt, erwartet ISG, dass sich die SSE-Komponenten und -Funktionen bis 2026 weiterentwickeln und IoT-Sicherheit, proaktives Edge Healing und auf KMU zugeschnittene Lösungen umfassen werden.

Technologische SSE-Trends:

- SSE-Lösungen übernehmen zunehmend Zero-Trust-Prinzipien und verlagern sich weg vom VPN-basiertem Fernzugriff hin zu identitätsgesteuerter Sicherheit. ZTNA bleibt die Grundlage von SSE und stellt sicher, dass nur autorisierte Benutzer und Geräte auf Ressourcen zugreifen; dahinter steht die Notwendigkeit, Fernarbeit und Cloud-Umgebungen abzusichern.

Zusammenfassung

- Anbieter und Produktverkäufer integrieren ML- und KI-gestützte Bedrohungserkennung zum Aufdecken von Anomalien, zur automatischen Behebung von Problemen und zur Durchsetzung von Richtlinien in Echtzeit.
- Unternehmen bevorzugen cloud-native SSE-Lösungen gegenüber herkömmlicher appliance-basierter Sicherheit; eine vollständige cloud-native Architektur unterstützt inzwischen verteilte Belegschaften und Multicloud-Umgebungen. Cloud-native SSE-Plattformen werden auf enorme Datenmengen ausgelegt und unterstützen die digitale Transformation mit flexibler, skalierbarer Sicherheit für hybride IT-Umgebungen.
- SSE-Lösungen zielen vor allem auf niedrige Latenzzeiten und minimale Ausfallzeiten ab, um den Anforderungen einer verteilten Belegschaft gerecht zu werden, ohne die Sicherheit zu beeinträchtigen.
- SSE-Plattformen sind tief in das Security Information & Event Management (SIEM) und Extended Detection & Response (XDR)-Lösungen integriert, um eine bessere Sichtbarkeit von Bedrohungen und eine bessere Reaktion darauf zu ermöglichen. Andererseits wird Autonomous Digital Experience Management/Monitoring (ADEM) in SSE integriert, um die Leistung und Sicherheit der Endanwender überwachen und KI für prädiktive Analysen und die Fehlerbehebung nutzen zu können.
- DLP, Verschlüsselung und adaptive Zugriffskontrollen entwickeln sich zu Standardfunktionen, die den zunehmenden Compliance-Anforderungen gerecht werden.
- Die Integration mit IAM und SSE (SSO/MFA) ist inzwischen Standard und hilft, strengere Authentifizierungsrichtlinien durchzusetzen.

Businessbezogene SSE-Trends:

- Viele Unternehmen führen zunächst SSE ein und integrieren später SD-WAN für eine vollständige SASE-Bereitstellung. Dieser Trend kann aber wahrscheinlich auch umgekehrt verlaufen, denn viele Unternehmen führen Netzwerklösungen ein, setzen dann SSE-Funktionen auf und migrieren so zu SASE. Somit verschwimmt die Grenze zwischen SSE und Secure Access Service Edge (SASE) immer mehr, denn die Anbieter offerieren einheitliche Plattformen, die Netzwerk- (SD-WAN) und Sicherheitsfunktionen (ZTNA, SWG, CASB, FWaaS) zusammenführen und hybride und verteilte Belegschaften unterstützen.
- Angesichts der mit VPN einhergehenden Grenzen ersetzt SSE herkömmliche Fernzugriffslösungen, da die Nachfrage nach SSE durch Fernarbeit und hybride Arbeitsformen steigt. Unternehmen setzen im Zuge der Verlagerung der Arbeit in die Cloud und des vermehrten Fernzugriffs zunehmend sichere Browser als wichtige erste Verteidigungslinie gegen browserbasierte Bedrohungen ein. Angesichts der zunehmenden Abhängigkeit von Webanwendungen wird dies als eine Notwendigkeit betrachtet.
- SSE-Plattformen nutzen KI und ML für die Erkennung von Bedrohungen in Echtzeit, die Verhaltensüberwachung und automatische Reaktionen; das reduziert manuelle Eingriffe und verbessert die proaktive Sicherheit.
- Unternehmen wenden sich OpEx-Modellen anstelle von traditionellen, kapazitätsintensiven Hardware-Investitionen zu und bevorzugen daher einen Wechsel hin zu abonnementbasierter Sicherheit (Security-as-a-Service).
- Unternehmen möchten lieber mit weniger Anbietern zusammenarbeiten, die durchgängige SSE-Lösungen offerieren, anstatt mehrere Sicherheitstools verwalten zu müssen. Dies treibt die Konsolidierung der Anbieterlandschaft voran und begünstigt Single-Vendor-Strategien, insbesondere für kleine und mittelständische Unternehmen.
- Branchen wie das Finanzwesen, das Gesundheitswesen und die öffentliche Verwaltung setzen auf SSE, um strenge Datenschutz- und Zugangskontrollvorschriften erfüllen zu können.

Jüngste Übernahmen im Bereich Zero Trust bzw. SSE:

- **Cloudflare:** Im Februar 2025 übernahm Cloudfare BastionZero, um seine Zero-Trust-Infrastruktur-Zugangskontrollen zu verbessern und die Funktionen von Cloudflare One, seiner SASE-Plattform, auszubauen. Außerdem erwarb das Unternehmen 2022 Area 1 Security und hat damit die E-Mail-Sicherheit innerhalb seines SSE-Angebots verbessert.
- **Zscaler:** Im Oktober 2024 übernahm Zscaler das Netzwerksegmentierungs-Startup Airgap Networks, um sein Zero-Trust-Sicherheitsangebot zu stärken. Im März 2024 kaufte der Anbieter das israelische Datensicherheits-Startup Avalor auf, um seine um seine KI-gesteuerten Datenschutzfunktionen zu verbessern. Im Februar 2024 übernahm Zscaler ein weiteres israelisches Unternehmen für Anwendungssicherheit, Canonic Security, für einen besseren Schutz vor SaaS-basierten Bedrohungen. Im Mai 2021 hatte der Anbieter bereits Smokescreen akquiriert und damit das Angebot um Täuschungstechnologie ergänzt und die Bedrohungserkennung verbessert.
- **Hewlett Packard Enterprise (HPE):** Im März 2023 erwarb HPE Axis Security, einen cloud-nativen SSE-Anbieter. Diese Übernahme stärkt durch die Integration von Axis Security in die Aruba-Netzwerkplattform die Edge-to-Cloud-Sicherheitsfähigkeiten von HPE; so wurde eine einheitliche SASE-Lösung geschaffen.
- **Netskope:** Im Juni 2022 übernahm Netskope WootCloud, einen Innovator bei der Anwendung von Zero-Trust-Prinzipien auf die IoT-Sicherheit, und weitete damit seine Zero-Trust-Fähigkeiten auf IoT aus. Darüber hinaus hat der Anbieter 2022 Infiot übernommen und damit seine Zero-Trust- und SD-WAN-Fähigkeiten gestärkt.
- **Palo Alto Networks:** Das Unternehmen erwarb im Jahr 2020 CloudGenix und integrierte SD-WAN und SSE, um einen vollständigen SASE-Stack zu schaffen. Dieser Schritt unterstreicht den Trend hin zu SSE/SASE-Plattformen eines einzigen Anbieters, die die Bereitstellung und Verwaltung vereinfachen und die Komplexität im Zusammenhang mit Multivendor-Umgebungen vermeiden.
- **Check Point:** Im September 2023 schloss das Unternehmen die Übernahme von Perimeter 81 aber und hat damit seine SASE-Fähigkeiten gestärkt. Die Funktionen von Perimeter 81 werden über eine benutzerfreundliche Cloud-Konsole verwaltet und gewährleisten eine zuverlässige Konnektivität über ein globales Backbone-Netzwerk; das SWG bietet Schutz vor Bedrohungen aus dem Internet.
- **SonicWall:** Im Januar 2024 übernahm SonicWall Banyan Security, eine Cloud-Plattform, die sich auf identitätszentrierte SSE-Lösungen fokussiert; damit werden die Sicherheitsfunktionen auf Cloud- und Hybrid-Umgebungen, Remote-Belegschaften und BYOD-Szenarien ausgeweitet. Das Framework von Banyan Security bewertete den Zustand von Geräten, um einen sicheren Zugang zu gewährleisten; dazu zählte auch ein SWG zur Abwehr von internetbasierten Bedrohungen. Hinzu kam VPN as a Service (VPNaaS) für einen modernen, sicheren Netzwerkzugang.

SSE bietet cloud-basierte Sicherheitsdienste wie SWG und ZTNA, die die sicherere Remote-Zusammenarbeit von verteilten Arbeitsgruppen erleichtert. Unternehmen müssen sich zudem an die sich ändernden rechtlichen Standards halten, was strenge Sicherheitsmaßnahmen zum Schutz von Unternehmens- und personenbezogenen Daten erfordert. Diverse Branchen setzen SSE-Lösungen ein, weil sie die Compliance durch zentralisierte Sicherheitsrichtlinien, Echtzeitüberwachung von Bedrohungen und Verhinderung von Datenverlusten erleichtern. Die unscharfen Grenzen zwischen SSE und Secure Access Service Edge (SASE) sind Hinweis auf einen überzeugenden Trend hin zum nahtlosen Einsatz von umfassenden Sicherheits- und Netzwerklösungen, die auf hybride und verteilte Belegschaften zugeschnitten sind. Der SSE-Markt ist auf Wachstumskurs und wird zu einem wesentlichen Bestandteil der Unternehmensstrategie und der betrieblichen Ausfallsicherheit im digitalen Zeitalter.

Zusammenfassung

Für eine effektive SSE-Einführung sollten Unternehmen mehrere Schlüsselstrategien übernehmen. Dazu gehören die Minimierung der Abhängigkeit von älterer Sicherheitshardware im Zuge der Nutzung der integrierten SSE-Funktionen und die Implementierung von Zero-Trust-Prinzipien über ZTNA für eine robuste Zugangskontrolle. Die Konsolidierung unterschiedlicher Sicherheitstools auf einer einheitlichen SSE-Plattform vereinfacht die Verwaltung; hybride und cloud-fähige SSE-Architekturen sorgen für Flexibilität. Eine gestaffelte Bereitstellung, beginnend mit kritischen Bereichen wie ZTNA, ermöglicht eine schrittweise und strategische Einführung. Darüber hinaus ist es von entscheidender Bedeutung, die Sicherheit von Remote-Arbeitsumgebungen in den Vordergrund zu stellen und eine positive UX mit DEM zu gewährleisten. Letztendlich wird eine strategische Budgetvergabe für SSE-Investitionen, die die Hauptrisiken adressieren, zu den wirkungsvollsten Sicherheitsergebnissen führen, und CIOs und Fachabteilungsleiter müssen sich auf entsprechende Sicherheitsbudgets einigen.

Unternehmen streben nach skalierbaren, leistungsstarken Lösungen mit nahtloser Integration, einheitlicher Verwaltung und einem klaren Pfad in Richtung einer vollständigen SASE-Lösung für zukunftsfähige Sicherheit. Die Anbieter tendieren zu agilen, einheitlichen und leistungsorientierten Sicherheits-Frameworks, doch das ultimative Ziel besteht darin, eine wirklich reibungslose und umfassende Sicherheitserfahrung für jeden Benutzer, jedes Gerät und jeden Standort zu bieten.

Anbieterpositionierung

Seite 1 von 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – 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
All for One Group	Not In	Not In	Not In	Not In	Contender	Contender	Not In	Not In
Aryaka	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Atos	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Axians	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
Bechtle	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader	Leader
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 2 von 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Bitdefender	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
BlackBerry (Arctic Wolf)	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	Leader	Leader	Leader	Market 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	Leader	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 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – 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	Leader	Leader	Leader
CoSoSys (Netwrix)	Not In	Contender	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	Leader	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 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – 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
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	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
Evidian IAM (Eviden)	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Fischer Identity	Product Challenger	Not In	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
Fortinet	Market Challenger	Not In	Leader	Leader	Not In	Not In	Not In	Not In
Fortra	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In
FusionAuth	Contender	Not In	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
Getronics	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Product Challenger
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
Gopher Security	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 6 von 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
HCLTech	Not In	Not In	Not In	Not In	Leader	Leader	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	Rising Star ★	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
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
indevis	Not In	Not In	Not In	Not In	Rising Star ★	Not In	Market Challenger	Market Challenger
InfoGuard	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★	Leader
Infosys	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In

Anbieterpositionierung

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
itWatch	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
JumpCloud	Contender	Not In	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	Contender	Not In
LMNTRIX	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Logicalis	Not In	Not In	Not In	Not In	Contender	Contender	Product Challenger	Product Challenger
Lookout	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger	Product Challenger
ManageEngine	Leader	Rising Star ★	Not In	Contender	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 8 von 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Materna	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★	Not In	Not In
Matrix42	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Menlo Security	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In
Mimecast	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Leader	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
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Leader	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

Anbieterpositionierung

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
OpenText	Product Challenger	Product Challenger	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
ORBIT	Not In	Not In	Not In	Not In	Contender	Contender	Not In	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	Contender	Contender	Contender
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

Anbieterpositionierung

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In	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
Seqrite	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Sequretek	Contender	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Not In
SonicWall (Banyan Security)	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Sophos	Not In	Not In	Rising Star ★	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

Anbieterpositionierung

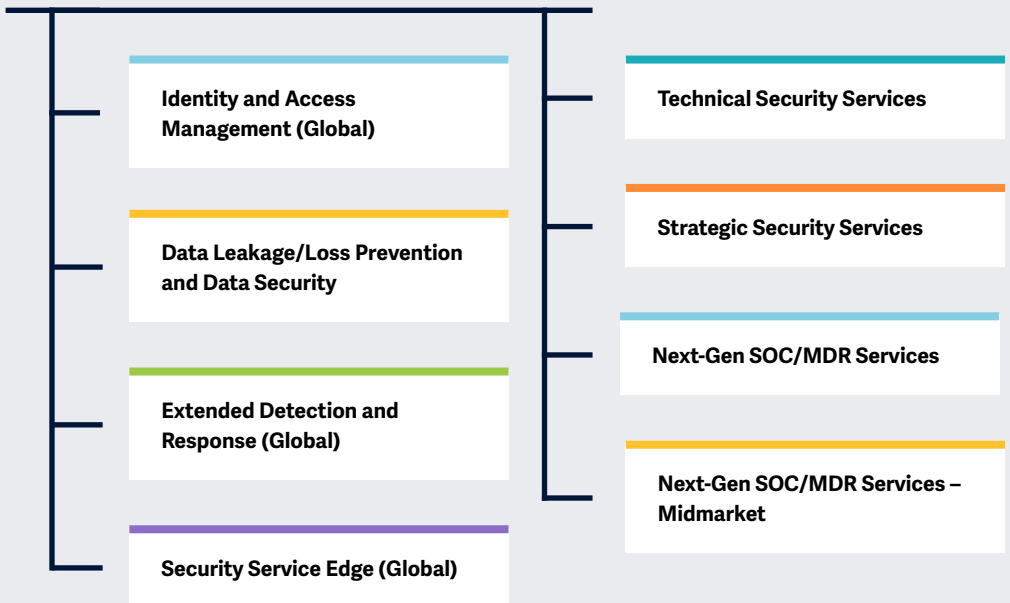
	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
suresecure	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
SVA	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★
Syntax	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	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	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Leader	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

Anbieterpositionierung

Seite 12 von 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
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	Product Challenger	Not In	Not In
Wipro	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In
Xantaro	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
Zscaler	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In	Not In

Abgedeckte Schwerpunkt-bereiche der Studie **Cybersecurity – Services und Solutions 2025**.



Vereinfachte Illustration; Quelle: ISG 2025

Definition

Cybersicherheit im Zeitalter der KI und neuer disruptiver Technologien

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

Die zunehmende Verbreitung von Technologien hat die Angriffsfläche vergrößert und stellt Unternehmen vor große Herausforderungen hinsichtlich OT/IT Security. Der Mangel an

qualifiziertem Cybersecurity-Personal hat diese Komplexität noch verstärkt und die Nachfrage nach Managed Security Services in die Höhe getrieben, denn zur Verstärkung ihrer Verteidigung greifen Unternehmen auf externes Fachwissen zurück.

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

Betrachtungsumfang der Studie

Dieser ISG Provider Lens™ Quadrantenreport deckt die folgenden acht Quadranten für Dienstleistungen/Lösungen ab: Identity and Access Management (Global), Data Leakage/ Loss Prevention and Data Security, Extended Detection and Response (Global), Security Service Edge (Global), Technical Security Services, Strategic Security Services, Next-Gen SOC/MDR Services und Next-Gen SOC/MDR Services – Midmarket.

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

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

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

Klassifizierung der Anbieter

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

Identity and Access Management (Global)

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Anbieter von Nutzen, die Lösungen für das **Identity & Access Management (IAM)** in **Deutschland** anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Anbieter evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Provider, basierend auf der Tiefe ihrer Leistungen und ihrer Marktpräsenz. Der Bericht geht auf die wichtigsten IAM-Herausforderungen ein, u.a. die Sicherung von Identitäten in hybriden IT-Umgebungen, die Ermöglichung eines nahtlosen Zugriffs und die Bekämpfung komplexer Bedrohungen (Advanced Threats), und betont die Notwendigkeit einer adaptiven Authentifizierung, von Zero Trust und einheitlichen Identitätslösungen für mehr Flexibilität.

Technologie-Experten

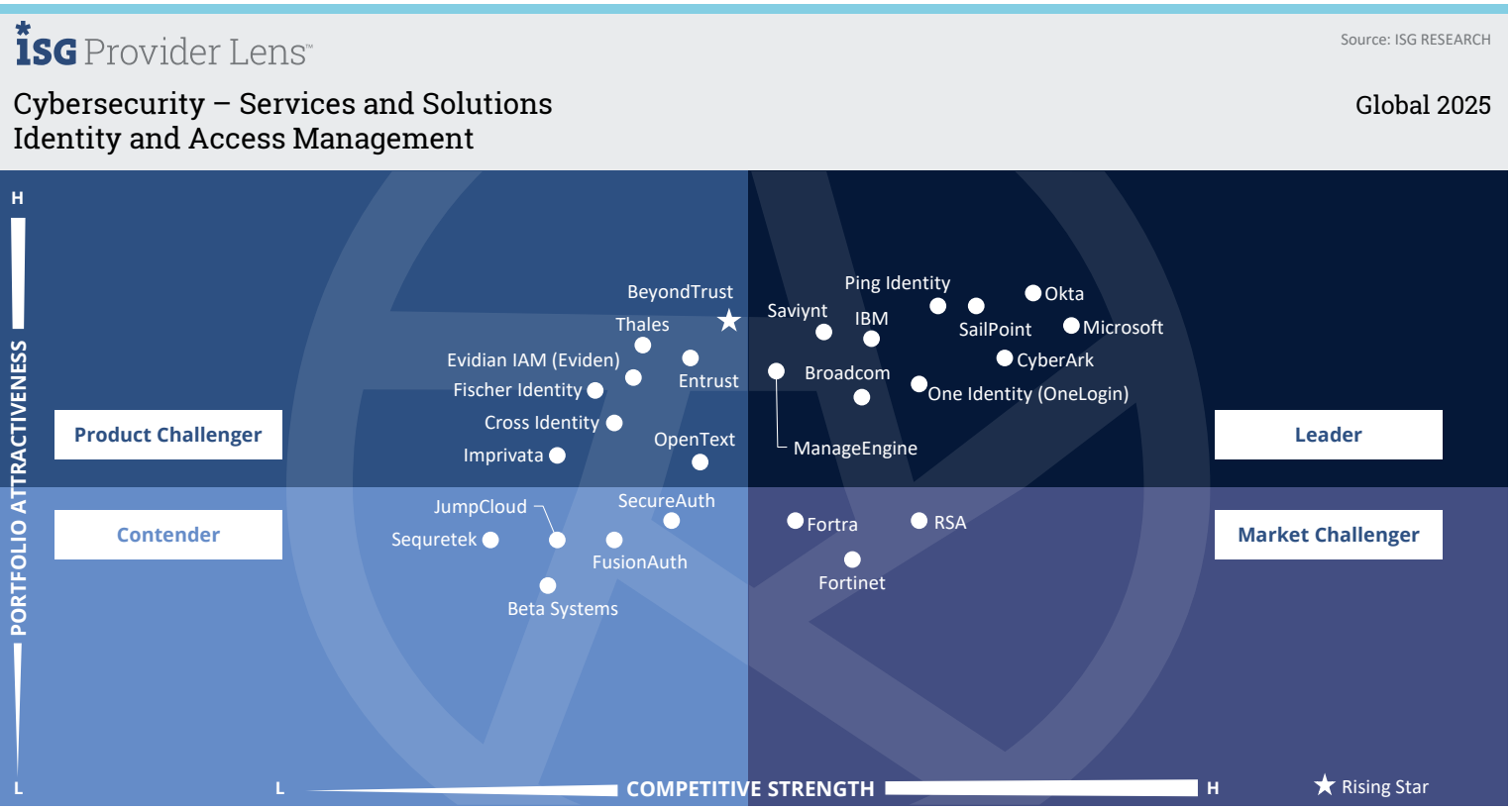
gewinnen aus diesem Bericht ein besseres Verständnis der Integrationsleistungen der Anbieter, die anhand fortschrittlicher Technologien zur Transformation von Altsystemen die Auswirkungen von Bedrohungen verringern.

Sicherheits- und Datenexperten

gewinnen durch diesen Bericht Einblicke in die Einhaltung der Sicherheits- und Datenschutzgesetze durch die Anbieter und können entsprechenden Markttrends Rechnung tragen.

Experten aus den Fachabteilungen

erhalten aus diesem Bericht Informationen, die ihnen helfen, Datensicherheit, CX und Datenschutz im aktuellen Geschäftsumfeld, in dem die digitale Transformation Priorität hat, in Balance bringen.



Im Rahmen dieses Quadranten werden IAM-Anbieter untersucht, die sich durch die Bereitstellung von **adaptiven Identitätslösungen** auszeichnen. Zu den wichtigsten Funktionen gehören **Echtzeit-Zugangskontrollen für Zero-Trust-Sicherheit**, eine **benutzerfreundliche Oberfläche** und die Einhaltung **gesetzlicher Vorschriften**.

Bhuvaneshwari Mohan (IAM)

Definition

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

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

Auswahlkriterien

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

Beobachtungen

Im Jahr 2025 wird sich der IAM-Markt rasch weiterentwickeln; die treibenden Faktoren sind KI-gestützte Sicherheit, passwortlose Authentifizierung und Compliance-Anforderungen. Die Anbieter fokussieren sich auf identitätsorientierte Sicherheit, Automatisierung und Benutzerfreundlichkeit, um Unternehmen bei der Verwaltung der digitalen Identitäten von menschlichen und nicht-menschlichen Identitäten in dynamischen und komplexen Umgebungen zu unterstützen.

Die Erkennung von und Reaktion auf Identitätsbedrohungen (Identity Threat Detection & Response, ITDR) hat in den letzten 12-18 Monaten erheblich an Aufmerksamkeit gewonnen. Anbieter integrieren KI und ML zur Erkennung von Identitätsbedrohungen, zur Automatisierung der Governance und zur Durchsetzung einer risikobasierten Authentifizierung. Sicherheitsteams setzen zunehmend intelligente Identitätsanalysen ein, um Bedrohungen in Echtzeit zu erkennen, darauf zu reagieren und die Angriffsfläche zu minimieren. Die passwortlose Authentifizierung, u.a. über Passkeys, Biometrie und FIDO2, entwickelt sich zum Standard, was das Phishing-Risiko verringert und auch einen nahtlosen Benutzerzugang gewährleistet.

IAM ist nach wie vor von Zero-Trust-Modellen geprägt, denn sie sind für ein robustes Identitätsmanagement unerlässlich. Echtzeit-Funktionen wie die dynamische Zugangsverwaltung für eine bessere Abstimmung auf die Zero-Trust-Prinzipien werden immer wichtiger. Mit integrierter prädiktiver KI für bessere Richtlinienentscheidungen und kontextbezogene Reaktionen entwickeln sich die meisten IAM-Plattformen stetig in Richtung einer halbautonomen Zugriffskontrolle weiter; auch die betriebliche Kontrolle wird gewährleistet.

Die Nutzung der Cloud beschleunigt die Verlagerung von IAM in Richtung skalierbarer, interoperabler IDaaS-Lösungen, die eine nahtlose Authentifizierung in hybriden und Multi-Cloud-Umgebungen sicherstellen. Auch dezentrale Identitäten sind im Kommen; sie geben den Nutzern mehr Kontrolle über ihre persönlichen Daten. Die Nachfrage nach CIAM-Lösungen steigt, denn Unternehmen wollen ihren Kunden sichere, personalisierte und nahtlose digitale Erfahrungen bieten, aber auch Betrugsversuchen vorbeugen und den Schutz der Privatsphäre gewährleisten.

Von den 61 Unternehmen, die für diese Studie global bewertet wurden, haben sich 26 für diesen Quadranten qualifiziert; zehn dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Broadcom

Broadcom hilft Unternehmen beim Wechsel von einem fragmentierten IAM zu einem vollständig orchestrierten IAM durch die Kombination von Technologie, Skalierung und Branchen-Know-how mit einem identitätszentrierten Sicherheitsmodell, das für hybride Clouds, Zero-Trust-Architekturen und regulatorische Agilität gewappnet ist.

CyberArk

CyberArk wandelt sich in einen leistungsstarken Anbieter von Identitätssicherheitslösungen, der moderne Angriffsflächen adressiert und dabei seine Führungsposition im PAM-Bereich beibehält; gestärkt wird diese Position noch durch den adaptiven Ansatz auf Zero-Trust-Basis.

IBM

Mit Security Verify von **IBM** können Unternehmen eine reibungslose und sichere Zugriffskontrolle in lokalen, Cloud- und Hybrid-Cloud-Umgebungen gewährleisten. Die Identitätsstruktur und die Orchestrierungsfunktionen ermöglichen hochgradig anpassbare Workflows.

ManageEngine

ManageEngine bietet kostengünstiges, modulares IAM, das auf Microsoft-Umgebungen zugeschnitten ist. Unternehmen profitieren von einer robusten Automatisierung des AD-Lebenszyklus, MFA und Auditing vor Ort, ohne eine vollständige Cloud-Migration durchführen zu müssen.

Microsoft

Microsoft Entra bietet eine einheitliche Identitätsplattform mit tiefer Integration in Microsoft 365, Azure und Anwendungen von Drittanbietern. Sie ist ideal für Unternehmen, die eine skalierbare, cloud-native Identität mit nativer Zero-Trust- und bedingter Zugriffskontrolle anstreben.

Okta

Die cloud-native Architektur von **Okta** sorgt für hohe Verfügbarkeit und Skalierbarkeit und ist damit ideal für Unternehmen jeder Größe. Die Multicloud-Kompatibilität ermöglicht die nahtlose Integration mit AWS, Google Cloud und Azure.

One Identity (OneLogin)

One Identity vereint Identity Governance & Administration (IGA) mit PAM auf einer einzigen Plattform, was ideal für Unternehmen ist, die ihr bestehendes IAM modernisieren und Kontrolle über privilegierte Zugriffe haben wollen. Die tiefe AD/LDAP-Integration und die robuste Governance-Automatisierung vereinfachen hybride Bereitstellungen.

Ping Identity zeichnet sich durch seine flexible, hybride IAM-Plattform aus, die KI-gesteuerte Risikoanalyse, No-Code-Orchestrierung über DaVinci und die umfassende Unterstützung von Standards kombiniert, um sicheren, adaptiven Zugriff in komplexen Unternehmensumgebungen zu ermöglichen.

SailPoint

SailPoint festigt seine Position als Marktführer im Bereich Identitätssicherheit mit innovativen KI-gestützten Lösungen und Cloud-First-Innovationen. Durch strategische Akquisitionen, u.a. für die Bereiche PAM, Third-Party Risk Management (TRM) und auf das Gesundheitswesen spezialisiertes IGA (Identity, Governance & Administration) hat der Anbieter seine Fähigkeiten ausgebaut; sie fördern ein sicheres, skalierbares Identitätsmanagement.

Saviynt

Saviynt ermöglicht Unternehmen cloud-native Identity Governance, die IGA, PAM und den Zugriff auf Erkenntnisse in einer einzigen Plattform vereint. Das fein abgestufte Berechtigungsmanagement und die risikobasierte Automatisierung unterstützen komplexe, compliance-gesteuerte Umgebungen.

BeyondTrust (Rising Star) zeichnet sich durch ein unternehmensweites Privileged Access Management aus, das adaptive, risikobasierte Kontrollen, Session Monitoring und Endpoint Privilege Security bietet, die für die Minimierung von Angriffsflächen in hybriden Infrastrukturen entscheidend sind.

Hidden Champions:

Entrust wird für seine starken Fähigkeiten im Bereich IAM als Hidden Champion anerkannt, insbesondere in den Bereichen digitale Identität, PKI und Authentifizierung. Das Angebot eignet sich vor allem für Unternehmen, die sich mit hybriden Arbeitsmodellen, der Einführung von Zero Trust und der Einhaltung gesetzlicher Vorschriften auseinandersetzen. Die Fähigkeit, skalierbare, sichere und compliance-konforme IAM-Lösungen zu liefern, macht Entrust zu einem wertvollen Enabler für robuste Zugangskontrolle und Vertrauenssicherung, insbesondere für Finanzinstitute und Behörden.

Fischer Identity gilt als Hidden Champion wegen der richtliniengesteuerten IGA-Automatisierung, des nahtlosen Identity as a Service (IDaaS)-Bereitstellungsmodells und der spezifischen Unterstützung für regulierte Sektoren wie das Bildungswesen und den öffentlichen Sektor. Der Anbieter zeichnet sich durch konfigurierbare Lifecycle Governance, zentralisiertes Identitätsdatenmanagement und auf die Compliance abgestimmte Zugriffskontrollen aus. Die optimierte Architektur reduziert die Komplexität und bietet ein starkes Wertversprechen für mittelständische Unternehmen, die eine schnelle Bereitstellung benötigen.

Data Leakage/Loss Prevention and Data Security

Wer sollte dieses Kapitel lesen

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

IT-Sicherheitsexperten

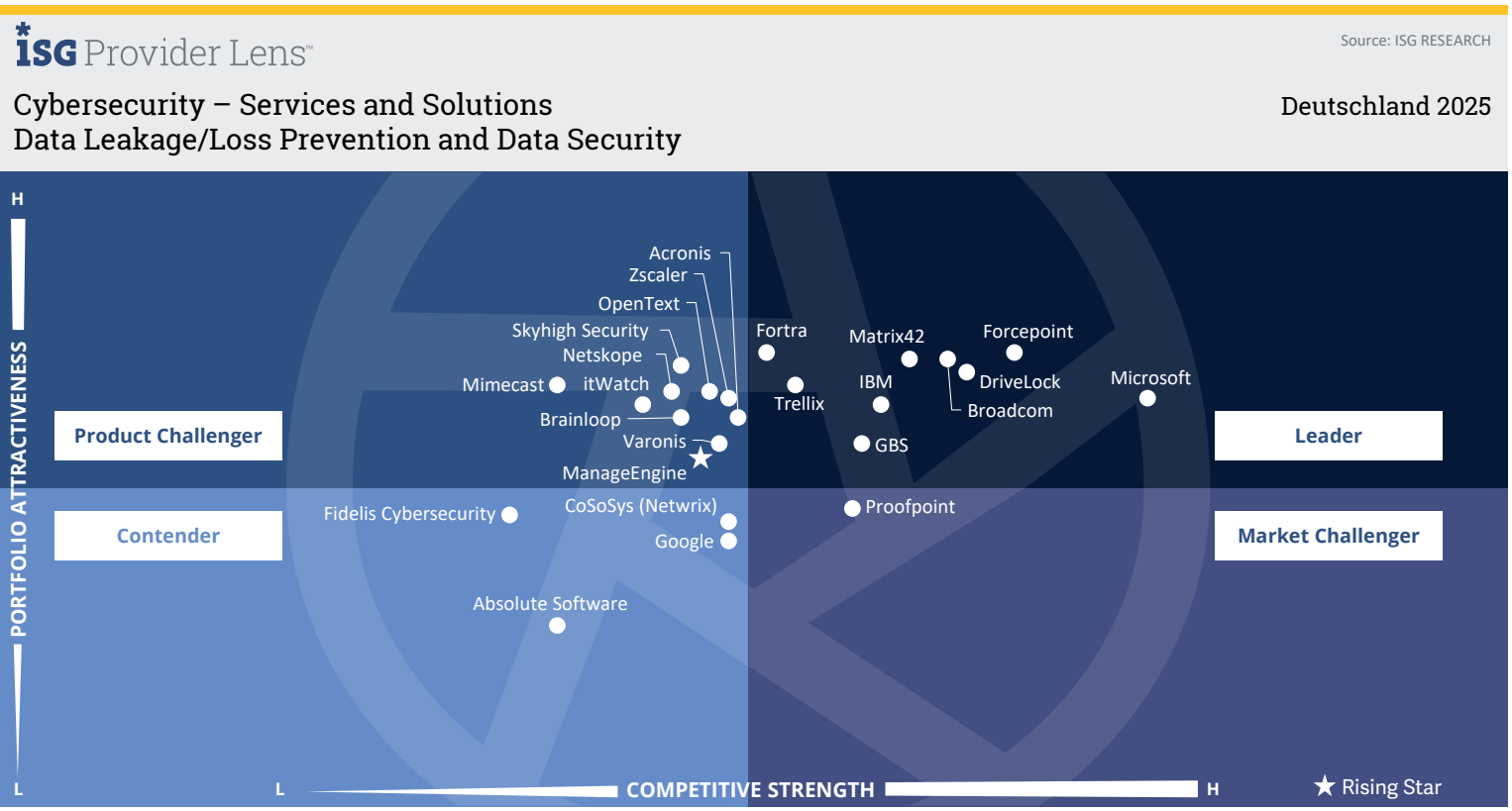
informiert dieser Bericht über neue Trends, innovative Funktionalitäten und Best Practices in diesem Bereich.

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. Die Sicherung **geistigen Eigentums** und drängende **Datenschutzbelange** tragen zur Bedeutung des Marktes bei.

Frank Heuer

Definition

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

DLP-Lösungen helfen Unternehmen, die Herausforderungen bei der Kontrolle von Datenbewegungen zu bewältigen; schließlich haben über ein Drittel der Datenverletzungen ihren Ursprung im Unternehmen. Die zunehmende Verbreitung von mobilen und anderen Geräten zur Datenspeicherung verstärkt diese Sorgen, da Daten ohne zentrale Gateways ausgetauscht werden können. Data-Security-Lösungen schützen vor unbefugtem Zugriff und Diebstahl durch die Priorisierung, Klassifizierung und Überwachung von Daten (im Ruhezustand und bei der Übertragung) und helfen, die Sicherheit der gefährdeten Daten zu verbessern.

Auswahlkriterien

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

Beobachtungen

Daten und geistiges Eigentum haben sich zu immer wichtigeren und teilweise existenziell bedeutsamen Unternehmens-Assets entwickelt. Dies trägt zum gewachsenen Interesse an DLP-Lösungen bei. Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen und teilweise auch aus rechtlichen Gründen nicht umfassend betrieblich überwacht werden dürfen. DLP-Lösungen müssen diese Einschränkungen bei der Kontrolle berücksichtigen, ohne betriebliche Sicherheitslücken zuzulassen. Mit der Datenschutz-Grundverordnung und der NIS-2-Richtlinie hat die Bedeutung des Datenschutzes in Unternehmen 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.

Mimecast und ManageEngine sind neu im Quadranten vertreten. Letzterer Anbieter ist zugleich der neue Rising Star.

Von den 68 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 24 für diesen Quadranten qualifizieren. Dabei erreichten neun eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Broadcom

Die Leistungsfähigkeit und Flexibilität der **Broadcom**-Lösung ist für den Anbieter und seine Kunden von Vorteil. Des Weiteren unterstützt Broadcom seine Kunden durch Zentralisierung und Vereinheitlichung.

DriveLock

DriveLock punktet mit seiner Vertrauenswürdigkeit und erwirbt sich dieses Vertrauen im Markt mit den Devisen „Made in Germany“ und „No Backdoor“. DriveLock zeichnet sich darüber hinaus durch einen konsequenten Einsatz von Machine-Learning-Algorithmen aus.

Forcepoint

Forcepoint hilft mit seinem Angebot an fortschrittlichen Lösungen den Anwendern schnell und entlastet sie zudem hinsichtlich ihrer Herausforderungen in Bezug auf die Sicherung vor Datenverlusten.

Fortra

Fortra ist in der Lage, seine Kunden mit proaktiver Datenklassifizierung, fortschrittlichen Analyse- und Reporting Services sowie einfacher Integration umfassend zu unterstützen.

GBS

Zur Leader-Position von **GBS** tragen die ausgefeilte Technik, das Vier-Augen-Prinzip und DLP made in Germany bei.

IBM

IBM verbindet eine hohe Marktpräsenz mit einer zukunftsweisenden DLP-Lösung und punktet dabei mit der kompetenten Verknüpfung von DLP mit künstlicher Intelligenz und Post-Quantum Encryption. Die Lösung von IBM deckt darüber hinaus ein universelles Einsatzspektrum ab.

MATRIX42

Matrix42 bietet eine effiziente DLP-Lösung mit einem sehr breiten Funktionsspektrum an. Matrix42 genießt dank anwenderfreundlich geringen Beeinträchtigungen eine hohe Akzeptanz bei den Endanwendern und fördert damit auch den erfolgreichen Einsatz der Lösung.

Microsoft

Microsoft versteht es, seine Position im deutschen Markt für DLP-Lösungen weiter auszubauen. Der Anbieter etabliert sich hierzulande immer mehr nicht nur mit Hilfe von Integration und Bundling, sondern auch mit überzeugenden Leistungsmerkmalen.

Trellix

Trellix ist im Hinblick auf die Delivery durch seine starke lokale und internationale Präsenz sehr vielseitig aufgestellt. Die Kunden von Trellix profitieren zudem von einem großen Leistungsumfang der DLP-Lösung.

ManageEngine

ManageEngine (Rising Star) hilft, die Gewährleistung der Datensicherheit durch Automatisierung zu erleichtern und die Einhaltung gesetzlicher Vorgaben zu vereinfachen. Damit steigt ManageEngine zum Rising Star im DLP-Markt auf.

Extended Detection and Response (Global)

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider, die **Extended Detection & Response (XDR)** -Produkte weltweit anbieten, von Nutzen um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Leistungsangebots und ihrer Marktpräsenz. Die Studie bewertet global tätige XDR-Dienstleister in Bezug auf verbesserte Transparenz und einheitliche Funktionen zur Erkennung von Bedrohungen, die Unternehmen mit begrenzten Ressourcen durch datengestützte Erkenntnisse und Integration unterstützen.

Security-Experten

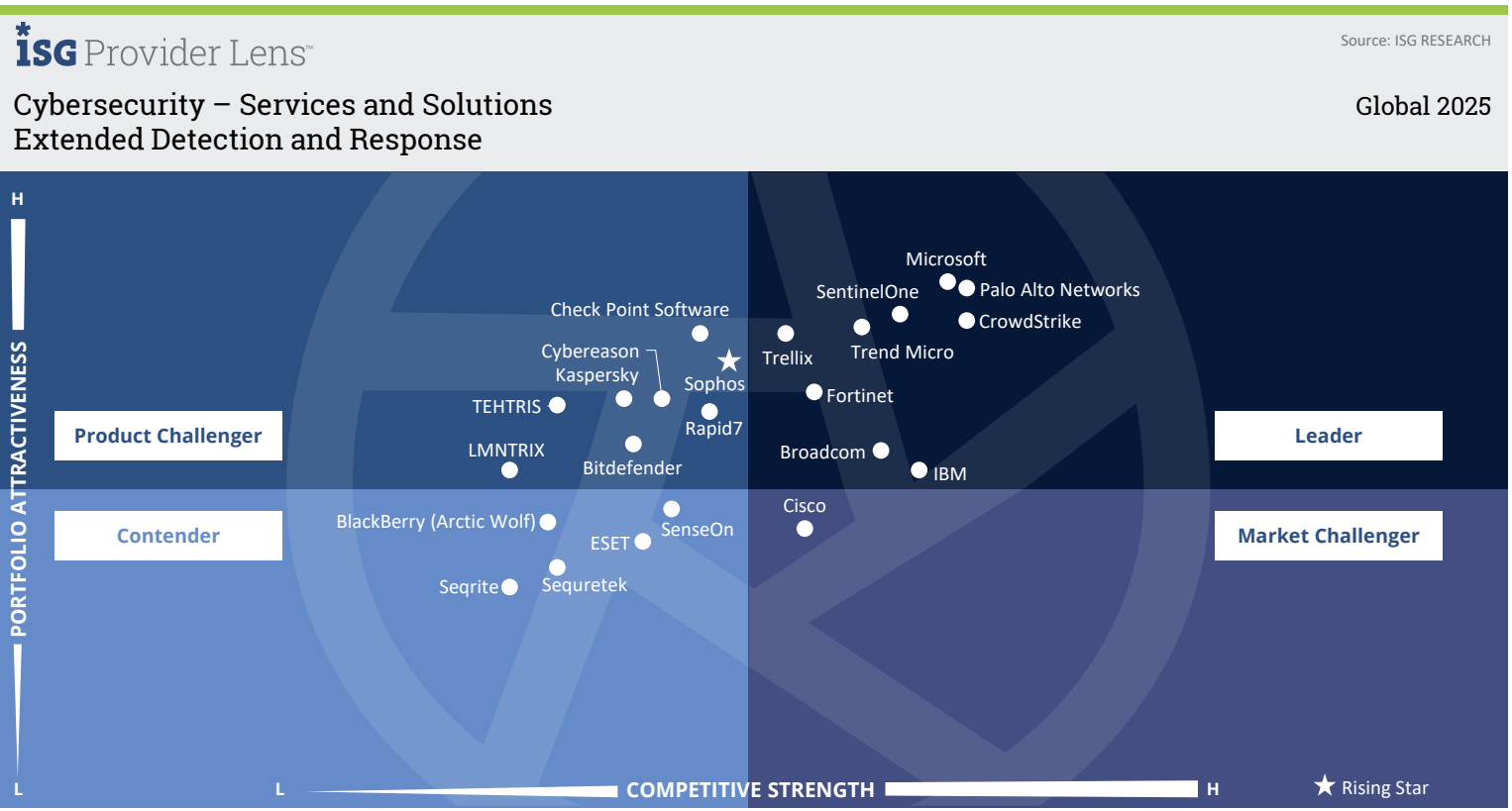
gewinnen aus diesem Bericht einen umfassenderen Überblick über Sicherheitstrends und dahingehend, wie sich die Leistungen der Anbieter zur Entwicklung von robusten Sicherheitsstrategien unterscheiden.

Technologie-Experten

gewinnen durch diesen Bericht Einblicke in die neuen Trends in der Sicherheitslandschaft und die Fähigkeiten der Anbieter, maßgeschneiderte Sicherheitsplattformen zu entwickeln.

Strategie-Experten

werden mit diesem Bericht über die relative Positionierung sowie die Fähigkeiten von Dienstleistern informiert, die den Entscheidungsprozess über Partnerschaften und Initiativen zur Kostensenkung unterstützen.



Dieser Quadrant bewertet die Fähigkeit von XDR-Anbietern und ihren Plattformen, **integrierte Funktionen zur Erkennung, Untersuchung und Reaktion auf Bedrohungen** bereitzustellen, **die die Transparenz und den Bedrohungskontext über mehrere Endpunkte, Netzwerke und Cloud-Umgebungen hinweg verbessern**.

Gowtham Sampath

Definition

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich durch ihre Plattformen aus, die Daten und Warnungen aus verschiedenen Komponenten zur Bedrohungsabwehr, -erkennung und -reaktion integrieren, korrelieren und kontextualisieren. XDR ist eine cloudbasierte Technologie, die mehrere Sicherheitslösungen integriert und Analysen zur Verbesserung der Erkennungsgenauigkeit einsetzt; sie konsolidiert Sicherheitsprodukte, um die Sichtbarkeit und den Bedrohungskontext in allen Arbeitsbereichen, Netzwerken und Workloads eines Unternehmens zu verbessern.

XDR-Lösungen nutzen Telemetrie- und Kontextdaten zur Erkennung und Reaktion und integrieren mehrere Produkte in eine einheitliche Schnittstelle. Sie zeichnen sich durch einen hohen Automatisierungsgrad aus und priorisieren Warnungen nach ihrem Schweregrad, um die erforderlichen maßgeschneiderten Reaktionen festzulegen. Reine Dienstleister, die keine XDR-Lösung auf Basis proprietärer Software anbieten, werden in diesem Quadranten nicht berücksichtigt. XDR-Lösungen zielen darauf ab, die Produktvielfalt, Alarmmüdigkeit und Integrationsprobleme zu verringern. Sie unterstützen Sicherheitsteams bei der Verwaltung von SIEM- (Security Information and Event Management) oder SOAR-Lösungen (Security Orchestration, Automation & Response) und helfen dabei, deren Wert zu steigern.

Auswahlkriterien

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

Beobachtungen

Der XDR-Markt verzeichnet im Zuge der steigenden Nachfrage nach integrierter Bedrohungserkennung, automatisierter Reaktion und fortschrittlicher Analyse über Endgeräte, Netzwerke, Cloud-Umgebungen und Identitäten hinweg eine rasante Entwicklung. Die Anbieter setzen KI und ML offensiv in ihre Plattformen ein, um die Verweilzeiten zu verkürzen, die Bedrohungsanalyse zu beschleunigen und prädiktive, verhaltensbasierte Erkennungsmodelle zu ermöglichen. Dadurch hat sich XDR von einem reaktiven Tool zu einer proaktiven Verteidigungsschicht entwickelt, insbesondere angesichts immer raffinierterer und gezielterer Angriffe.

Die Integration von nativen Lösungen und Lösungen von Drittanbietern ist nach wie vor ein entscheidendes Differenzierungsmerkmal. XDR-Plattformen erweitern die Telemetrie-Ingestion-Funktionen, um SIEMs von Drittanbietern, SOAR-Tools, Threat Intelligence Feeds und angrenzende Sicherheitstechnologien einzubeziehen. Viele Lösungen bieten inzwischen einheitliche Analysten-Workbenches, kuratierte Erkennung und automatisierte Playbooks zur Unterstützung schlanker Security Operations Center (SOC) Teams. Dies erhöht die Transparenz und ermöglicht eine schnellere Korrelation und Kontextualisierung von Warnmeldungen, was Fehlalarme und die Alarmmüdigkeit von Analysten reduziert.

Die Anbieter übernehmen aktiv Konkurrenten und treiben Innovationen voran, um die Fähigkeiten zur Erkennung von Bedrohungen zu verbessern, in neue Kundensegmente zu expandieren oder Know-how im Bereich Managed Detection & Response (MDR) einzubinden.

Für Unternehmen stehen inzwischen weniger die neuesten Tools, sondern die Ergebnisse im Vordergrund, und so entwickeln sich XDR-Plattformen weiter und bieten modulare, in der Cloud bereitgestellte Architekturen mit flexiblen Bereitstellungsmodellen. Die Anbieter fokussieren sich zudem auf modulare Bereitstellungsoptionen für hybride und Multicloud-Umgebungen, damit Unternehmen die Sicherheitsabdeckung erweitern können, ohne die Komplexität zu erhöhen.

Von den 61 Unternehmen, die für diese Studie global bewertet wurden, haben sich 23 für diesen Quadranten qualifiziert; neun dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Broadcom

Die Symantec XDR-Lösung von **Broadcom** bietet eine einheitliche Bedrohungserkennung und -reaktion und integriert Telemetrie für diverse Bereiche. Der Schwerpunkt liegt auf der Verringerung der Alarmmüdigkeit durch Korrelation, Priorisierung und Automatisierung innerhalb eines breiten Ökosystems von Symantec-Lösungen.

CrowdStrike

Die Falcon Insight XDR-Plattform von **CrowdStrike** baut auf der bekannten EDR-Grundlage und der cloud-nativen Architektur auf und bietet eine skalierbare, leistungsstarke Erkennungs- und Reaktionslösung, die Bedrohungsdaten, KI und Verhaltensanalysen kombiniert.

Fortinet

FortiXDR von **Fortinet** bietet erweiterte Erkennungs- und Reaktionsmöglichkeiten durch die enge Integration in seine native Sicherheitsstruktur, u.a. Netzwerk, Endpunkt, E-Mail und Cloud. Der Schwerpunkt der Plattform liegt auf automatisierten Reaktionen, KI-gesteuerten Analysen und tiefer Telemetrie-Korrelation.

IBM

Im Mittelpunkt der XDR-Strategie von **IBM** steht die QRadar Suite, die Funktionen zur Erkennung, Untersuchung und Reaktion auf Bedrohungen in hybriden Umgebungen vereint. Die Plattform zeichnet sich durch offene Integration, KI-gesteuerte Automatisierung und tiefe Threat Intelligence über IBM X-Force aus.

Microsoft

Der 100-prozentige Schutz von **Microsoft** Defender XDR in den MITRE Engenuity ATT&CK® Evaluations weist vollständige Sichtbarkeit und den Schutz über alle Angriffsstadien hinweg nach, u.a. in Windows und Linux, was die robuste plattformübergreifende Unterstützung unterstreicht.

Palo Alto Networks

Palo Alto Networks hat die Übernahme von IBMs QRadar SaaS Assets abgeschlossen. Ziel des Unternehmens ist es, seinen Kunden fortschrittliche Sicherheitslösungen auf Basis von SOCs der nächsten Generation und KI zu bieten.

SentinelOne

SentinelOne wird sein altes Deception-Produkt einstellen; der Anbieter will sich auf wachstumsstärkere Segmente konzentrieren und Investitionen in KI-gestützte Sicherheit Priorität einräumen. SentinelOne ist autorisiert, KI-gestützte Sicherheitstools an Bundesbehörden der höchsten Sicherheitsstufe zu verkaufen.

Trellix

Trellix bietet eine offene und anpassungsfähige XDR-Plattform zur Unterstützung dynamischer Verteidigungsstrategien. Der Schwerpunkt liegt auf Integration, Threat Intelligence und ML, um eine schnellere Erkennung und autonome Reaktion in Unternehmensumgebungen zu ermöglichen.

Trend Micro

Trend Micro hat Trend Cybertron auf den Markt gebracht, ein spezialisiertes Cybersecurity Large Language Model (LLM), das in seine Trend Vision One Plattform integriert ist. Dieser innovative, KI-gestützte Cybersecurity-Agent soll Unternehmen zum Wechsel auf ein proaktives Sicherheitsmodell verhelfen.

Sophos

Die jüngste Übernahme des MDR-Geschäftsbereichs von Secureworks durch **Sophos** (Rising Star) dürfte die Fähigkeiten des Anbieter zur Erkennung von Bedrohungen, die servicebasierten Angebote und die Intercept X-Plattform mit verbesserter Transparenz und Automatisierung erheblich ausbauen.

Security Service Edge (Global)

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Security Service Edge (SSE)**-Produkte weltweit anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Anbieter evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Provider, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz. Unternehmen gewinnen anhand dieses Berichtes Einblicke in die Anbieter von Security Service Edge (SSE)-Produkten, die für die Gewährleistung der Sicherheit in hybriden und Multicloud-Umgebungen entscheidend sind.

Datenmanagement-Experten

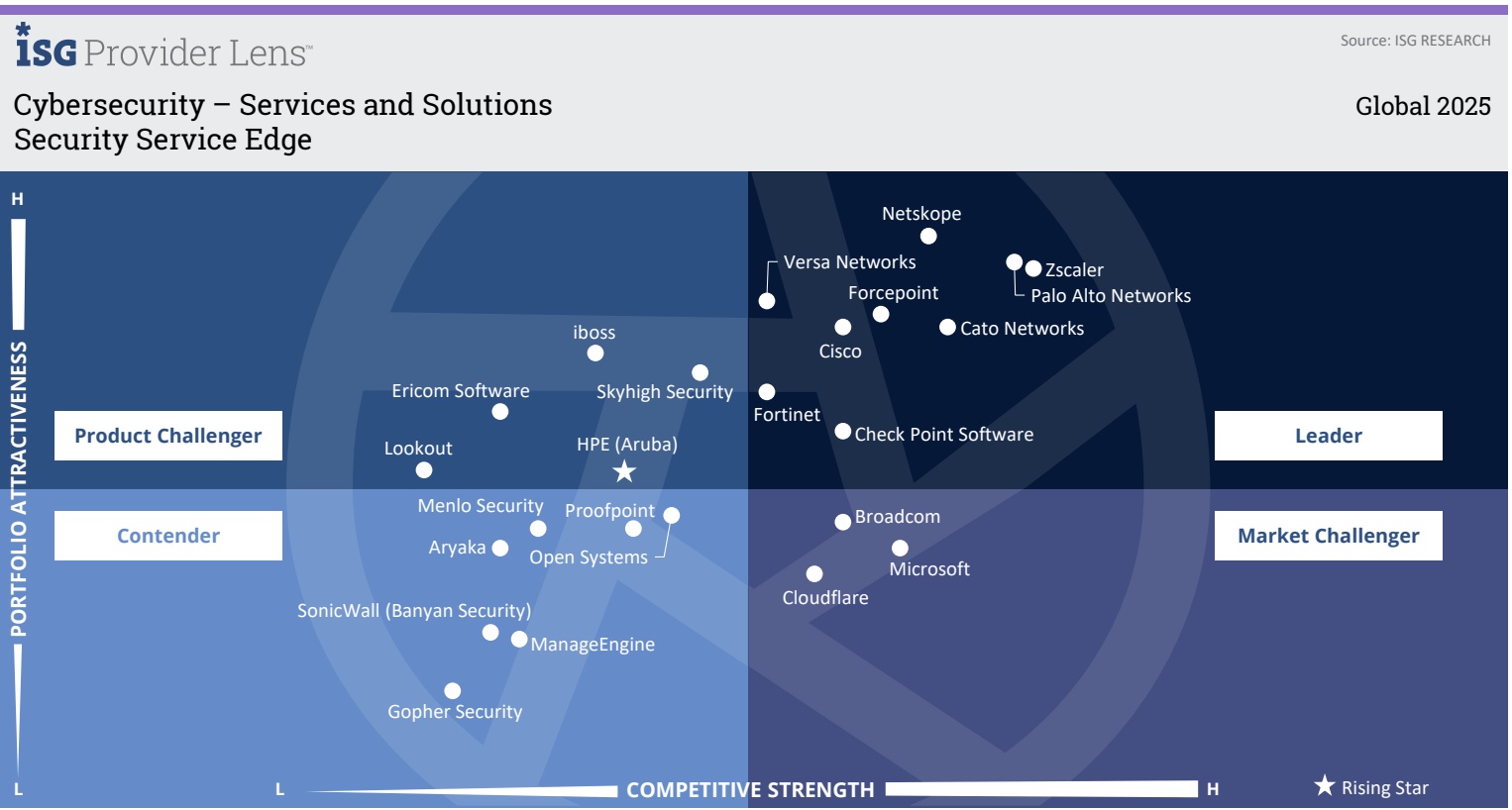
sollten diesen Bericht lesen, um zu verstehen, wie SSE-Anbieter Unternehmen dabei helfen, die Herausforderungen zu meistern, die sich aus der Datengesetzgebung ergeben, und zwar durch verbesserte Richtlinienkontrolle und Berichterstattung.

Technologieexperten

gewinnen aus diesem Bericht ein besseres Verständnis dahingehend, wie SSE-Anbieter bei der Einführung von unternehmensweiten Zero-Trust-Frameworks dabei helfen, ihre Sicherheitslage zu verbessern.

Strategieexperten

erhalten mit diesem Bericht Einblicke in die kritischen Fähigkeiten von SSE-Anbietern und deren Fokus auf Benutzerorientierung, um Sicherheit am Edge bzw. für Geräte über die Cloud bieten zu können.



In diesem Quadranten geht es insbesondere um die User Experience; es werden SSE-Anbieter bewertet, die **cloud-zentrierte Lösungen** offerieren und verschiedene Angebote integrieren, um einen sicheren Zugang zu Cloud-, **SaaS- und Webdiensten sowie privaten Anwendungen** zu ermöglichen.

Yash Jethani

Security Service Edge (Global)

Definition

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

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

Auswahlkriterien

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

Beobachtungen

Für die meisten Unternehmen sind SASE- oder SSE-Architekturen mit integrierter Sicherheit und Vernetzung eine Priorität. Der Umstieg auf cloud-native Diensten für Skalierbarkeit und Ausfallsicherheit nimmt zu; KI verbessert zunehmend die Abwehr von Bedrohungen und den Schutz von Daten. Zero Trust wird allgemein für die Sicherung des Anwendungs- und Datenzugriffs empfohlen. Viele Anbieter expandieren weltweit und verstärken ihr Angebot durch Partnerschaften; der Fokus liegt dabei meist auf Cybersicherheit, Datenschutz und Bedrohungsabwehr.

Zu den Differenzierungsmerkmalen der führenden Anbieter zählen allerdings eher die kontextbezogene Durchsetzung von Richtlinien, zukunftssichere Sicherheit und strategische Wachstumspartnerschaften. Viele Anbieter heben fortschrittliche Bedrohungsabwehr und Datenschutz als Hauptstärken hervor und bieten integrierte oder cloud-native Lösungen für verschiedene Umgebungen an. Insbesondere Innovationen im Bereich der KI-gesteuerten Sicherheit, intelligente Dienstleistungen für Zielmärkte und die Vorschau auf neue Technologien wie sichere Browser, Quanten- und KI-Anwendungen sind Alleinstellungsmerkmale. Die Konvergenz von Netzwerken und Sicherheit für Hochleistungsumgebungen erfordert zudem, dass die Anbieter ihre Fähigkeiten ständig anpassen und erweitern, um die Komplexität der modernen Sicherheit bewältigen zu können. UX und cloud-native Skalierbarkeit sind wichtige Prioritäten, insbesondere für HPE (Aruba) und Fortinet über globale PoPs und Partnerschaften. Single-Vendor-Lösungen von Versa und Netskope optimieren die Bereitstellung; Prisma SASE von Palo Alto wiederum zielt auf das Digital Experience Monitoring (DEM) ab. Das prognostizierte Marktwachstum dürfte sich im Zuge der Zunahme an KI-Anwendungen, die die Sicherheit neu gestalten werden, verdrei- bis verfünffachen.

Von den 61 Unternehmen, die für diese Studie global bewertet wurden, haben sich 24 für diesen Quadranten qualifiziert; neun dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Cato Networks

Cato Networks liefert die skalierbare, robuste Cato Single Pass Cloud Engine (Cato SPACE) Architektur für einen globalen Cloud-Service mit umfassender kontextbezogener Richtliniendurchsetzung auf Basis von Netzwerk-, Geräte-, Identitäts-, Anwendungs- und Datenattributen.

Checkpoint

Checkpoint setzt auf Quantum SASE und Harmony Connect mit Fokus auf Cloud-Sicherheit und ZTNA. Partnerschaften, u.a. mit Tata Communications, verbessern die globale Reichweite und fördern das regionale Wachstum durch Auszeichnungen, Beratungsexpertise, globale Forschung & Entwicklung sowie KI-gesteuerte Sicherheitsinnovationen.

Cisco

Cisco hat auf dem Mobile World Congress 2025 seine Bedrohungsabwehr vorgestellt und für 2025 die Integration von KI-Assistenten angekündigt.

Forcepoint

Forcepoint etabliert sich mit seiner Forcepoint ONE™-Plattform als Marktführer im Bereich Datenschutz und KI und bietet eine umfassende cloud-native SSE-Lösung für die Cloud, das Web, private Apps und Endpunkte.

FortiSASE

FortiSASE von Fortinet stützt sich auf Partnerschaften und die KI-Services von FortiGuard und zielt mit einem Lizenzierungsmodell auf hybride Umgebungen ab. Der Anbieter fokussiert sich auf Verbesserungen von einheitlichen SASE-Lösungen, die Weiterentwicklung von Hybrid-Mesh Firewalls und die Integration von OT-Sicherheit.

Netskope

Netskope bewirbt seine intelligenten SSE- und NewEdge-Cloud-Lösungen und hat im Januar 2024 eine auf MSPs zugeschnittene SASE-Lösungen für das Mittelstandssegment auf den Markt gebracht, die auf Zero-Trust-Telemetrie setzt.

Palo Alto Networks

Palo Alto Networks rechnet mit einer Verdrei- bis Verfünffachung der Zahl an KI-Apps - und damit mit einem Schub für die Nutzung seines sicheren Browsers. In Prisma SASE wird KI integriert, und SSE zeichnet sich durch starke Zero Trust- und Threat Prevention-Funktionen aus.

Versa Networks

Versa Networks verfügt über mehr als 100 Gbps Unified SASE Gateways und konzentriert sich auf die Konsolidierung von Netzwerken und Sicherheit für Großunternehmen über ein robustes Partner-Ökosystem.

zscaler

Zscaler hebt seine Zero-Trust-SASE-Lösung mit neuen SD-WAN-Funktionen hervor, die im Januar 2024 eingeführt wurden und den Fokus auf eine nahtlose UX und KI-gesteuerte Sicherheitsverbesserungen legen.

HPE (Aruba)

HPE (Aruba) (Rising Star) hat nach der Übernahme von Axis Security im Jahr 2023 seine SSE-Lösungen mit SD-WAN integriert. Mit den zusätzlichen KI-Verbesserungen und der geplanten Übernahme von Juniper Networks (im Jahr 2025) kann der Anbieter seine Fähigkeiten weiter ausbauen.

Technical Security Services

Wer sollte dieses Kapitel lesen

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

Technologie-Experten

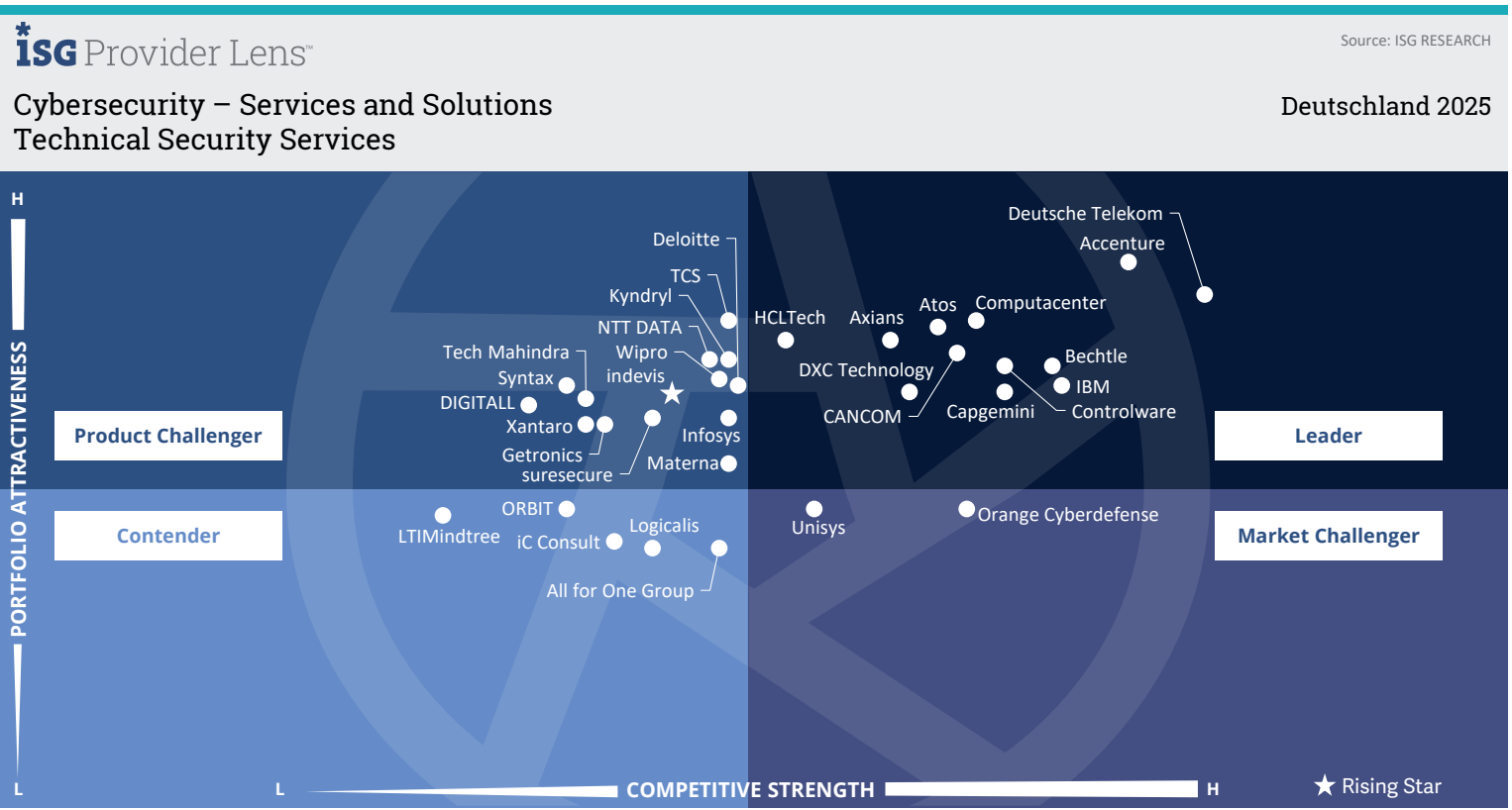
gewinnen aus diesem Bericht ein besseres Verständnis dahingehend, wie die Integrationsleistungen der Anbieter die Auswirkungen von Bedrohungen im Zuge der Modernisierung von Altsystemen und des Einsatzes fortschrittlicher Technologien verringern können.

Sicherheits- und Datenexperten

gewinnen durch diesen Bericht Einblicke in die Einhaltung der Sicherheits- und Datenschutzgesetze durch die Anbieter und können entsprechenden Markttrends Rechnung tragen.

Experten aus den Fachabteilungen

hilft dieser Bericht, Datensicherheit, CX und Datenschutz im Zusammenhang mit der derzeit so wichtigen digitalen Transformation in Balance zu bringen.



In diesem Quadranten geht es um die **relevantesten** Anbieter von technischen Security Services in Deutschland, deren Leistungen **nicht nur die eigenen Produkte** abdecken. Durch den Fachkräftemangel spielen **externe Provider** eine immer **wichtigere Rolle**.

Frank Heuer

Definition

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

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

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

Auswahlkriterien

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

Beobachtungen

Die immer intensiveren wie auch raffinierteren, komplexeren und ständig neuen Cyberattacken sind für Unternehmen in Deutschland nach wie vor eine Herausforderung, die durch den Mangel an Cybersecurity-Experten noch erschwert wird. Daher sind Firmen immer häufiger darauf angewiesen, externe Dienstleister in Anspruch zu nehmen. 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.

Der deutsche Dienstleister indevis ist neuer Rising Star. Getronics, LTIMindtree, ORBIT und Xantaro sind neu im Quadranten vertreten. Alice&Bob.Company wurde nicht mehr in diesen Quadranten aufgenommen. Noch nicht für den Quadranten hat sich Riedel Networks aus dem hessischen Butzbach qualifiziert, bringt für die Zukunft aber gute Voraussetzungen durch die zeitgemäße Integration von Netzwerk- und Security-Solutions mit.

Von den 68 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 33 für diesen Quadranten qualifizieren. Dabei erreichten 12 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Die Security Automation Factory von **Accenture** unterstützt bei der Transformation von prozess- und ressourcenintensiven Aufgaben mit Hilfe von Robotic Process Automation. Accenture deckt ein sehr umfangreiches Themen- wie auch Leistungsspektrum ab.

Atos

Atos ist mit den Anforderungen und gesetzlichen Regelungen im Zusammenhang mit Security-Projekten vertraut und unterstützt seine Kunden bei der Einhaltung dieser Vorgaben. Atos verfolgt einen ganzheitlichen Cybersecurity-Ansatz, der auch die Geschäftsrelevanz betont.

axians

Axians IT Security unterhält Partnerschaften mit zahlreichen renommierten Cybersecurity-Technologieanbietern. Die technischen IT-Sicherheitsdienstleistungen von Axians lassen keine Wünsche offen und adressieren ein sehr breites Spektrum.

BECHTLE

Bechtle zeigt hierzulande große lokale Präsenz und ist in Deutschland mit zahlreichen Standorten vertreten. Bechtle ist ein profilierter Anbieter von Technical Security Services für das dynamisch wachsende Marktsegment der mittelständischen Unternehmen.

CANCOM

Die Technical Security Services von **CANCOM** decken sowohl ein umfangreiches Themen- als auch Leistungsspektrum ab. Mit seinen Technical Security Services hat CANCOM einen starken Fokus auf mittelständische Unternehmen.

Capgemini

Capgemini ist ein Security-Dienstleister mit Thought Leadership. Der Anbieter ist in der Lage, im Rahmen von Cybersecurity-Projekten für seine Kunden fortschrittliche Technologien wie Security Automation und künstliche Intelligenz einzusetzen.

Computacenter

Die Technical Security Services von **Computacenter** sind sehr breit aufgestellt. Computacenter unterhält Beziehungen zu zahlreichen großen IT-Sicherheitsherstellern sowie vielen kleineren und aufstrebenden Anbietern.

controlware

Mit seiner deutschen Herkunft ist **Controlware** insbesondere im Schwerpunktsegment des gehobenen Mittelstands, der Dienstleistern mit deutschen Wurzeln besonderes Vertrauen entgegenbringt, gut aufgestellt. Das Angebot von Controlware ist bedarfsgerecht modular aufgebaut.

T

Die **Deutsche Telekom** bietet ihren Kunden lückenlose Technical Security Services, die ein komplettes Spektrum an Themen abdecken. Das Expertenteam für Cybersecurity ist sehr groß. Mit „Security made in Germany" kann die Deutsche Telekom nicht nur im Mittelstand punkten.

DXC TECHNOLOGY

DXC Technologys Portfolio beinhaltet integrierte Lösungen aus Cybersecurity und verbundener IT-Technologie. Die globale Präsenz und die globalen Ressourcen sind umfangreich.

HCLTech

HCLTech ist zunehmend erfolgreich und steigt vom Rising Star zum Leader im deutschen Markt für technische Cybersecurity-Dienstleistungen auf. Dazu tragen die große Erfahrung, das umfassende Portfolio sowie hochklassige Partnerschaften bei.

IBM

IBM ist ein erfahrener und erfolgreicher Cybersecurity-Technologieanbieter und besitzt ein tiefes Verständnis von IT-Security-Lösungen. IBM ist im deutschen Markt mit einem der breitesten Portfolios für IT Security Services vertreten.

indevis

Der neue „Rising Star" für technische Cybersecurity-Dienstleistungen in Deutschland ist **indevis**. Dazu tragen Erfahrung, Kompetenz und die entschlossene Erweiterung des Geschäftes bei.

Leader

„Das modulare Angebot von Controlware ist sehr gut auf die Bedürfnisse des wachstumsstarken Mittelstandssegments eingestellt. Diese Zielgruppe schätzt auch sehr Security-Lösungen „made in Germany“.“

Frank Heuer

Controlware

Übersicht

Controlware ist ein deutscher IT-Dienstleister mit Hauptsitz in Dietzenbach in Hessen, beschäftigt rund 1.000 Mitarbeitende und unterhält ein Vertriebs- und Servicenetz mit 16 Standorten in Deutschland, Österreich und der Schweiz. Neben Strategic und Managed Security Services bietet Controlware auch Technical Security Services an, mit denen Kunden vom gehobenen Mittelstand bis zu Großunternehmen und großen öffentlichen Kunden adressiert werden. Mit seinen Dienstleistungen deckt Controlware Cloud-, On-Premise- und hybride Lösungen ab.

Stärken

Zahlreiche qualifizierte Experten: Es wird ein umfangreiches Expertenteam für die technischen IT-Security-Leistungen zur Verfügung gestellt. Controlware kann dabei nicht nur quantitativ punkten; die Mitarbeiter verfügen auch über zahlreiche Security-Zertifizierungen.

Deutscher Dienstleister: Mit seiner Herkunft ist Controlware insbesondere im Schwerpunktsegment des gehobenen Mittelstands, der lokal präsenten Dienstleistern besonderes Vertrauen entgegenbringt, gut aufgestellt.

Schwerpunkt im Wachstumssegment: Controlware ist stark im gehobenen deutschen Mittelstand aufgestellt. Mit dem Schwerpunkt im Segment der mittelgroßen Unternehmen kann der Anbieter vom überdurchschnittlichen Wachstum des Mittelstands profitieren.

Umfassendes Portfolio ist modular strukturiert: Das Angebot von Controlware für technische IT-Sicherheitsdienstleistungen ist modular aufgebaut. So ist es möglich, die Bedürfnisse der Kunden optimal und individuell abzudecken. Zudem wird auf diese Weise der Aufwand für die Realisierung der Lösungen auf das Notwendige beschränkt. Abhängig von den Anforderungen der Kunden kann Controlware die gesamte Wertschöpfungskette für Cloud-, On-Premises- und Hybrid-Umgebungen abdecken.

Herausforderungen

Die Technical-Security-Dienstleistungen von Controlware sind umfangreich, decken jedoch bislang keine Data Leakage/Loss Prevention ab. Ein entsprechender Ausbau des Angebotes könnte erwägenswert sein.

Strategic Security Services

Wer sollte dieses Kapitel lesen

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

Cybersecurity-Experten

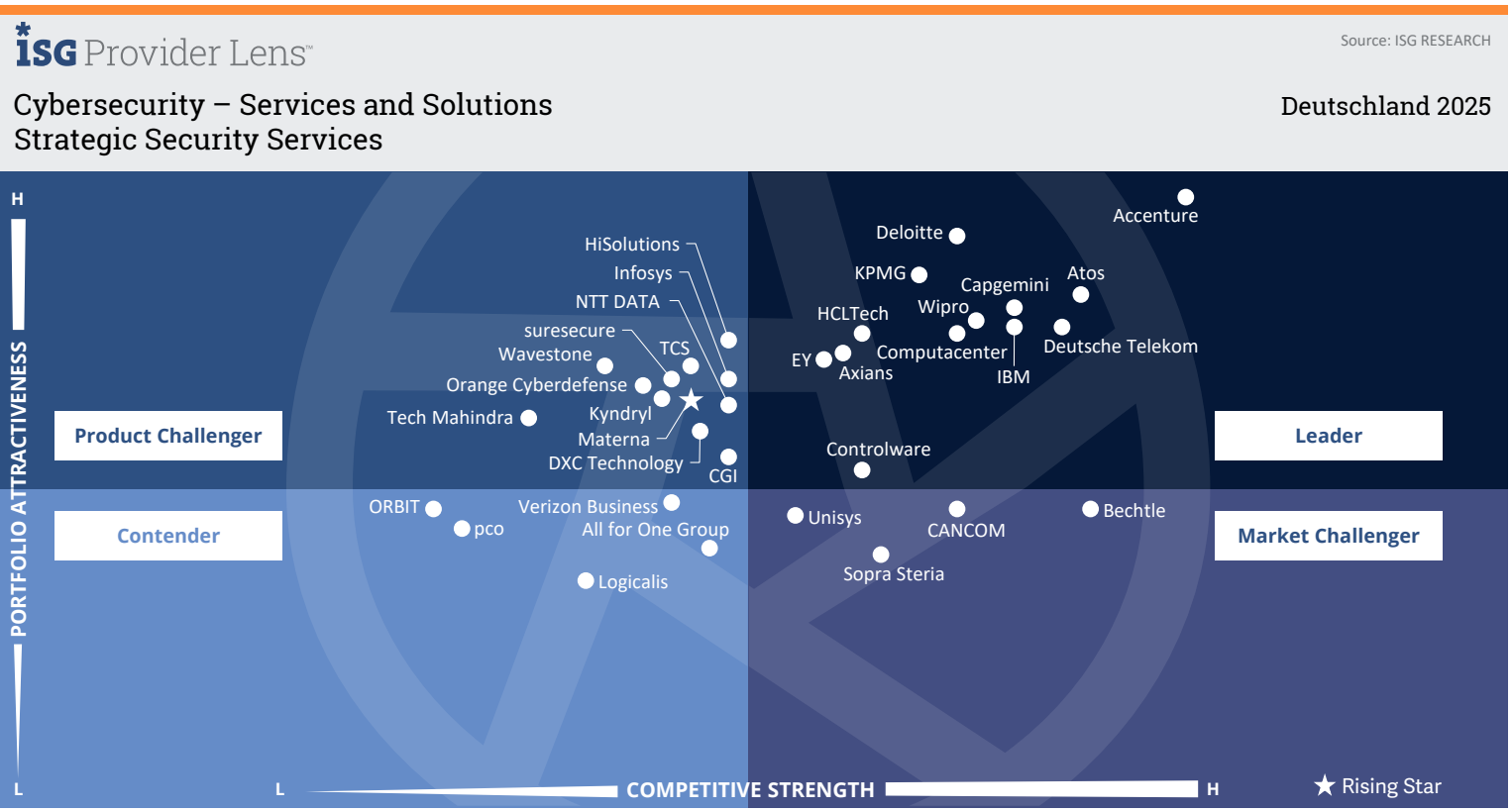
gewinnen aus diesem Bericht einen umfassenderen Überblick über Sicherheitstrends und die Leistungen der Anbieter bei der Entwicklung von Sicherheitsstrategien.

Technologie-Experten

werden mit diesem Bericht über die neuen Trends in der Sicherheitslandschaft und die Fähigkeiten der Anbieter, maßgeschneiderte Sicherheitsplattformen zu entwickeln, informiert.

Strategie-Experten

werden mit diesem Bericht über die relative Positionierung und die Fähigkeiten von Dienstleistern informiert, die zu fundierten Entscheidungsprozessen bezüglich Partnerschaften und Initiativen zur Kostensenkung beitragen können.



In diesem Quadranten geht es um die **relevantesten** Cybersecurity-Berater in Deutschland, die Leistungen **nicht nur für die eigenen Produkte** offerieren. Zunehmende Cyberbedrohungen und neue Technologien führen zu **wachsender Nachfrage**.

Frank Heuer

Definition

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

Sie beschäftigen erfahrene Sicherheitsberater für die Planung und Verwaltung von umfassenden Sicherheitsprogrammen für Unternehmenskunden. Angesichts der steigenden Nachfrage von KMUs und des Fachkräftemangels stellen SSS Provider Experten auf Abruf über virtuelle CISO-Dienste zur Verfügung. Sie erstellen Geschäftskontinuitätspläne, legen Prioritäten für die Wiederherstellung kritischer Anwendungen fest und führen praktische Notfallübungen durch, um die Cyberkompetenz und die Reaktionsfähigkeit von Unternehmensführern und Mitarbeitenden zu verbessern. Hinzu kommt Unterstützung bei der Auswahl von Sicherheitstechnologien und Lieferanten, der Überprüfung von Organisationsstrukturen für die Cybersicherheit sowie der Bewertung von Sicherheitsprozessen und -praktiken und deren Verbesserung im Hinblick auf bestehende Risiken. In diesem Quadranten werden Dienstleister betrachtet, die sich nicht ausschließlich auf eigene Produkte bzw. Lösungen fokussieren.

Auswahlkriterien

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

Beobachtungen

Cybersecurity-Gefährdungen werden immer bedrohlicher – zunehmend auch für neue Zielgruppen. Der Ukraine-Krieg mit seinen Begleiterscheinungen ist dabei nur ein Beispiel für das Anfachen von Bedrohungen; kommerziell motivierte Cyber-Angriffe sind weiterhin nicht minder Anlass für Besorgnis. Zudem zeichnen sich neue, technisch ausgefeilte Bedrohungen ab.

Von Cyber-Bedrohungen 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. Aufgrund dieser Faktoren benötigen Unternehmen zunehmend externe Unterstützung. Am Anfang steht hierbei häufig die Beratung.

Unter anderem sind Dienstleister im Vorteil, die ihren Kunden neben Sicherheitsberatung auch -Umsetzung und -Betrieb anbieten können, damit die Strategie bruchlos umgesetzt werden kann, und ebenso Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen – gegebenenfalls auch zugehörige neugestaltete Geschäftsprozesse – aus einem Guss anbieten können. Zunehmend stellen sich Berater auf Consulting zur Abwehr von quantum-basierenden Cyber-Attacken ein – zumal durch den „Harvest now – decrypt later"-Ansatz die Gefahr drängender als bisher angenommen ist.

Materna ist der neue Rising Star. ORBIT und pco sind neu im Quadranten vertreten, Secureworks nicht mehr. Noch nicht für den Quadranten hat sich die DGC AG aus Flensburg qualifiziert. Dieser Dienstleister bringt für die Zukunft durch die Konzentration auf die Cybersecurity-Beratung und die Herkunft aus Deutschland aber gute Voraussetzungen mit.

Von den 68 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 34 für diesen Quadranten qualifizieren. Dabei erreichten 13 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Die Berater von **Accenture** zeichnen sich durch große Kompetenz und Erfahrung aus – einer der Gründe dafür, dass sie Zugang zur Vorstandsebene haben. Das Serviceportfolio ist sehr breit und wird systematisch weiterentwickelt.

Atos

Atos verfolgt in der Cybersecurity-Beratung einen ganzheitlichen Ansatz. Der Anbieter ist in der Lage, im Rahmen seiner Security-Beratung bei seinen (potenziellen) Kunden Vertrauen durch zahlreiche Zertifizierungen zu schaffen.

axians

Axians IT Security kann im deutschen Markt für Cybersecurity Consulting mit pragmatischen, zielgerichteten Lösungen speziell bei mittelständischen Unternehmen punkten. Der Anbieter verfügt über ein starkes Partnernetzwerk.

Capgemini

Das Beratungsspektrum von **Capgemini** zum Thema Cybersecurity ist sehr umfangreich und wird weiter ausgebaut. Capgemini profiliert sich des Weiterem mit seinem erfahrenen Beraterteam, das sich nicht nur auf die Theorie, sondern auch auf die praktische Umsetzung versteht.

Computacenter

Computacenter kann sich mit einem ganzheitlichen Security-Ansatz und Verständnis für die Infrastruktur- und Geschäftsanforderungen der Kunden als strategischer Partner positionieren. Das Beratungsportfolio und die adressierten Security-Themen sind sehr umfangreich.

controlware

Dank Expertise und Kundenorientierung steigt **Controlware** zum Leader für Strategic Security Services in Deutschland auf.

Deloitte.

Deloitte kann eine starke globale Präsenz vorweisen und besitzt im Rahmen der Security-Beratung ein tiefes Verständnis auch für die speziellen Businessbedürfnisse seiner Kunden in Deutschland.

Deutsche Telekom bietet ihren Kunden End-to-End-Dienstleistungen aus einer Hand, besitzt zudem Expertise auch für anspruchsvolle Umgebungen und verfügt über langjährige zertifizierte Cybersecurity-Kompetenz.

EY

Umfassende Branchenkenntnisse, ein ganzheitlicher Beratungsansatz und große Erfahrung tragen dazu bei, dass **EY** wieder unter die führenden Anbieter für Strategic Security Services in Deutschland zurückkehrt.

HCLTech

HCLTech steigt in Deutschland unter die führenden Anbieter von Strategic Security Services auf. Dazu tragen ein umfangreiches und zeitgemäßes Beratungsangebot bei.

IBM

Das Portfolio von **IBM** für die Beratung im Bereich Cybersecurity ist umfassend, integriert und innovativ. Das Security Consulting von IBM fußt auf tiefen technischen Insights, die auch aus der Erfahrung von IBM als Security-Produktanbieter resultieren.

KPMG

KPMG vermag es, in seiner Beratung zu Cybersecurity-Themen geschickt Business- und technisches Verständnis miteinander zu verbinden. Die Berater von KPMG besitzen im Rahmen der Sicherheitsberatung auch hohe strategische Kompetenz.

wipro

Wipro offeriert ein umfangreiches Portfolio für die Cybersecurity-Beratung und besitzt großes technisches Fachwissen, welches in die Cybersicherheitsberatung einfließt.

MATERNA RADAR CYBER SECURITY

Materna ist der neue „Rising Star" im deutschen Markt für Strategic Security Services. Dies hat der Dienstleister durch verstärkte Konzentration auf Beratungsleistungen erreicht.

Leader

„Controlware steigt durch Expertise und Kundenorientierung zum führenden Anbieter für Strategic Security Services in Deutschland auf."

Frank Heuer

Controlware

Übersicht

Controlware ist ein deutscher IT-Dienstleister mit Hauptsitz in Dietzenbach in Hessen, beschäftigt rund 1.000 Mitarbeitende und unterhält ein Vertriebs- und Servicenetz mit 16 Standorten in Deutschland, Österreich und der Schweiz. Neben Technical und Managed Security Services bietet Controlware auch Strategic Security Services an, mit denen Kunden vom gehobenen Mittelstand bis zu Großunternehmen und großen öffentlichen Kunden adressiert werden. Mit seinen Dienstleistungen deckt Controlware Cloud-, On-Premise- und hybride Lösungen ab.

Stärken

Hybrides Konzept für Kundenorientierung: Controlware kombiniert die Vorteile seiner bundesweit verteilten regionalen Niederlassungen mit seinen Competence Centern, die sich auf Spitzentechnologien und das dazugehörige Prozess- und Methodenwissen spezialisieren. Die Kombination der regionalen Niederlassungen und der zentralen Einheiten ermöglicht es, ein tiefes Verständnis für die Kunden zu entwickeln.

Schwerpunkt im Wachstumssegment: Controlware ist stark im gehobenen deutschen Mittelstand aufgestellt. Mit dem Schwerpunkt im Segment der mittelgroßen Unternehmen kann der Anbieter vom überdurchschnittlichen Wachstum des Mittelstands profitieren.

Zahlreiche qualifizierte Experten: Es wird ein umfangreiches Expertenteam für die technischen IT-Security-Leistungen zur Verfügung gestellt. Controlware kann dabei nicht nur quantitativ punkten; die Mitarbeiter verfügen auch über zahlreiche Security-Zertifizierungen.

Deutscher Dienstleister: Mit seiner Herkunft ist Controlware insbesondere im Schwerpunktsegment des gehobenen Mittelstands, der lokal präsenten Dienstleistern besonderes Vertrauen entgegenbringt, gut aufgestellt.

Herausforderungen

Zur Erreichung einer noch stärkeren Marktposition könnte es hilfreich sein, die internationale Präsenz selektiv auszubauen, zum Beispiel in der EU und den USA. So könnte Controlware bei entsprechenden Interessenten noch häufiger in die engere Wahl kommen.

Next-Gen SOC/MDR Services

Wer sollte dieses Kapitel lesen

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

Cybersecurity-Experten

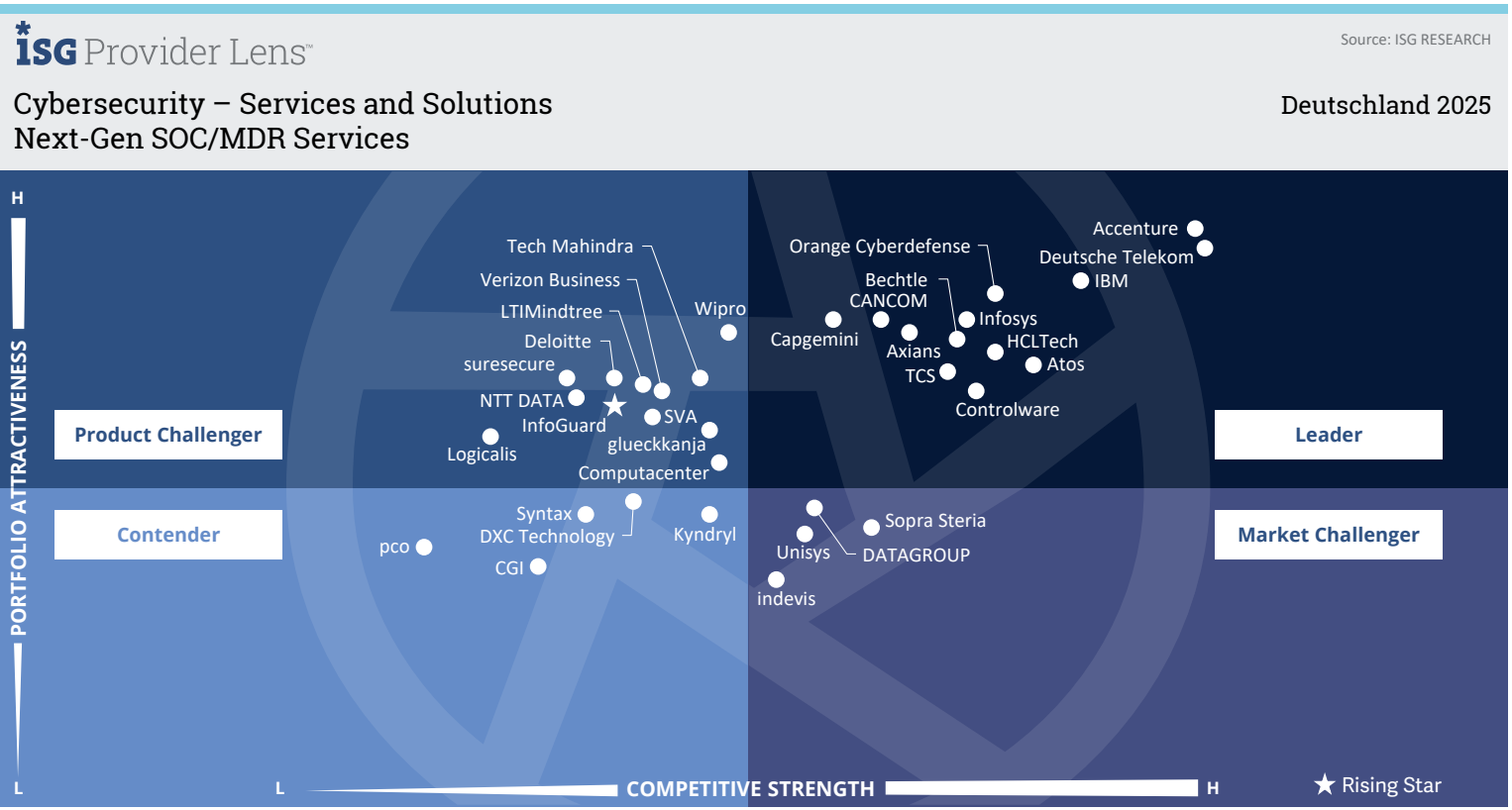
hilft dieser Bericht die neuen Trends und unmittelbaren Bedrohungen zu verstehen. Er kann bei der strategischen Entscheidungsfindung helfen und gleichzeitig die Produktivität steigern und die Komplexität von Sicherheitsmaßnahmen reduzieren.

Technologieexperten

werden mit diesem Bericht über sich abzeichnende Trends informiert, gewinnen Einblicke in maßgeschneiderte Sicherheitsplattformen und strategische Ziele und können so der sich verändernden Sicherheitslandschaft Rechnung tragen.

Experten auf der Geschäftsseite

gewinnen aus diesem Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht werden können, und werden über praktische Lösungen zur Reduzierung der Komplexität und Effizienzsteigerung informiert.



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

Frank Heuer

Definition

Die in diesem Quadranten bewerteten Anbieter offerieren Services im Zusammenhang mit der kontinuierlichen Überwachung von IT- und OT-Infrastrukturen durch ein Security Operations Center (SOC). Es werden Dienstleister untersucht, die sich nicht ausschließlich auf proprietäre Produkte konzentrieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Reaktion auf und Behebung von Problemen.

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

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

Auswahlkriterien

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

Beobachtungen

Die Nachfrage nach Managed Detection & Response (MDR) Services und Diensten von Security Operations Centers (SOCs) wird durch immer raffiniertere, häufigere, komplexere und wandlungsfähigere Cyberattacken getrieben. Das erforderliche stets aktuelle Spezialistenwissen und der gleichzeitige Mangel an qualifizierten Fachleuten rücken diese Managed Services zunehmend in den Fokus deutscher Unternehmen.

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

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

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

InfoGuard ist der neue Rising Star. pco ist neu im Quadranten vertreten, Materna Radar nicht mehr, da sich der Themenfokus verändert hat. Noch nicht für den Quadranten haben sich Advens, CyberProof, I-TRACING und Riedel Networks qualifiziert, sie zeigen jedoch vielversprechende Ansätze für eine zukünftige Präsenz in der Anbieterbewertung.

Von den 68 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 34 für diesen Quadranten qualifizieren. Dabei erreichten 13 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

Accenture offeriert seinen Kunden ein sehr umfangreiches Spektrum an Leistungsmerkmalen und kann sämtliche Themen aus einer Hand abdecken. Accenture kommt den Anforderungen seiner oft global aktiven Großkunden durch die eigene internationale Präsenz sehr gut entgegen.

Atos

Deutschland zählt zu den SOC-Standorten von **Atos**, was auch für viele Großunternehmen interessant ist. Sowohl die abgedeckten Themen als auch die Leistungen der Next-Gen SOC/MDR Services adressieren ein breites Spektrum.

axians

Axians IT Security offeriert im Rahmen seiner Next-Gen SOC/MDR Services ein breites Spektrum an Services und gemanagten Security-Themen. Für besonders gefährdete Daten und Systeme werden ein erhöhtes Maß an Sicherheit und flexible Lösungen geboten.

BECHTLE

Bechtles Next-Gen SOC/MDR Services decken ein breites Spektrum an Leistungen und gemanagten Technologien ab. Zudem sind sie modular anpassungsfähig. Bechtle betreibt auch in Deutschland ein dediziertes SOC mit deutschsprachigem Support.

CANCOM

Das Next-Gen SOC/MDR Services Portfolio von **CANCOM** deckt ein breites Spektrum an gemanagten Technologien ab und bietet zahlreiche Leistungen. CANCOM betreibt unter anderem in Deutschland ein dediziertes Security Operations Center.

Capgemini

Capgemini bietet im Rahmen seiner Next-Gen SOC/MDR Services vielfältige Dienstleistungen an, die ein breites Spektrum gemanagter Security-Themen adressieren. Speziell auch gemessen an der Anzahl der Kunden stellt Capgemini in Deutschland ein großes Expertenteam bereit.

controlware

Speziell auch gemessen an der Anzahl der Kunden unterhält **Controlware** in Deutschland ein großes Expertenteam und offeriert seinen Kunden modulare, individualisierbare Next-Gen SOC/MDR Services.

Die **Deutsche Telekom** betreibt Next-Gen SOC/MDR Services unter anderem in Deutschland und unterhält hierzulande zudem ein äußerst großes Team für seine Services. Der Anbieter entwickelt sein bereits sehr umfassendes Angebot kontinuierlich weiter.

HCLTech

Allein in Deutschland betreibt **HCLTech** mehrere dedizierte Security Operations Centers. Auch personell ist HCL hinsichtlich seiner Next-Gen SOC/MDR Services in Deutschland stark aufgestellt. Das Portfolio deckt viele Leistungen und Technologien an.

IBM

IBM ist im Markt mit einem der breitesten Portfolios für IT Security Services vertreten. Die Next-Gen SOC/MDR Services des Anbieters basieren auf der leistungsstarken, hauseigenen Technologie. Das weltweite Netzwerk aus SOCs ermöglicht einen globalen Betrieb.

Infosys

Die Leistungen von **Infosys** im Rahmen der Next-Gen SOC/MDR Services lassen keine Wünsche offen. Darüber hinaus ist Infosys auch personell hinsichtlich dieser Services in Deutschland stark aufgestellt.

Cyberdefense

Orange Cyberdefense ist weltweit mit SOCs vertreten und ermöglicht so einen globalen Betrieb der Cybersecurity-Lösungen. Auch Deutschland zählt zu den Staaten, in denen Orange Cyberdefense Security Operations Centers betreibt.

TCS TATA CONSULTANCY SERVICES

Die Next-Gen SOC/MDR Services von **TCS** ermöglichen den Betrieb sämtlicher Cybersecurity-Technologien, inklusive OT-Sicherheit. Sowohl in absoluter Zahl als auch gemessen an der Anzahl der Kunden unterhält TCS in Deutschland ein großes Team.

InfoGuard SWISS CYBER SECURITY

InfoGuard steigt zum „Rising Star“ unter den Anbietern von Next-Gen SOC/MDR Services auf. Dazu trägt das verstärkte Engagement in Deutschland bei.

Leader

„Mit seinem modularen Angebot und Next-Gen SOC/MDR Services aus Deutschland geht Controlware zielgerichtet auf die Bedürfnisse seiner mittelständischen Kunden ein."

Frank Heuer

Controlware

Übersicht

Controlware ist ein deutscher IT-Dienstleister mit Hauptsitz in Dietzenbach in Hessen, beschäftigt rund 1.000 Mitarbeitende und unterhält ein Vertriebs- und Servicenetz mit 16 Standorten in Deutschland, Österreich und der Schweiz. Neben Strategic und Technical Security Services bietet Controlware auch Managed Security Services an, mit denen Kunden, vom gehobenen Mittelstand bis zu Großunternehmen und großen öffentlichen Kunden, adressiert werden. Die SOC/MDR Services sind Teil der Cyber Defense Services von Controlware.

Stärken

Große Manpower: Speziell auch gemessen an der Anzahl der Kunden unterhält Controlware in Deutschland ein großes Expertenteam für seine Managed Security Services.

Fokus auf Wachstumssegment: Controlware hat hinsichtlich seiner Managed-Security-Services einen starken und klaren Fokus auf das Segment der mittelständischen Unternehmen – eine Zielgruppe mit besonders hohem Wachstumspotenzial.

Delivery aus Deutschland: Controlware betreibt in Deutschland ein dediziertes Security Operations Center. Dies entspricht klar den Erwartungen vieler mittelständischer Kunden, dem wichtigsten Kundensegment von Controlware.

Flexible, kundenorientierte Services: Die Leistungen von Controlware sind kundenorientiert. Der Anbieter offeriert seinen Kunden modulare Managed Security Services, was besonders interessant für Kunden ist, die keine alle Leistungen und Themen abdeckende Lösung benötigen. Dies gilt vor allem für viele mittelständische Unternehmen. Als Systemintegrator ist Controlware zudem in der Lage, mittel- bis langfristige Lösungen für Cybersicherheitsprobleme anzubieten, die über das SOC-Sicherheitsvorfallmanagement hinausgehen, sowie Vorfälle zu entschärfen und die Infrastruktur von Kunden umzugestalten.

Herausforderungen

Zur Erreichung einer noch stärkeren Marktposition könnte es hilfreich sein, die internationale Präsenz selektiv auszubauen, zum Beispiel in der EU und den USA. So könnte Controlware bei Interessenten noch häufiger in die engere Wahl kommen.

Next-Gen SOC/MDR Services – Midmarket

Wer sollte dieses Kapitel lesen

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

Experten auf der Geschäftsseite

gewinnen aus diesem Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht werden können, und werden über praktische Lösungen zur Reduzierung der Komplexität und Effizienzsteigerung informiert.

Cybersecurity-Experten

hilft dieser Bericht die neuen Trends und unmittelbaren Bedrohungen zu verstehen. Er kann bei der strategischen Entscheidungsfindung helfen und gleichzeitig die Produktivität steigern und die Komplexität von Sicherheitsmaßnahmen reduzieren.

Technologieexperten

werden mit diesem Bericht über sich abzeichnende Trends, maßgeschneiderte Sicherheitsplattformen und strategische Ziele informiert und können so der sich verändernden Sicherheitslandschaft Rechnung tragen.

ISG Provider Lens™

Source: ISG RESEARCH

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

Deutschland 2025

In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/ MDR Services** für deutsche Mittelständler, ohne Provider, die nur eigene Produkte betreuen. Insbesondere der Fachkräftemangel bewirkt eine **zunehmende Nachfrage**.

Frank Heuer

Definition

Die in diesem Quadranten bewerteten Anbieter offerieren Services im Zusammenhang mit der kontinuierlichen Überwachung von IT- und OT-Infrastrukturen durch ein Security Operations Center (SOC). Es werden Dienstleister untersucht, die sich nicht ausschließlich auf proprietäre Produkte konzentrieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Reaktion auf und Behebung von Problemen.

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

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

Auswahlkriterien

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

Beobachtungen

Noch stärker als Großunternehmen sind mittelständische Unternehmen in Deutschland 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 sowie MDR Services angewiesen.

Für das Mittelstandssegment sind SOCs in Deutschland aus Gründen des Vertrauens und des Datenschutzes ein Pluspunkt. Auch deutschsprachige Ansprechpartner spielen für diese Kundengruppe eine wichtige Rolle. Viele Mittelständler erwarten von ihren Dienstleistern eine unkomplizierte, schnelle Umsetzung und somit 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.

Der bisherige Rising Star suresecure ist in diesem Jahr zum Leader aufgestiegen. SVA ist der neue Rising Star. Getronics ist neu im Quadranten vertreten. Noch nicht für den Quadranten haben sich NVISO, Skaylink und Vodafone qualifiziert, sie zeigen jedoch vielversprechende Ansätze für eine zukünftige Präsenz in der Anbieterbewertung.

Von den 68 Anbietern, die in dieser Studie dediziert für den deutschen Markt bewertet wurden, konnten sich 22 für diesen Quadranten qualifizieren. Dabei erreichten acht eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

axians

Axians IT Security überzeugt seine mittelständischen Kunden mit auf ihre Bedürfnisse zugeschnittenen, umfangreichen Next-Gen-SOC-/MDR-Dienstleistungen.

BECHTLE

Bechtles tiefes Verständnis für die Anforderungen des Mittelstandes sowie die umfangreichen und anpassungsfähigen Dienstleistungen tragen zum Erfolg im deutschen Markt für Next-Gen-SOC-/MDR-Dienstleistungen bei.

CANCOM

Mit einem weiterentwickelten Angebot an SOC/MDR-Dienstleistungen für den deutschen Mittelstand profiliert sich **CANCOM** als führender Provider.

controlware

Controlware adressiert zielgerecht die Bedürfnisse deutscher mittelständischen Kunden. Dazu tragen die modularen Next-Gen-SOC-/MDR-Dienstleistungen und der SOC-Betrieb in Deutschland bei.

DATAGROUP

Mit hochwertigen Dienstleistungen, die von eigenen Experten und einem starken Partner erbracht werden, erreicht **DATAGROUP** eine führende Position im Markt der Next-Gen SOC/MDR Services für den deutschen Mittelstand.

Die **Deutsche Telekom** festigt ihre eindeutige Führungsposition im mittelständischen Next-Gen-SOC-/ MDR-Markt durch Investitionen in ihr attraktives Angebot und in die Leistungsbereitstellung aus Deutschland.

InfoGuard
SWISS CYBER SECURITY

InfoGuard gelingt der Sprung unter die führenden Anbieter von Next-Gen SOC/MDR Services für den deutschen Mittelstand. Dazu trägt auch die entschlossene Übernahme von Com-Sys bei.

sure[secure]

Der letztjährige Rising Star **suresecure** steigt durch Konzentration auf die dynamisch wachsende Zielgruppe und eine innovative Technologieplattform zum Leader unter den Anbietern von SOC-Services für den deutschen Mittelstand auf.

SVA

Dank eines attraktiven Angebotes und Delivery aus Deutschland ist **SVA** der neue Rising Star unter den Anbietern von Next-Gen SOC/MDR Services für den Mittelstand in Deutschland.

Leader

„Mit seinen modularen Next-Gen-SOC-/ MDR-Dienstleistungen und dem Betrieb in Deutschland adressiert Controlware zielgerecht die Bedürfnisse deutscher mittelständischen Kunden."

Frank Heuer

Controlware

Übersicht

Controlware ist ein deutscher IT-Dienstleister mit Hauptsitz in Dietzenbach in Hessen, beschäftigt rund 1.000 Mitarbeitende und unterhält ein Vertriebs- und Servicenetz mit 16 Standorten in Deutschland, Österreich und der Schweiz. Neben Strategic und Technical Security Services bietet Controlware auch Managed Security Services an, mit denen Kunden, vom gehobenen Mittelstand bis zu Großunternehmen und großen öffentlichen Kunden, adressiert werden. Die SOC/MDR Services sind Teil der Cyber Defense Services von Controlware.

Stärken

Profitieren von wachstumsstarker Zielgruppe: Controlware hat hinsichtlich seiner Managed Security Services einen starken und klaren Fokus auf das Segment der mittelständischen Unternehmen – aufgrund des häufig fehlenden eigenen Know-hows eine Zielgruppe mit besonders hohem Wachstumspotenzial.

Bedarfsgerechte, flexible Dienstleistungen: Die Services von Controlware sind kundenorientiert. Es werden modulare Managed Security Services offeriert, was besonders interessant für Kunden ist, die keine alle Leistungen und Themen abdeckende Lösung benötigen. Dies gilt vor allem für viele mittelständische Unternehmen, die oft auf Kosteneffizienz besonders Wert legen müssen. Als Systemintegrator ist Controlware zudem in der Lage, mittel- bis langfristige Lösungen für Cybersicherheitsprobleme anzubieten, die über das SOC-Sicherheitsvorfallmanagement hinausgehen, sowie Vorfälle zu entschärfen und die Infrastruktur von Kunden zu optimieren.

SOC-Betrieb in Deutschland: Controlware betreibt in Deutschland ein dediziertes Security Operations Center. Dies entspricht klar den Erwartungen vieler mittelständischer Kunden, dem wichtigsten Kundensegment von Controlware.

Ein umfangreiches Team: Speziell auch gemessen an der Anzahl der Kunden unterhält Controlware in Deutschland ein großes Expertenteam für seine Managed Security Services.

Herausforderungen

Die internationale Präsenz selektiv auszubauen, zum Beispiel in der EU und den USA, kann sich für eine noch stärkere Marktposition lohnen. Auch mittelständische Unternehmen sind international zunehmend präsent; so könnte Controlware noch häufiger in die engere Wahl bei entsprechenden Interessenten kommen.

Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2025 – Cybersecurity – Services and Solutions" analysiert die entsprechenden Softwareanbieter und 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,
Bhuvaneshwari Mohan (Global-IAM),
Gowtham Sampath (Global-XDR) und
Yash Jethani (Global - SSE)

Editoren:
Maria Müller-de Haen und Indrani Saha

Forschungsanalysten:
Sandya Kattimani und Monika K

Datenanalysten:
Rajesh Chillappagari und Laxmi Kadve

Beratende Berater:
Tim Merscheid und Marco Ezzy

Projektleiter:
Shreemadhu Rai B

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

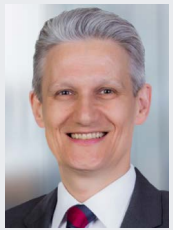
Die in dieser Studie vorgestellten Marktforschungs- und Analysedaten stammen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. 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 2025. ISG ist sich darüber im Klaren, dass zwischenzeitlich eventuell Fusionen und Übernahmen stattgefunden haben; diese Veränderungen werden in diesem Bericht allerdings nicht berücksichtigt.

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

Dabei wurde die Studie in folgende Schritte gegliedert:

1. Definition des Marktes für Cybersecurity – Services and Solutions
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 (Global - IAM)

Bhuvaneshwari Mohan
Autor und Forschungsanalyst

Bhuvaneshwari ist als Senior Research-Analystin für ISG tätig; in dieser Rolle unterstützt sie und ist Co-Autorin von Provider Lens™ Studien zu den Themen Digital Business Enablement, Supply Chain, ESG Services und Cybersecurity. Sie bringt die notwendigen Daten und Marktanalysen in den Researchprozess ein, entwickelt Inhalte aus Unternehmensperspektive und verfasst Global Summary Reports. Sie verfügt über acht Jahre praktische Erfahrung und hat fundierte maßgeschneiderte Berichte für diverse Branchen erstellt.

Sie ist eine vielseitige Research-Expertin mit Erfahrung in den Bereichen Wettbewerbs-Benchmarking Social-Media-Analysen und Talent Intelligence. Vor ihrer Tätigkeit bei ISG sammelte sie Research-Erfahrung in Sales-Enablement-Positionen bei IT- und Digital-Dienstleistern und arbeitete meist in Sales Enablement Teams.

Autor (Global - XDR)

Gowtham Sampath

Assistant Director und Principal Analyst, ISG Provider Lens™

Gowtham Sampath ist Principal Analyst bei ISG Research und verantwortlich für die Erstellung von ISG Provider Lens™ Quadrantenberichten für die Bereiche Banking Technology/ Platforms, Digital Banking Services, Cybersecurity und Analytics Solutions & Services. Auf Basis seiner 15-jährigen Marktforschungserfahrung arbeitet Gowtham an der Analyse von und Überbrückung der Kluft zwischen Datenanalyseanbietern und Unternehmen und befasst sich mit Marktchancen und Best Practices.

In seiner Funktion arbeitet er auch mit Beratern zusammen, um Ad-hoc-Research für Unternehmenskunden im IT-Dienstleistungssektor branchenübergreifend durchzuführen. Darüber hinaus verfasst er Thought Leadership Research, Whitepapers und Artikel über neue Technologien im Bankensektor in den Bereichen Automatisierung, DX und UX sowie über die Auswirkungen der Datenanalyse in verschiedenen Branchen.

Autor (Global - SSE)

Yash Jethani

Senior Manager und Principal Analyst

Yash verfügt über mehr als 14 Jahre Berufserfahrung , vor allem in den Bereichen Technologie, Medien und Telekommunikation (TMT). Er hat zu Thought Leadership, Markt- und Wettbewerbsforschung, Beratung, Geschäftsentwicklung und Due Diligence sowie Account Management beigetragen, das die Funktionen Corporate Marketing, Risiko, Strategie und Vertrieb umfasst. Vor seiner Tätigkeit bei ISG arbeitete Yash bei KPMG in Indien und unterstützte die nationale TMT-Praxis in den Bereichen Beratung, Thought Leadership und strategische Aktivitäten. Während seiner Zeit bei IDC war er verantwortlich für die Bereitstellung kundenspezifischer sowie als auch syndizierter Forschung für Telco & IoT Asien Pazifik Kunden. Er war auch bei CGI und TCS tätig und unterstützte deren Marketinginitiativen für Unternehmen und Kunden mit Schwerpunkt auf next-gen IT delivery within Telco/ Comms verticals. Derzeit trägt er zu den globalen Forschungsstudien von ISG Provider Lens als leitender Analyst für softwaredefinierte Netzwerke, verwaltete Netzwerkdienste sowie Telekommunikations- und Medienverwaltungsdienste Studien in verschiedenen Regionen bei. Yash hat einen PGDM-Abschluss in Telekommunikation und IT sowie einen Ingenieurabschluss in Computer. Er ist außerdem TM Forum-zertifiziert und leistet einen aktiven Beitrag als Mitglied des Bangalore Software Process Improvement Network, einer gemeinnützigen Organisation.

Forschungsanalystin

Monica K
Assistant Manager und Lead Research Specialist

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

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

Forschungsanalystin

Sandya Kattimani
Senior Forschungsanalyst

Sandya Kattimani ist als Senior Research-Analystin für ISG tätig; in dieser Rolle unterstützt sie und ist Co-Autorin von ISG Provider Lens™ Studien zu den Themen Contact Center, Life Sciences und Mainframes. Sandya verfügt über mehr als sechs Jahre Erfahrung mit Technologieresearch und war in ihrer vorherigen Position für die Durchführung von Primär- und Sekundärrecherchen zuständig. Ihre Fachgebiete sind Competitive Intelligence, Customer Journey Analysen, Battle Cards, Marktanalysen und die digitale Transformation.

Zu ihren Aufgaben gehört das Verfassen von Enterprise Content und Global Summary Reports mit regionalen und globalen Markttrends und Erkenntnissen. Zuvor war sie als Analystin für Technologieforschung verantwortlich für Projekte, die detailliertes Technologie-Scouting, Wettbewerbsanalysen, Unternehmensanalysen, Technologiestudien und andere Ad-hoc-Researchaufträge umfassten.

Sponsor der Studie

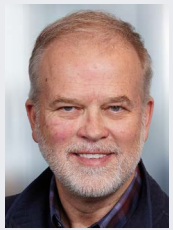
Heiko Henkes

Director und Principal Analyst, Global IPL Content Lead

Heiko Henkes ist Director und Principal Analyst bei ISG und leitet das globale ISG Provider Lens™ (IPL)-Programm für alle IT-Outsourcing (ITO)-Studien; zudem nimmt er im Rahmen von globalen IPL-Studien eine Schlüsselrolle als strategischer Programmmanager und Vordenker für IPL Lead Analysts ein.

Heiko Henkes leitet das „Star of Excellence" Programm, die globale Kundenerfahrungsinitiative von ISG, und steuert das Programmdesign und dessen Integration mit dem IPL-Programm und der ISG Sourcing Practice. Er begleitet Unternehmen durch IT-basierte Geschäftsmodell-Transformationen und nutzt dabei sein tiefes Verständnis für kontinuierliche Transformation, IT-Kompetenzen, nachhaltige Geschäftsstrategien und Change Management in einem auf Cloud-KI basierenden Geschäftsumfeld. Heiko Henkes ist ein bekannter Keynote-Speaker zum Thema digitale Innovation und gibt Einblicke in die Nutzung von Technologie für das Wachstum und die Transformation von Unternehmen.

Produktverantwortlicher



Jan Erik Aase

Partner und globaler Leiter – ISG Provider Lens™

Herr Aase verfügt über umfangreiche Erfahrung bezüglich Implementierung und Research im Bereich Service- Integration und Management sowohl von IT- als auch von Geschäftsprozessen mit. Mit mehr als 35 Jahren Erfahrung ist er hochqualifiziert darin, Trends und Methoden der Vendor Governance zu analysieren, Ineffizienzen in aktuellen Prozessen zu identifizieren und als Berater tätig zu sein. Jan Erik hat Erfahrung auf allen vier Seiten des Sourcing- und Vendor-Governance- Lebenszyklus – als Kunde, als Branchenanalyst, als Dienstleister und als Berater. Als Research Director, Principal Analyst und Global Leader des ISG Provider Lens™ Programms ist er sehr gut in der Lage, den aktuellen Stand der Branche zu beurteilen und darüber zu berichten sowie Empfehlungen für Unternehmen und Service-Provider-Kunden auszusprechen.

ISG Provider Lens™

Die ISG Provider Lens™ Quadranten-Reports bieten Bewertungen von Dienstleistern und kombinieren als einzige Studien dieser Art datengestützte Forschung und Marktanalysen mit praktischen Erfahrungen und Beobachtungen, gestützt auf das globale 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 (Nasdaq: III) ist ein globales, KI-orientiertes Technologieforschungs- und Beratungsunternehmen. Als vertrauenswürdiger Partner von mehr als 900 Kunden, darunter 75 der 100 weltweit führenden Unternehmen, ist ISG seit langem führend in der Beschaffung von Technologie- und Business-Services und nimmt inzwischen eine Spitzenstellung bei der KI-Nutzung ein; damit kann Organisationen zu operativer Exzellenz und schnellerem Wachstum verholfen werden.

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

Weitere Informationen unter isg-one.com.

ISG Provider Lens™

JULI 2025

BERICHT: CYBERSECURITY – SERVICES AND SOLUTIONS