ISG Provider Lens™

Cybersecurity – Services and Solutions

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

Customized report courtesy of:

QUADRANT REPORT | JULI 2025 | SCHWEIZ, GLOBAL

Inhaltsverzeichnis

Autor des Berichts: Frank Heuer

„Swissness" und disruptive Technologien prägen den Schweizer Cybersecurity-Markt

Die Gefährdung Schweizer Unternehmen nimmt durch immer häufigere, raffiniertere, komplexere und wandlungsfähigere Cyberattacken zu. Der Mangel an qualifizierten Cybersecurity-Fachleuten verschärft die Situation und begünstigt zugleich die Nachfrage nach externen Dienstleistungen. Neue Technologien fördern Cyberbedrohungen, bieten andererseits aber auch neue Geschäftschancen für Dienstleister. Serviceanbieter, die zusätzlich mit „Swissness" punkten können und sich auf die Anforderungen verschiedener Zielgruppen verstehen, werden bevorzugt.

In Bezug auf Cybersecurity sind die Verantwortlichen in Schweizer Unternehmen aktuell vor verschiedene Herausforderungen gestellt. Die verstärkten Cyberbedrohungen und selbstverständlich auch der langfristige Trend hin zur Digitalisierung haben in der Schweiz zu vergrösserten Angriffsflächen für Cyberattacken geführt, die entsprechender Gegenmassnahmen bedürfen.

Im Zuge der Digitalisierung werden Geschäftsprozesse zunehmend in die IT verlagert. Zudem wird geistiges Unternehmenseigentum immer mehr digital dargestellt. Mit der steigenden Notwendigkeit, IT- und Kommunikationssysteme zu schützen, hat sich IT-Sicherheit zur Unternehmenssicherheit gewandelt. Durch die verbreitete Home-Office-Nutzung in der Schweiz – und die dadurch bedingte externe Anbindung der Mitarbeitenden – sind IT-Systeme leichter angreifbar.

Über die Digitalisierung und die vermehrte Remote-Arbeit hinaus hat die zunehmende Bereitstellung von Ressourcen aus der Cloud zu einer grösseren Angreifbarkeit der IT-Systeme und infolgedessen zu einer zunehmenden Relevanz des Zero-Trust-Ansatzes geführt. Perimetersicherheit reicht nicht mehr aus. Der Grundsatz „never trust, always verify" (nie vertrauen, immer überprüfen) bedeutet unter anderem gegenseitige Authentifizierung und kontinuierliche Überwachung des Netzwerks.

Die grosse Dynamik der **Cyberbedrohungen** fördert die Nachfrage nach externen Services.

Zusammenfassung

In der jüngsten Vergangenheit waren wieder einige spektakuläre Cyberattacken zu verzeichnen – manifeste Hinweise darauf, dass Cyberkriminelle in immer kürzeren Abständen neue, raffiniertere und komplexere Methoden realisieren, um die Cyberverteidigungssysteme von Schweizer Unternehmen und Behörden zu überwinden. Aber auch nicht so prominente Angriffe, etwa durch Ransomware, machen immer mehr Unternehmen zu schaffen. Entsprechend müssen die Cybersecurity-Massnahmen lückenlos auf dem neuesten Stand sein. Damit sind Schweizer Unternehmen und Behörden nicht zuletzt durch den Cybersecurity-Fachkräftemangel immer mehr überfordert. Infolgedessen beauftragen IT-Verantwortliche immer öfter externe Dienstleistungen, zum Beispiel über Security Operations Centers. Diese Provider sowie auch viele IT-Security-Produktanbieter setzen, um selbst mit den Bedrohungen mithalten zu können, verstärkt auf proaktive statt reaktive Methoden, die zum Beispiel auf künstlicher Intelligenz basieren.

Über den Eigenschutz des Unternehmens hinaus zwingen auch gesetzliche Regelungen Schweizer Unternehmen dazu, stärkere Sicherheitsmassnahmen umzusetzen, um Cyberattacken vorzubeugen. Das betrifft besonders den Datenschutz, der in der Schweiz höchste Priorität hat. Das Vermögen der hier ansässigen Grossbanken ist stark mit Daten verknüpft. Zudem besteht in der Schweiz auch generell ein grösseres Vertrauen in die Ressourcen im eigenen Land. Diese Haltung wurde in den letzten Jahren durch die Infragestellung des Datenschutzabkommens mit den USA weiter gestärkt. In der Folge stossen Anbieter von IT-Produkten und IT-Dienstleistungen, die ihr Angebot in der Schweiz erstellen (die so genannte „Swissness"), auf ein grösseres Interesse Dies gilt insbesondere für den Betrieb von Lösungen, z.B. im Hinblick auf Cloud-Lösungen und Security Operations Centers. Gerade mittelständische Unternehmen legen grossen Wert auf Swissness, und sie haben auch besonders mit gesetzlichen (Datenschutz-) Anforderungen zu kämpfen.

Die mittelgrossen Unternehmen in der Schweiz sind ein interessantes Marktsegment für Cybersecurity-Anbieter. Ihre Cybersecurity-Systeme sind insgesamt betrachtet weniger ausgereift als die von Grossunternehmen, sie sind aber durch die oben beschriebenen Faktoren zu Nachrüstungen gezwungen. Infolgedessen haben sie einen hohen Nachholbedarf und verzeichnen dementsprechend eine überdurchschnittlich stark wachsende Nachfrage nach Cybersecurity-Lösungen. Noch vorteilhafter für die Anbieter ist eine ausgewogene Kundenstruktur aus Grossunternehmen und mittelständischen Firmen, um auch von den grossen Budgets der Large Accounts zu profitieren.

Der Schweizer Mittelstand mit seiner überdurchschnittlich wachsenden Nachfrage ist ein zunehmend attraktives Marktsegment, 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.

Trotz der grossen Bedeutung der IT-Sicherheit kämpfen IT-Verantwortliche wieder vermehrt mit der Aufgabe, Investitionen in Cybersicherheit gegenüber Stakeholdern des Unternehmens zu legitimieren, besonders gegenüber dem Finanzmanager. Im Gegensatz zu anderen IT-Projekten ist es nicht immer möglich, die Rentabilität von Cybersecurity-Investitionen nachzuweisen; auch Bedrohungsrisiken zu quantifizieren ist nicht einfach. Es ist allerdings festzustellen, dass auch Führungskräfte zunehmend erkennen, dass Cyberattacken zu massiven – unter Umständen existenziellen – finanziellen und Imageschäden führen können. In der Folge gewinnt die Sicherheit der IT in Schweizer Unternehmen an Bedeutung, und die Führungsetage wird verstärkt in das Cyberrisikomanagement eingebunden.

Nach wie vor wird die Erfahrung gemacht, dass die Ursache für Cybersecurity-Zwischenfälle oft

nicht (allein) auf der technischen Seite liegt. Zahlreiche Angriffe werden durch unbedachtes Verhalten von Anwendern begünstigt, wie z.B. bei Trojaner- und Phishing-Angriffen. Neben einem zeitgemässen IT-Sicherheitsequipment spielen daher Beratung und Nutzerschulungen weiterhin eine wichtige Rolle.

Beratung ist auch vermehrt hinsichtlich aktueller und neuer technischer Bedrohungen gefragt. Hinsichtlich KI-basierter Bedrohungen und Lösungen nimmt der Beratungsbedarf zu; dies gilt besonders für quantum-basierende Angriffe. Sie 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 Beratungsangebote werden in der Schweiz vor allem von Versicherungen und Banken in Anspruch genommen, da ihre Vermögenswerte aus virtuellen Assets bestehen und sie auf die neuen Bedrohungen frühzeitig vorbereitet sein wollen.

Strategic Security Services

Die Lage hinsichtlich Cybersecurity-Gefährdungen in der Schweiz wird weiterhin bedrohlicher. Hiervon sind schon lange nicht mehr nur die bekannten grossen Unternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelgrosse Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin.

Unter dem besonders starken Fachkräftemangel hinsichtlich IT-Security haben gerade mittelgrosse Unternehmen zu leiden. Der Mittelstand ist damit ein überdurchschnittlich wachsendes – und entsprechend zunehmend attraktives – Marktsegment.

Technical Security Services

Immer intensivere, raffiniertere, komplexere und ständig neue Cyberattacken gefährden Schweizer Unternehmen. Erschwert wird diese Situation noch durch den Mangel an Cybersecurity-Experten. Daher sind die Unternehmen immer mehr auf externe Dienstleister angewiesen, um ihre IT-Security-Systeme auf dem laufenden Stand zu halten.

Cybersecurity-Projekte sind häufig vielfältig und anspruchsvoll angelegt. Daher sind hier insbesondere Dienstleister im Vorteil, die ein breites Leistungsspektrum an Technical Security Services aus einer Hand bieten können.

Managed Security Services – SOC

In der Schweiz wächst die Nachfrage nach Managed Detection & Response (MDR) Services und Diensten, die von Security Operations Centers (SOCs) erbracht werden, stark an. Dieses Wachstum wird durch immer häufigere, komplexere und wandlungsfähigere Cyberattacken gefördert. Darüber hinaus rücken die Knappheit an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen SOC- und MDR-Dienstleistungen in den Fokus Schweizer Unternehmen.

Grosse wie speziell auch mittelständische Kunden wissen SOCs mit Schweizer Standort aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen – speziell beim Betrieb und der Bereitstellung von SOC Services zählt „Swissness" ganz besonders. Für beide Marktsegmente sind darüber hinaus auch End-to-End Security Services, integrierte Lösungen aus IT- und zugehörigen Security-Lösungen sowie eine hohe Innovationskraft wichtig, um im Wettlauf mit den Cyberkriminellen stets einen Vorsprung zu haben.

Managed Security Services Provider setzen vermehrt künstliche Intelligenz und Automatisierung ein, um der zunehmend komplexen und vielfältigen Cyberbedrohungen Herr zu werden. Als ideal erweist sich eine Kombination der maschinellen Effizienz mit umfassender menschlicher Expertise.

Zusammenfassung

Anbieter mit „Swissness“ und Fachwissen in den Bereichen künstliche Intelligenz und Post-Quantum-Verschlüsselung sind bestens positioniert, um die hohen Standards der Schweiz im Bereich Cybersicherheit zu erfüllen. Vorteile haben dabei Dienstleister, die eine ausgewogene Zielgruppe adressieren und 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 Unternehmensbedürfnisse, 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

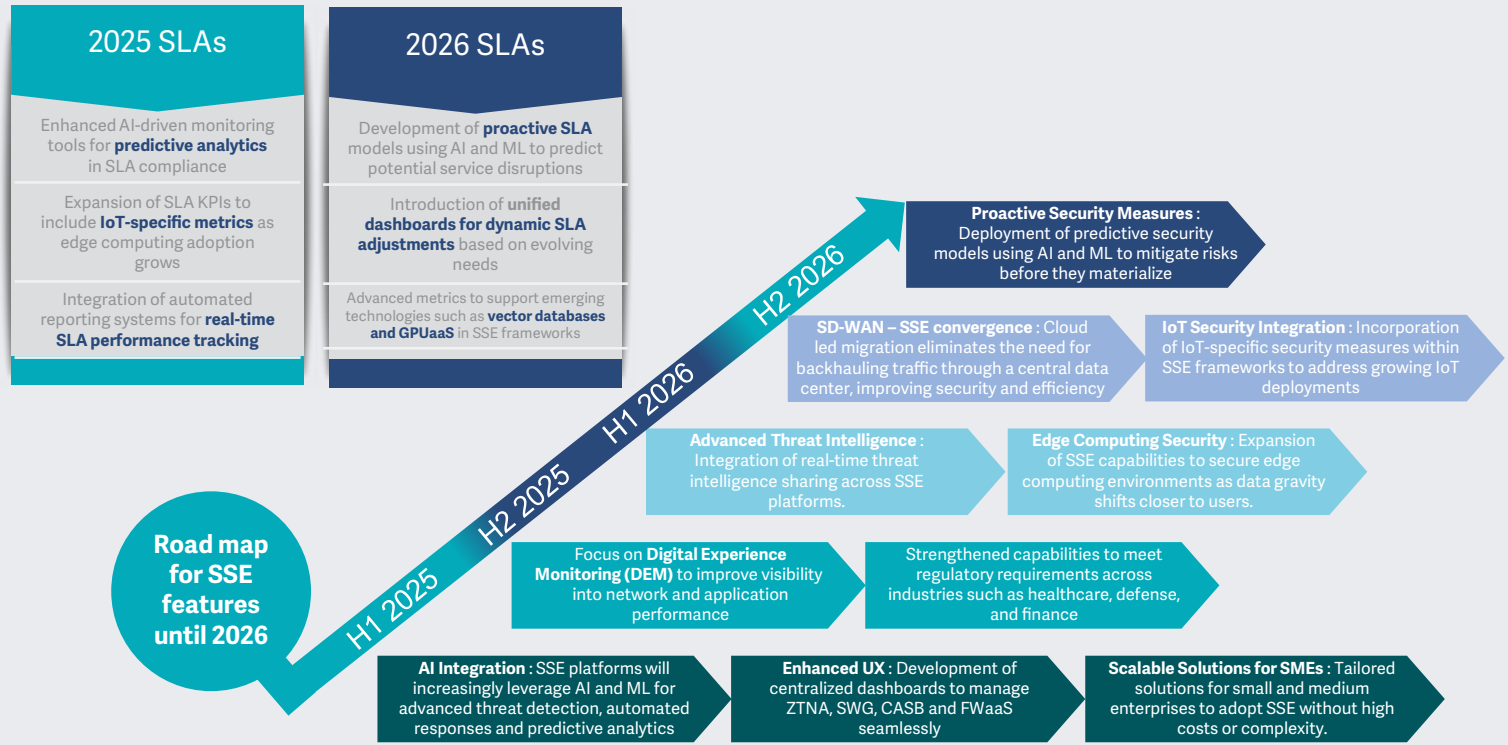
Eine fundierte Cybersicherheitsstrategie integriert diese Elemente in ein Zero-Trust Framework und schafft so mehrere Verifizierungsebenen, die vor komplexen Bedrohungen schützen.

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 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Accenture	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Not In
All for One Group	Not In	Not In	Not In	Contender	Contender	Not In	Not In	Not In
Aryaka	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Atos	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Not In
Aveniq	Not In	Not In	Not In	Contender	Product Challenger	Leader	Not In	Leader
Axians	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Product Challenger
Bechtle	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger	Product Challenger	Product Challenger
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

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Bitdefender	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
BlackBerry (Arctic Wolf)	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Product Challenger	Leader	Not In
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Product Challenger	Contender	Contender	Contender
Check Point Software	Not In	Product Challenger	Leader	Not In	Not In	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 3 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	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	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Product Challenger	Not In
Deloitte	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Product Challenger	Not In
Deutsche Telekom	Not In	Not In	Not In	Leader	Product Challenger	Leader	Leader	Leader
DXC Technology	Not In	Not In	Not In	Leader	Contender	Contender	Contender	Not In
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 4 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	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	Leader	Not In	Not In	Not In
Fischer Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Fortinet	Market Challenger	Leader	Leader	Not In	Not In	Not In	Not In	Not In
Fortra	Market Challenger	Not In	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

Anbieterpositionierung

Seite 5 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Gopher Security	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Product Challenger
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Leader	Not In
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
InfoGuard	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader
Infosys	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader	Not In
Intrinsec	Not In	Not In	Not In	Contender	Contender	Contender	Not In	Contender

Anbieterpositionierung

Seite 6 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
iSPIN	Not In	Not In	Not In	Leader	Product Challenger	Leader	Product Challenger	Leader
JumpCloud	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Leader	Not In	Not In	Not In
Kudelski Security	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger	Leader
Kyndryl	Not In	Not In	Not In	Product Challenger	Product Challenger	Contender	Market Challenger	Not In
LMNTRIX	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Lookout	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger

Anbieterpositionierung

Seite 7 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
ManageEngine	Leader	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Menlo Security	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In
MTF	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Contender
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Product Challenger	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	Contender	Not In	Not In	Market Challenger	Market Challenger	Rising Star ★

Anbieterpositionierung

Seite 8 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
OpenText	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Product Challenger	Rising Star ★	Leader	Leader	Not In
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Rapid7	Not In	Product Challenger	Not In	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
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 9 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Seqrite	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Sequretek	Contender	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
SonicWall (Banyan Security)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Market Challenger	Market Challenger	Product Challenger	Product Challenger	Product Challenger

Anbieterpositionierung

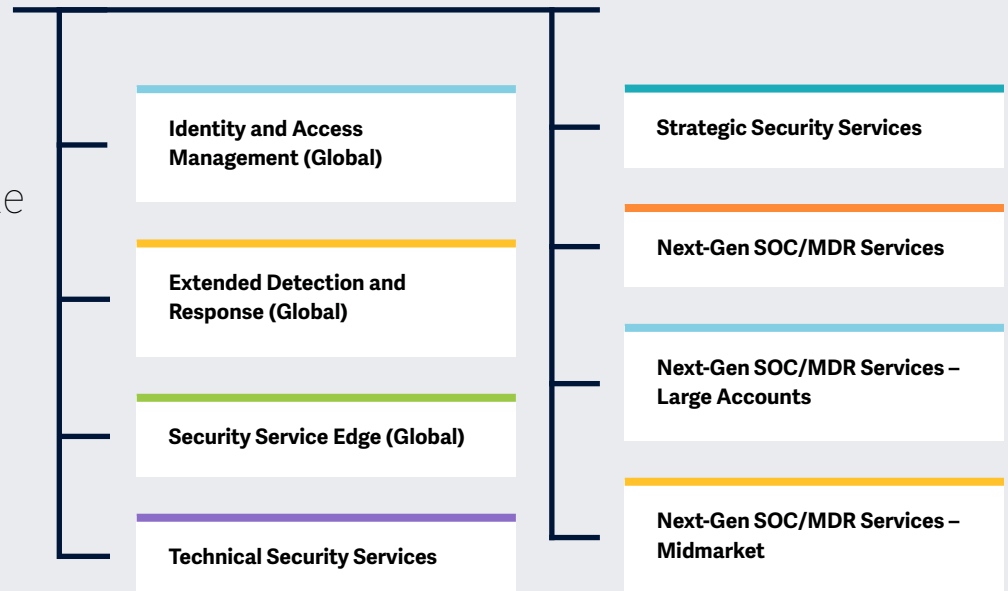
	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Swisscom	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger	Product Challenger
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
terreActive	Not In	Not In	Not In	Not In	Not In	Contender	Contender	Contender
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
UMB	Not In	Not In	Not In	Rising Star ★	Leader	Leader	Rising Star ★	Leader

Anbieterpositionierung

Seite 11 von 11

	Identity and Access Management (Global)	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 – Large Accounts	Next-Gen SOC/ MDR Services – Midmarket
Unisys	Not In	Not In	Not In	Market Challenger	Contender	Market Challenger	Market Challenger	Not In
United Security Providers	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Leader
Verizon Business	Not In	Not In	Not In	Not In	Contender	Product Challenger	Product Challenger	Not In
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Leader	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Leader	Leader	Leader	Not In
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In

Abgedeckte Schwerpunktbereiche der Studie „Cybersecurity – Services & 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™ Quadrant Report behandelt die folgenden acht wichtigen Themen für Dienstleistungen/Lösungen: Identity and Access Management (Global), 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 – Large Accounts, 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 **Schweiz** 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

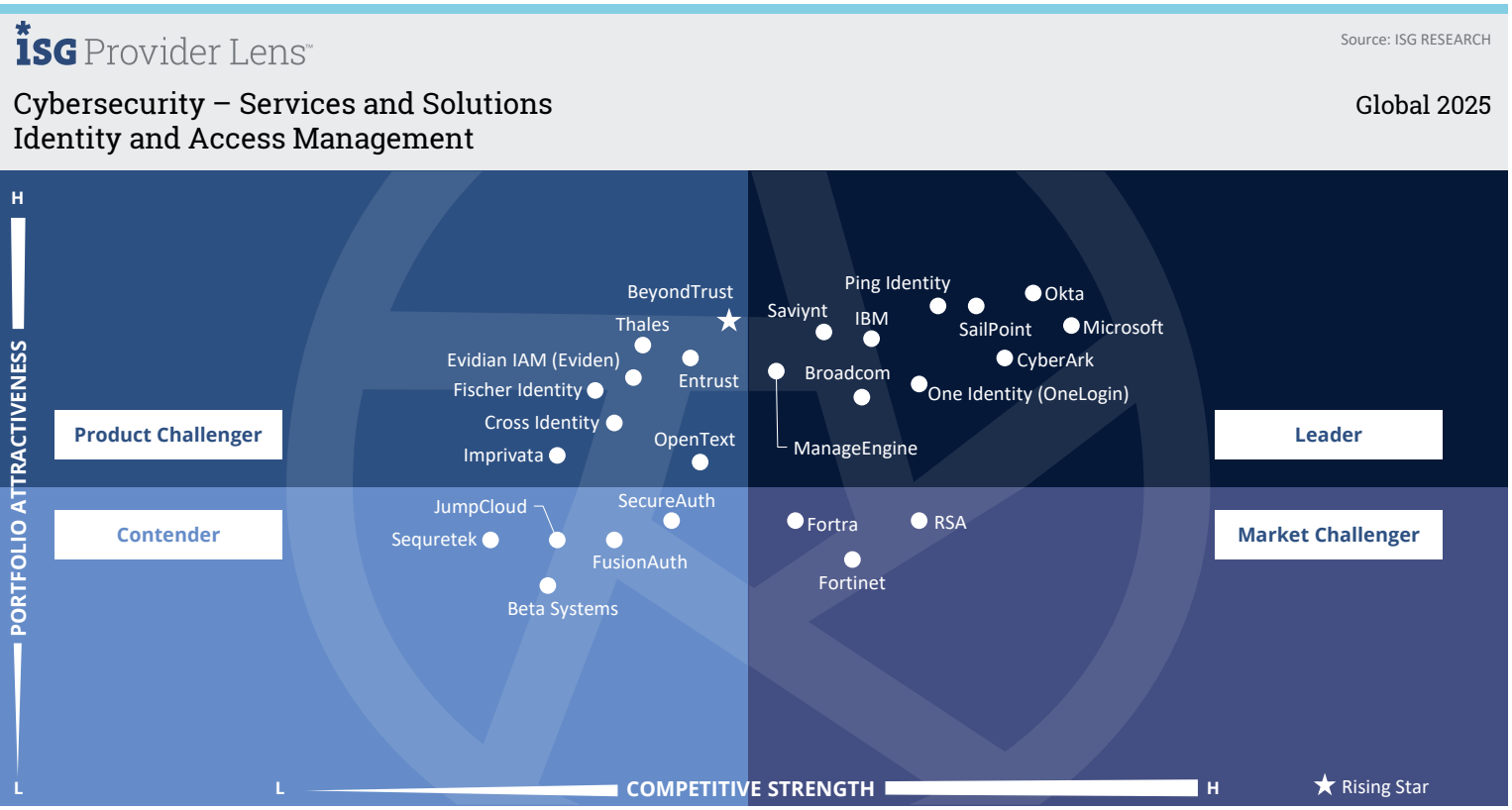
gewinnen aus diesem Bericht ein besseres Verständnis der Integrationsleistungen der Anbieter, die anhand fortschrittlicher Technologien zur Transformation von Altsystemen die Auswirkungen von Bedrohungen verringern.

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

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 am 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 (OneLogin) 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.

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

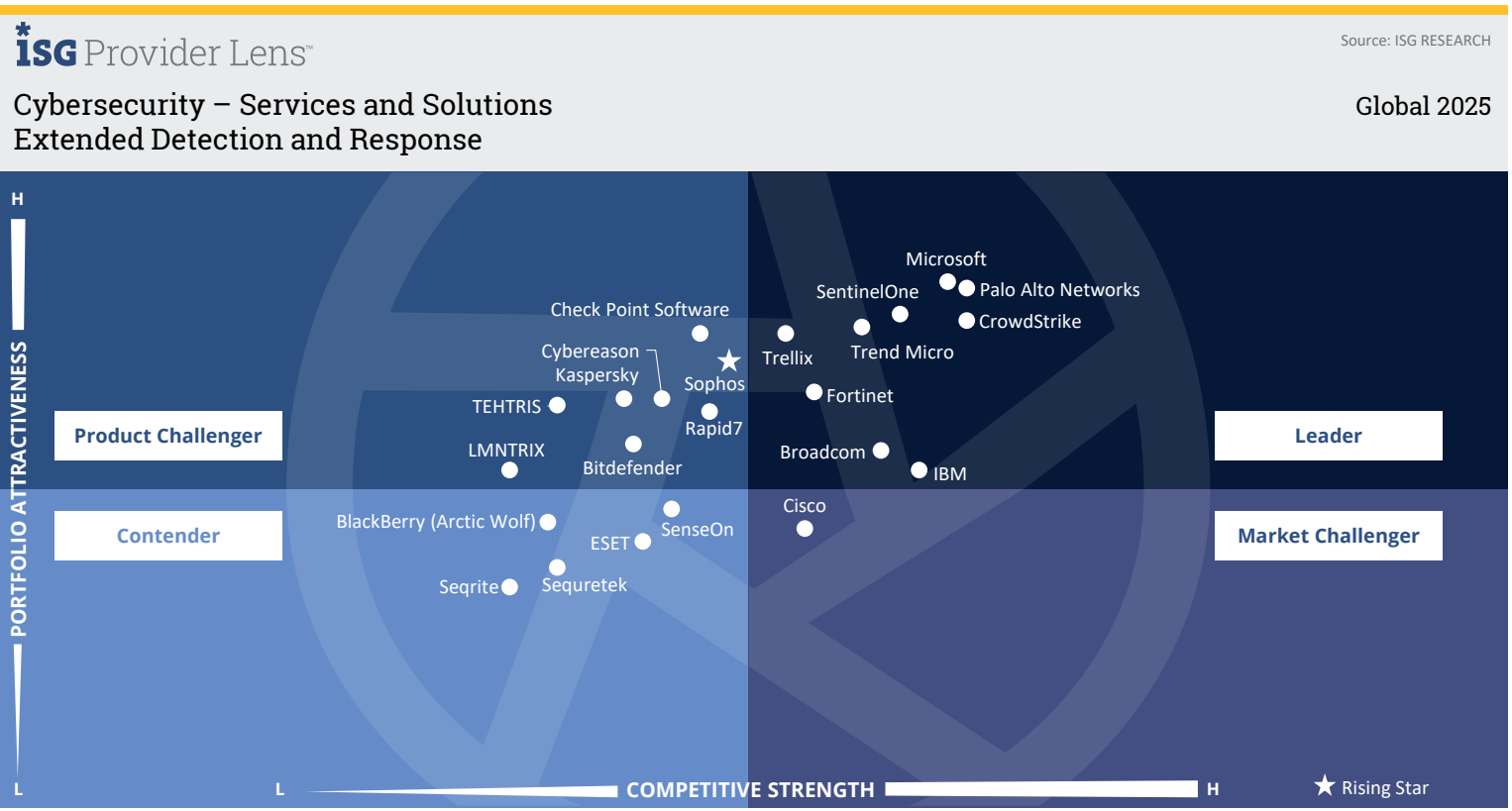
gewinnen aus diesem Bericht einen umfassenderen Überblick über Sicherheitstrends und dahingehend, wie sich die Leistungen der Anbieter zur Entwicklung von robusten Sicherheitsstrategien unterscheiden.

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

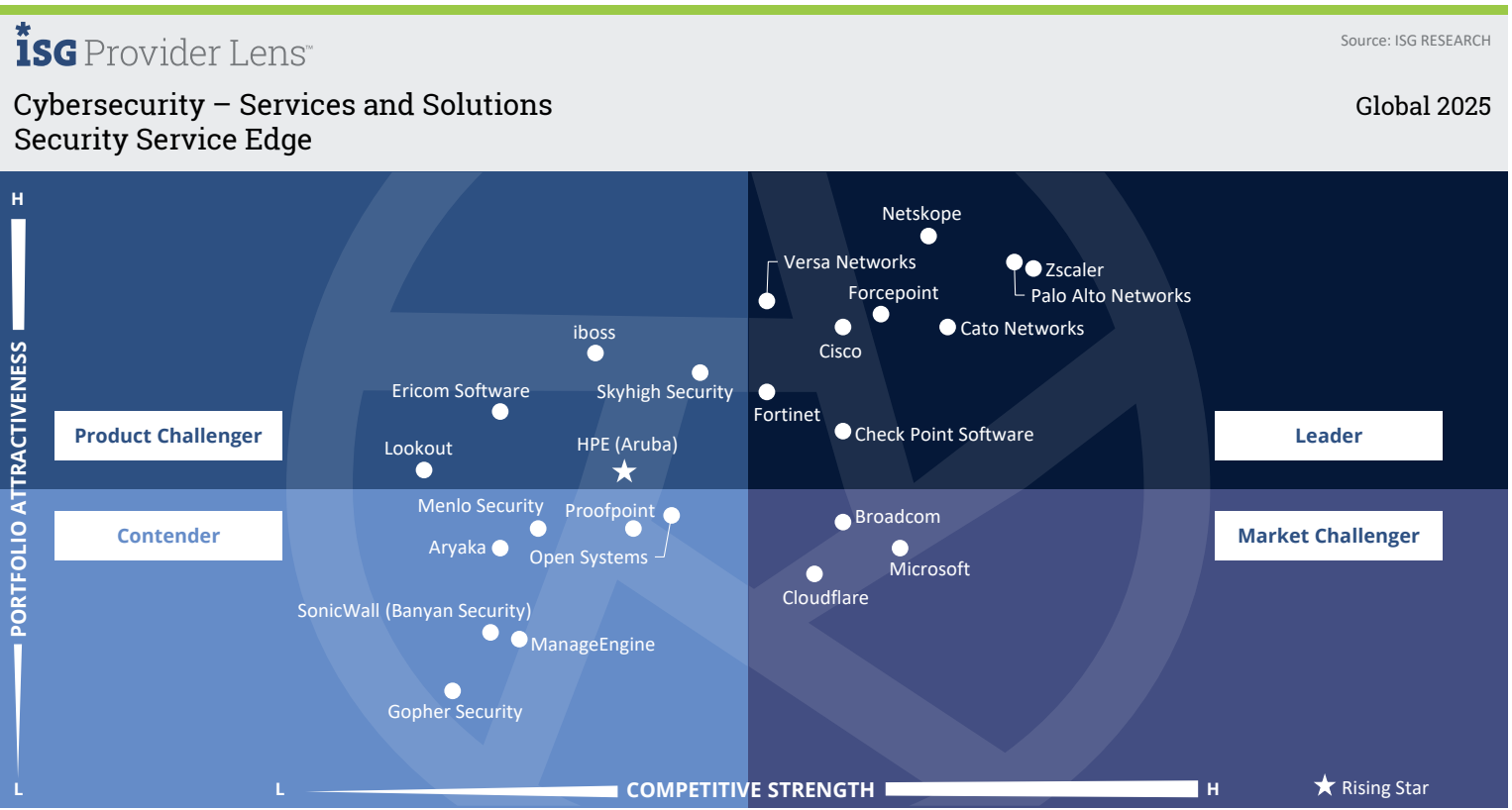
sollten diesen Bericht lesen, um zu verstehen, wie SSE-Anbieter Unternehmen dabei helfen, die Herausforderungen zu meistern, die sich aus der Datengesetzgebung ergeben, und zwar durch verbesserte Richtlinienkontrolle und Berichterstattung.

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.

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.

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.

Technical Security Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Technical Security Services (TSS)** in der **Schweiz** 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

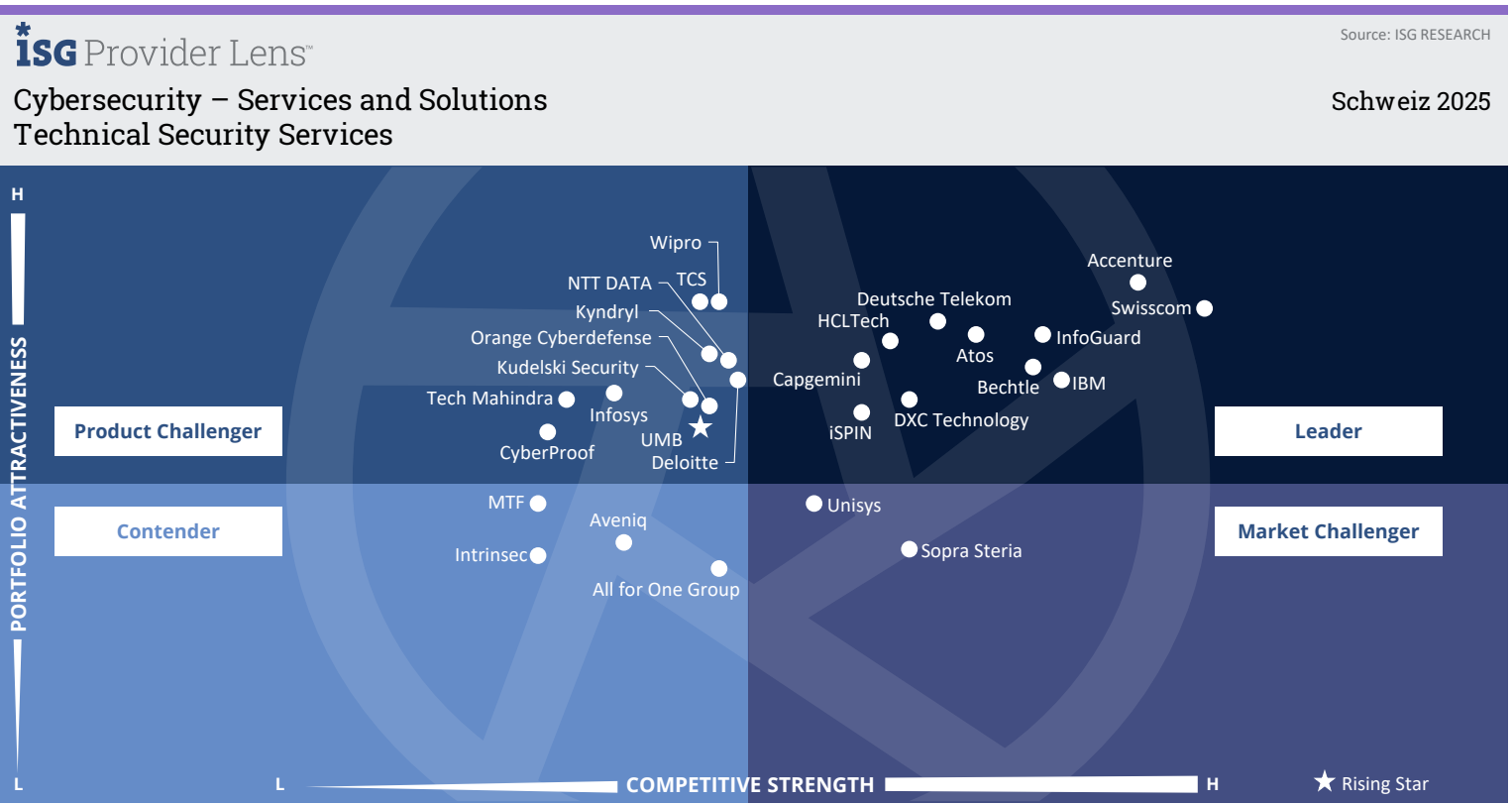
gewinnen aus diesem Bericht ein besseres Verständnis der Integrationsleistungen der Anbieter, die die Auswirkungen von Bedrohungen im Zuge der Modernisierung von Altsystemen und des Einsatzes fortschrittlicher Technologien verringern können.

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 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 der Schweiz, 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

Immer intensivere, raffiniertere, komplexere und ständig neue Cyberattacken gefährden Schweizer Unternehmen. Erschwert wird diese Situation noch durch den Mangel an Cybersecurity-Experten. Daher sind die Unternehmen immer mehr auf externe Dienstleister angewiesen. Günstige Voraussetzungen bringen dabei Provider mit, die neben ausgeprägten technischen Kompetenzen auch die Anforderungen verschiedener Zielgruppen adressieren.

Mittelständische Unternehmen in der Schweiz haben u.a. aufgrund des IT-Fachkräftemangels besonderen Nachholbedarf und nehmen zunehmend externe Dienstleister in Anspruch. Dabei sind Anbieter mit lokaler Präsenz, die kurze Wege und unkomplizierte, schnelle Unterstützung bieten, im Vorteil.

Für Erfolg im anspruchsvollen Grosskundenmarkt müssen Anbieter grosse, auch internationale Erfahrung und Teams präsentieren können.

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

Cybersecurity-Projekte sind häufig anspruchsvoll, vielfältig und zunehmend unter Einbeziehung von KI angelegt. Daher sind Provider im Vorteil, die umfangreiche technische IT-Security-Services aus einer Hand bieten und zahlreiche Technologien, z.B. auch OT Security, abdecken. Zudem profitieren Dienstleister von Kooperationen mit renommierten Technologieanbietern.

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

Der Schweizer Dienstleister UMB ist der neue Rising Star in diesem Quadranten.

Von den 38 Anbietern, die in dieser Studie dediziert in der Schweiz bewertet wurden, konnten sich 28 für diesen Quadranten qualifizieren. Dabei erreichten 11 eine Position als Leader, ein Anbieter wurde als Rising Star identifiziert.

accenture

Mit seinem innovativen, umfassenden Leistungsangebot für technische Cybersecurity Services ermöglicht **Accenture** End-to-End-Sicherheit für die digitale Transformation von Schweizer Unternehmen.

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.

BECHTLE

Bechtle ist in der Schweiz mit zahlreichen Standorten vertreten. Bechtle ist ein profilierter Anbieter von Technical Security Services für das dynamisch wachsende Marktsegment der mittelständischen Unternehmen.

Capgemini

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

Umfangreiche End-to-End Services und die überzeugende Bewältigung von Sicherheitsanforderungen anspruchsvoller Umgebungen machen die **Deutsche Telekom** zu einem Leader im Schweizer Markt für technische Cybersecurity Services.

DXC TECHNOLOGY

DXCs Portfolio beinhaltet integrierte Lösungen aus Cybersecurity und verbundener IT-Technologie. Die globale Präsenz und die globalen Ressourcen sind umfangreich. Trotz der grossen Manpower entwickelt DXC auch die Themen Automatisierung und Blueprints weiter.

HCLTech

HCLTech kann zahlreiche renommierte Technologieanbieter als Partner vorweisen und offeriert eine grosses und tiefes Technical Security Services Portfolio mit einem umfangreichen Spektrum an Services, das zahlreiche Security-Themen einbezieht.

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

Ein umfangreiches, zielgerichtetes Portfolio und ein überzeugendes Preismodell tragen zur Leader-Position von **InfoGuard** im Schweizer Markt für Technical Security Services bei.

iSPIN ist nicht nur ein leistungsfähiger Dienstleister für Technical Security Services, sondern auch in der Beratung für Cybersecurity aktiv und auf das wichtige Thema Netzwerksicherheit spezialisiert.

Im Schweizer Markt für Technical Security Services überzeugt die **Swisscom** als führender Anbieter mit Security-Lösungen, die auf umfassenden Kompetenzen und starken Technologiepartnerschaften beruhen.

UMB

Aufgrund seines attraktiven Angebots wurde **UMB** zum Rising Star im Segment der Technical Security Services in der Schweiz gekürt.

Leader

„Die überzeugende Bewältigung von Sicherheitsanforderungen anspruchsvoller Umgebungen sowie umfangreiche End-to-End Services machen die Deutsche Telekom zu einem Leader im Schweizer Markt für technische Cybersecurity Services."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt 198.194 Mitarbeitende in mehr als 50 Ländern. Im GJ24 erwirtschaftete das Unternehmen einen Umsatz von 115,8 Mrd. €. Der Anbieter hat seinen Schweizer Hauptsitz in Zollikofen. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt die Deutsche Telekom in ihren Geschäftskundenbereichen Deutschland, Europa und T-Systems mehr als 2.600 Mitarbeitende im Bereich Cybersecurity. Neben Managed Security Services und Strategic Security Services werden auch Technical Security Services angeboten.

Stärken

Umfassende End-to-End Lösungen: Die Deutsche Telekom offeriert den Kunden lückenlose Technical Security Services mit einem kompletten Spektrum an Themen. Neben Technical Security Services sind auch Strategic Security Services und Managed Security Services verfügbar, so dass der gesamte Lifecycle eines Security-Projektes aus einer Hand abgedeckt werden kann. Darüber hinaus ermöglicht die Deutsche Telekom aufgrund der generellen IT-Kompetenz auch IT-Lösungen mit damit verbundener Cybersecurity. Hervorzuheben ist insbesondere auch das spezielle Know-how hinsichtlich der Kombination von IT, TK-Services und Security.

Erfüllung höchster Anforderungen: Die Erfahrung der Deutschen Telekom mit hochanspruchsvollen Umgebungen ist beeindruckend. Der Anbieter hat Projekte mit höchsten Anforderungen an die Zuverlässigkeit und den Schutz von IT-Infrastrukturen durchgeführt. Das Vertrauen in die eigene Leistung kommt u.a. in der Einführung ergebnisorienterter Preismodelle zum Ausdruck.

Zahlreiche namhafte Technologiepartner: Die Deutsche Telekom kooperiert mit zahlreichen renommierten Herstellern von Cybersecurity-Produkten und kann dabei oft den höchsten Partnerlevel vorweisen. So ist es der Deutschen Telekom möglich, die jeweils optimale Lösung für Kunden auf hohem Niveau zu erstellen.

Herausforderungen

Die Deutsche Telekom ist inzwischen auf drei Kontinenten vertreten, gemessen an anderen international aktiven Anbietern auf demselben Leistungsniveau ist die internationale Präsenz jedoch noch ausbaufähig.

Strategic Security Services

Wer sollte dieses Kapitel lesen

Dieser Bericht ist für Service Provider von Nutzen, die **Strategic Security Services (SSS)** in der **Schweiz** 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

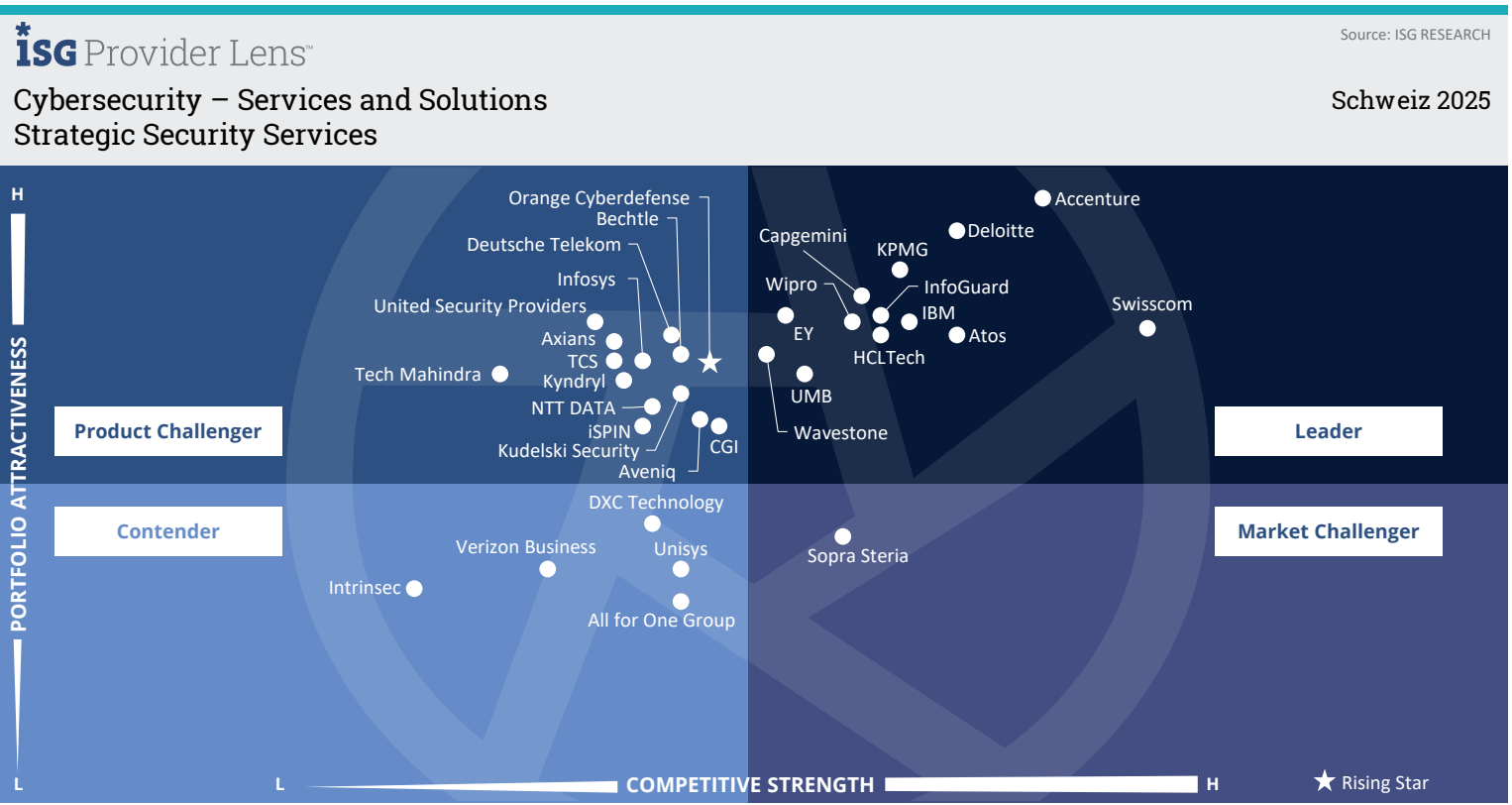
gewinnen aus diesem Bericht einen umfassenderen Überblick über Sicherheitstrends und die Leistungen der Anbieter bei der Entwicklung wirksamer Sicherheitsstrategien.

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

können sich mit diesem Bericht über die relative Positionierung und die Fähigkeiten von Dienstleistern informieren und erfahren, wie diese Faktoren den Entscheidungsprozess über Partnerschaften und Initiativen zur Kostensenkung unterstützen.



In diesem Quadranten geht es um die relevantesten **Cybersecurity-Berater** in der Schweiz, die Leistungen nicht **nur für die eigenen Produkte** offerieren. **Neue Technologien** und zunehmende **Cyberbedrohungen** 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

Die Lage hinsichtlich Cybersecurity-Gefährdungen in der Schweiz wird weiterhin bedrohlicher. Zusammen mit mangelnden Ressourcen ergibt sich ein zunehmendes Orientierungsbedürfnis hinsichtlich Cybersicherheit. Perspektivisch zeichnen sich zudem neue, technisch ausgefeilte Bedrohungen ab.

Angesichts immer komplexerer Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Hiervon sind schon lange nicht mehr nur die Schweizer Grossunternehmen betroffen, sondern zunehmend auch mittelständische Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin, besonders im Mittelstand.

Diese Faktoren bewirken, dass Unternehmen zunehmend externe Beratung benötigen. Anbieter mit einer ausgewogenen Kundenstruktur aus Grosskunden und mittelständischen Unternehmen profitieren sowohl von den umfangreichen Budgets der Grosskunden als auch vom überdurchschnittlichen Nachfragewachstum der Mittelständler.

Des Weiteren sind Dienstleister, die ihren Kunden neben Sicherheitsberatung auch -Umsetzung und -Betrieb anbieten können, im Vorteil; das gilt auch für Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen 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.

EY und UMB sind in den Leader-Quadranten aufgestiegen. Orange Cyberdefense ist der neue Rising Star. Infosys und Intrinsec sind neu im Quadranten vertreten. MTF ist bisher nicht im Quadranten präsent, hat aber aufgrund des starken Wachstum zukünftig gute Chancen.

Von den 38 Anbietern, die in dieser Studie dediziert in der Schweiz bewertet wurden, konnten sich 33 für diesen Quadranten qualifizieren. Dabei erreichten 13 eine Position als Leader, ein Anbieter wurde als Rising Star identifiziert.

accenture

Innovative Ansätze, tiefgehende Kompetenz und grosse Erfahrung in der Beratung für Cybersicherheit geben den Beratern von **Accenture** Zugang zur Vorstandsetage der Schweizer Kunden.

Atos

Der Ansatz von **Atos** in der Cybersecurity-Beratung ist ganzheitlich ausgeprägt. Atos ist in der Lage, im Rahmen seiner Security-Beratung bei seinen (potenziellen) Kunden Vertrauen durch zahlreiche Zertifizierungen zu schaffen.

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.

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 der Schweiz.

EY

Dank seiner Erfahrung und seines ganzheitlichen Beratungsansatzes steigt **EY** unter die Leader für Strategic Security Services in der Schweiz auf.

HCLTech

HCLTechs Dienstleistungen sind lückenlos, und auch die einbezogenen Technologien lassen keine Wünsche offen. HCL nimmt bereits eine führende Rolle im Schweizer Markt für Strategic Security Services ein und baut diese auch hinsichtlich der Marktpräsenz weiter aus.

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.

InfoGuard hat sich dank seiner optimalen Kundenstruktur und seines umfangreichen Portfolios erfolgreich unter den führenden Anbietern von Strategic Security Services in der Schweiz etabliert.

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.

Die **Swisscom** geht in der Cybersecurity-Beratung auf Basis eines breiten Leistungsprogramms auf die individuellen Bedürfnisse ihrer Kunden ein und verkörpert auf einzigartige Weise Swissness.

UMB

Dank umfassender Cybersecurity-Beratungsleistungen steigt **UMB** unter die führenden Anbieter von Strategic Security Services in der Schweiz auf.

Wavestone

Mit breiter Branchenexpertise etabliert sich **Wavestone** als ein Leader im Segment der Strategic Security Services in der Schweiz.

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

Mit vielfältigen Ressourcen sowie seinem attraktiven Angebot steigt **Orange Cyberdefense** zum Rising Star für Cybersecurity-Beratungsleistungen in der Schweiz auf.

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 der **Schweiz** anbieten, um ein besseres Verständnis ihrer Marktposition zu gewinnen, und ebenso für Unternehmen, die diese Provider evaluieren möchten. Im Rahmen dieses Quadranten beleuchtet ISG die aktuelle Marktpositionierung dieser Anbieter, basierend auf der Tiefe ihres Dienstleistungsangebots und ihrer Marktpräsenz.

Cybersicherheits-Experten

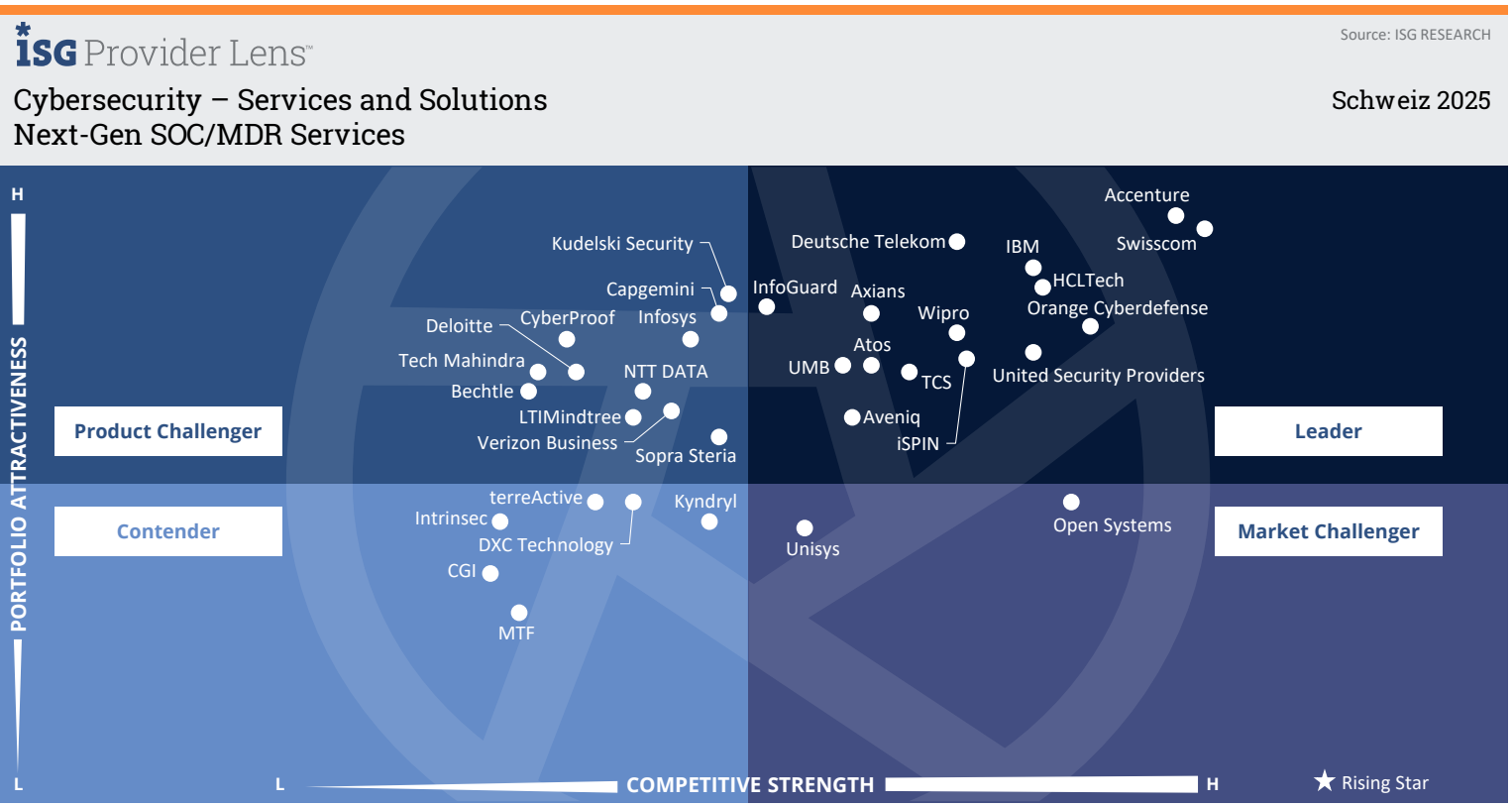
gewinnen durch diesen Bericht ein besseres Verständnis der sich abzeichnenden Trends und unmittelbaren Bedrohungen, was bei der strategischen Entscheidungsfindung hilft, die Produktivität steigert und die Komplexität der Sicherheitsmassnahmen reduziert.

Technologieexperten

werden mit diesem Bericht über sich abzeichnende Trends informiert, gewinnen Einblicke in massgeschneiderte Sicherheitsplattformen und können strategische Ziele und die sich verändernde Sicherheitslandschaft aufeinander abstimmen.

Experten auf der Geschäftsseite

gewinnen aus diesem Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht sowie praktische Lösungen zur Reduzierung der Komplexität gefunden werden können und die Effizienz gesteigert werden kann.



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/MDR Services** in der Schweiz, ohne Dienstleister, die ihre Leistungen nur für eigene Produkte erbringen. Die **dynamische Bedrohungslage** und der Fachkräftemangel **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

In der Schweiz wächst die Nachfrage nach Managed Detection & Response (MDR) Services und Diensten, die von Security Operations Centers (SOCs) erbracht werden, stark an. Dieses Wachstum wird durch immer häufigere, komplexere und wandlungsfähigere Cyberattacken gefördert. Die Knappheit an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen rücken diese Services darüber hinaus in den Fokus Schweizer Unternehmen.

Grossunternehmen erwarten häufig individuell zugeschnittene Lösungen für ihre speziellen Anforderungen. Des Weiteren spielen aufgrund der häufig internationalen Präsenz dieser Kunden global verteilte SOCs eine besondere Rolle. Aber auch den Betrieb in der Schweiz wissen grosse Firmen aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen.

Schweizer Betrieb und Herkunft – gemeinhin als „Swissness" bezeichnet – werden besonders von Mittelständlern geschätzt. Diese Zielgruppe interessiert sich immer mehr für SOC/MDR Services, um den zunehmenden Herausforderungen bei gleichzeitig besonders starkem Fachkräftemangel gewachsen zu sein.

Generell wird zudem von den Anbietern eine hohe Innovationskraft erwartet, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählen unter anderem künstliche Intelligenz und Automatisierung sowie proaktive Leistungen zur Vorbeugung. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen zunehmend interessant.

InfoGuard und UMB sind in den Leader-Quadranten aufgestiegen. Intrinsec und Kyndryl sind neu in der Analyse berücksichtigt.

Von den 38 Anbietern, die in dieser Studie dediziert in der Schweiz bewertet wurden, konnten sich 34 für diesen Quadranten qualifizieren. Dabei erreichten 15 eine Position als Leader.

accenture

Accenture ist mit seinem leistungsstarken, umfangreichen Angebot und der weltweiten Präsenz als Anbieter von Next-Gen SOC/MDR Services nicht nur für Grosskunden zunehmend attraktiv.

Atos

Die Schweiz zählt zu den SOC-Standorten von **Atos**, was auch für viele Grossunternehmen interessant ist. Sowohl die abgedeckten Themen als auch die Leistungen der Managed Security Services adressieren ein breites Spektrum.

AVENIQ

Das Portfolio von **Aveniq** für Next-Gen SOC/MDR Services deckt ein breites Spektrum an Leistungen ab. Aveniq bietet zudem End-to-End Cybersecurity Services und betreibt ein dediziertes SOC in der Schweiz.

axians

Axians IT Services offeriert im Rahmen seiner Next-Gen SOC/MDR Services ein breites Spektrum an Services und gemanagten Security-Themen. Für besonders gefährdete Daten und Systeme bietet das globale Cyber Defence Center ein erhöhtes Mass an Sicherheit.

Die **Deutsche Telekom** vereint erfolgreich grosse Branchenexpertise mit attraktiven Services „made in Switzerland" und ist so ein führender Anbieter von Next-Gen SOC/MDR Services in der Schweiz.

HCLTech

Allein in der Schweiz betreibt **HCLTech** mehrere dedizierte Security Operations Centers. Auch personell ist HCL hinsichtlich seiner Managed Security Services in der Schweiz stark aufgestellt. Das Portfolio deckt viele Leistungen und Technologien an.

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

Mit innovativer Technologie und attraktiven Services gelingt **InfoGuard** der Sprung unter die führenden Anbieter von Next-Gen SOC/MDR Services in der Schweiz.

iSPIN betreibt ein dediziertes SOC in der Schweiz und kombiniert dabei die Vorteile der Automatisierung mit der Erfahrung und Expertise seiner Fachleute.

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

Swisscoms umfassende und leistungsfähige Services sowie ihre ausprägte Swissness tragen zur eindeutigen Leader-Position im Schweizer Markt für Next-Gen SOC/MDR Services bei.

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 der Schweiz ein grosses Team.

UMB

Dank ausgeprägter Swissness und End-to-End-Services kann **UMB** zunehmend mehr Kunden von sich überzeugen und steigt unter die führenden Anbieter von Next-Gen SOC/MDR Services in der Schweiz auf.

United Security Providers

Zusammen mit der Swisscom bildet **United Security Providers** den grössten Cyber-Security-Kompetenzcluster der Schweiz. Mit „Security made in Switzerland" kann United Security Providers speziell angesichts der Datenschutzdiskussion punkten.

Die Leistungen von **Wipro** im Rahmen seiner Next-Gen SOC/MDR Services lassen keine Wünsche offen. Wipro konnte in den letzten zwölf Monaten in der Schweiz zahlreiche neue Deals gewinnen.

Leader

„Die Deutsche Telekom vereint erfolgreich attraktive Services „made in Switzerland“ mit grosser Branchenexpertise und ist so ein Leader für Next-Gen SOC/MDR Services in der Schweiz.”

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt 198.194 Mitarbeitende in mehr als 50 Ländern. Im GJ24 erwirtschaftete das Unternehmen einen Umsatz von 115,8 Mrd. €, wobei Services das grösste Segment sind. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH“ innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt die Deutsche Telekom in ihren Geschäftskundenbereichen Deutschland, Europa und T-Systems mehr als 2.600 Mitarbeitende im Bereich Cybersecurity. Das Unternehmen hat seinen Schweizer Hauptsitz in Zollikofen und betreibt ein Security Operations Center in der Schweiz.

Stärken

Diensterbringung auch aus der Schweiz: Die Deutsche Telekom bietet umfassende Managed Security Services in der Schweiz an. Der Anbieter betreibt zudem fortschrittliche Cyber Defense und Security Operations Centers und generiert als globaler Carrier umfangreiche Threat Intelligence. Mit der in der Schweiz angesiedelten Sicherheitsinfrastruktur inklusive SOC kann das Unternehmen seine Position stärken, insbesondere im Hinblick auf die Datenschutzdebatte.

Business-Erfahrung und -Expertise: Die Deutsche Telekom hat durch die Zusammenarbeit mit Unternehmen aus verschiedenen Branchen umfangreiche Erfahrungen gesammelt und ein tiefes Verständnis für deren spezifische Geschäftsanforderungen gewonnen. Der Anbieter kann daher eine breite Palette von Case Studies vorweisen. Darüber hinaus verfügt das Unternehmen über differenzierte Erkennungsmuster entsprechend den Anforderungen, individuellen Risiken und Vorgaben seiner Kunden.

Attraktives Service Portfolio: Die Deutsche Telekom baut ihr bereits umfassendes Angebot an Dienstleistungen kontinuierlich aus, um auch zukünftig ein leistungsfähiges Angebot offerieren zu können. Auf der Roadmap sind zahlreiche Vorhaben aufgeführt.

Herausforderungen

Um für global tätige Kunden noch attraktiver zu werden, könnte die Deutsche Telekom eine Ausweitung ihrer internationalen Präsenz in Erwägung ziehen. Im Vergleich zu zahlreichen anderen Anbietern auf einem ähnlich hohen Leistungsniveau ist die globale Präsenz der Deutschen Telekom noch ausbaufähig.

Next-Gen SOC/MDR Services – Large Accounts

Wer sollte dieses Kapitel lesen

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

Cybersicherheits-Experten

gewinnen durch diesen Bericht ein besseres Verständnis der sich abzeichnenden Trends und unmittelbaren Bedrohungen, was bei der strategischen Entscheidungsfindung hilft, die Produktivität steigert und die Komplexität der Sicherheitsmassnahmen reduziert.

Technologieexperten

werden mit diesem Bericht über sich abzeichnende Trends informiert, gewinnen Einblicke in massgeschneiderte Sicherheitsplattformen und können strategische Ziele und die sich verändernde Sicherheitslandschaft aufeinander abstimmen.

Experten auf der Geschäftsseite

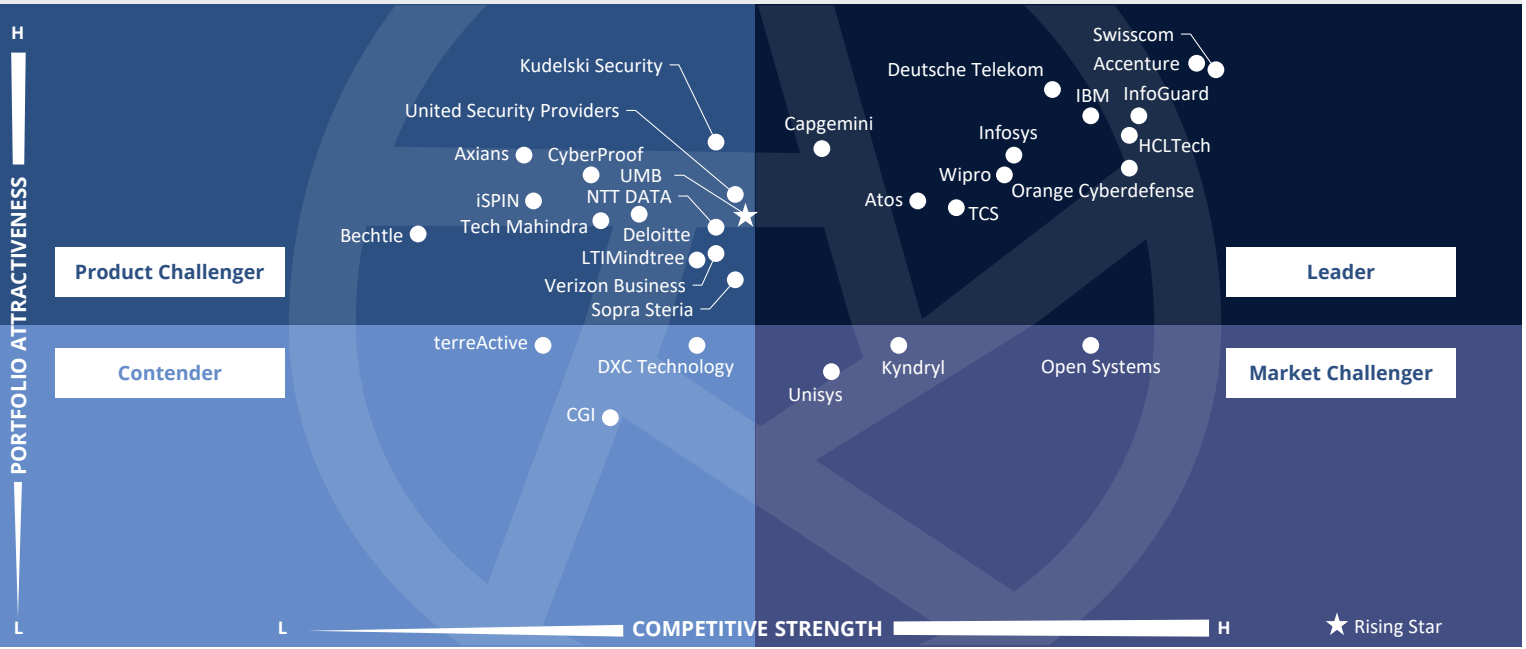
gewinnen aus diesem Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht sowie praktische Lösungen zur Reduzierung der Komplexität gefunden werden können und die Effizienz gesteigert werden kann.

ISG Provider Lens™

Source: ISG RESEARCH

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

Schweiz 2025



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/ MDR Services** für Schweizer **Grosskunden**, ohne Dienstleister, die ihre Leistungen nur für eigene Produkte erbringen. Hier zählt **Leistungsfähigkeit auf höchstem Niveau.**

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

Wie insgesamt in der Schweiz, wächst die Nachfrage nach Managed Detection & Response (MDR) Services sowie Diensten von Security Operations Centern (SOCs) im Marktsegment der Grosskunden deutlich an, wenngleich dieser Teilmarkt bereits eine höhere Reife als der Gesamtmarkt aufweist. Dieses Wachstum wird durch immer häufigere, komplexere und wandlungsfähigere Cyberattacken gefördert. Die Knappheit an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen rücken SOC- und MDR-Dienstleistungen seit einigen Jahren in den Fokus der Schweizer Grossunternehmen.

Entscheider in Grossunternehmen erwarten häufig individuell zugeschnittene Lösungen für ihre speziellen Anforderungen. Des Weiteren spielen aufgrund der oft internationalen Präsenz dieser Kunden global verteilte SOCs eine besondere Rolle. Aber auch den Betrieb in der Schweiz wissen grosse Firmen aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen.

Besonders Grosskunden erwarten von ihren Dienstleistern eine hohe Innovationskraft, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählen unter anderem künstliche Intelligenz und Automatisierung sowie proaktive Leistungen zur Vorbeugung. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen zunehmend interessant.

UMB ist dieses Jahr unter den betrachteten Anbietern zum Rising Star aufgestiegen. Kyndryl ist neu im Quadranten vertreten.

Von den 38 Anbietern, die in dieser Studie dediziert in der Schweiz bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten 12 eine Position als Leader, ein Anbieter wurde als Rising Star identifiziert.

accenture

Accenture ist mit seinem umfassenden, leistungsstarken Angebot und seiner globalen Präsenz Leader unter den Anbietern von Next-Gen SOC/MDR Services für Grosskunden in der Schweiz.

Atos

Auch mit der neuen alten Marke überzeugt **Atos** seine Grosskunden in der Schweiz mit globalem SOC-Betrieb und innovativer Technologie.

Capgemini

Internationale Präsenz und umfassende, innovative Dienstleistungen sind die Basis für **Capgeminis** Erfolg im Schweizer Markt der Next-Gen SOC/MDR Services für Grosskunden.

Die **Deutsche Telekom** ist mit ihren umfassenden Next-Gen-SOC-/MDR-Dienstleistungen „made in Switzerland", die von einem grossen, qualifizierten Team erbracht werden, Leader unter den Providern für Grosskunden in der Schweiz.

HCLTech

HCLTech bekennt sich erfolgreich zum Standort Schweiz und überzeugt seine Grosskunden mit der kontinuierlichen Weiterentwicklung seiner Next-Gen SOC/MDR Services.

IBM

IBM positioniert sich mit globaler Präsenz und umfassenden Next-Gen SOC/MDR Services, die auf leistungsstarker Technologie basieren, als ein führender Anbieter im Schweizer Markt für Grosskunden.

InfoGuard profiliert sich mit innovativer Technologie und attraktiven Services als ein Leader unter den Anbietern von Next-Gen SOC/MDR Services für Grossunternehmen in der Schweiz.

Infosys entwickelt im Schweizer Markt für Next-Gen SOC/MDR Services sein Angebot kontinuierlich mit grossem Ressourcenengagement zum Vorteil seiner Grosskunden weiter und positioniert sich damit als ein führender Provider.

Dank attraktiver Next-Gen SOC/MDR Services und globaler Präsenz ist **Orange Cyberdefense** ein führender Anbieter für Grosskunden in der Schweiz.

Umfangreiche und leistungsfähige Services sowie ihr starkes Expertenteam und beispielhafte **Swissness** tragen zur eindeutigen Leader-Position der Swisscom im Schweizer Markt der Next-Gen-SOC-/MDR-Dienstleistungen für Grosskunden bei.

TCS bietet im Rahmen seiner Next-Gen SOC/MDR Services erfolgreich kostenoptimierte, leistungsfähige Lösungen für global aktive Grosskunden an.

Mit seinen Next-Gen SOC/MDR Services ist **Wipro** in der Schweiz zunehmend erfolgreich. Dazu tragen Wipros umfangreiche, innovative Services für Grosskunden bei.

UMB

Dank ausgeprägter Swissness und End-to-End-Services steigt **UMB** zum „Rising Star" unter den Anbietern von Next-Gen SOC/MDR Services für Grossunternehmen in der Schweiz auf.

Leader

„Mit ihren umfassenden Next-Gen-SOC-/MDR-Dienstleistungen „made in Switzerland“, die von einem grossen, qualifizierten Team erbracht werden, ist die Deutsche Telekom Leader unter den Providern für Grosskunden in der Schweiz.“

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt 198.194 Mitarbeitende in mehr als 50 Ländern. Im GJ24 erwirtschaftete das Unternehmen einen Umsatz von 115,8 Mrd. €, wobei Services das grösste Segment sind. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH“ innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt die Deutsche Telekom in ihren Geschäftskundenbereichen Deutschland, Europa und T-Systems mehr als 2.600 Mitarbeitende im Bereich Cybersecurity. Das Unternehmen hat seinen Schweizer Hauptsitz in Zollikofen und betreibt ein Security Operations Center in der Schweiz.

Stärken

Services auch aus der Schweiz: Die Deutsche Telekom bietet umfassende Managed Security Services in der Schweiz an. Der Anbieter betreibt zudem fortschrittliche Cyber Defense und Security Operations Centers und generiert als globaler Carrier umfangreiche Threat Intelligence. Mit der in der Schweiz angesiedelten Sicherheitsinfrastruktur inklusive SOC kann das Unternehmen seine Position stärken, insbesondere im Hinblick auf die Datenschutzdebatte.

Ausgeprägtes Geschäftsverständnis: Die Deutsche Telekom hat durch die Zusammenarbeit mit Unternehmen aus verschiedenen Branchen umfangreiche Erfahrungen gesammelt und ein tiefes Verständnis für deren spezifische Geschäftsanforderungen gewonnen. Der Anbieter kann daher eine breite Palette von Case Studies vorweisen. Darüber hinaus verfügt das Unternehmen über differenzierte Erkennungsmuster entsprechend den Anforderungen, individuellen Risiken und Vorgaben seiner Kunden.

Umfangreiches, wachsendes Dienstleistungsangebot: Die Deutsche Telekom baut ihr bereits umfassendes Angebot an Dienstleistungen kontinuierlich aus, um auch zukünftig ein leistungsfähiges Angebot offerieren zu können. Auf der Roadmap sind zahlreiche Vorhaben aufgeführt .

Herausforderungen

Um für global tätige Grosskunden noch attraktiver zu werden, könnte die Deutsche Telekom eine Ausweitung ihrer internationalen Präsenz in Erwägung ziehen. Im Vergleich zu zahlreichen anderen Anbietern mit einem ähnlich hohen Leistungsniveau ist die globale Präsenz der Deutschen Telekom noch ausbaufähig.

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 der **Schweiz** 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

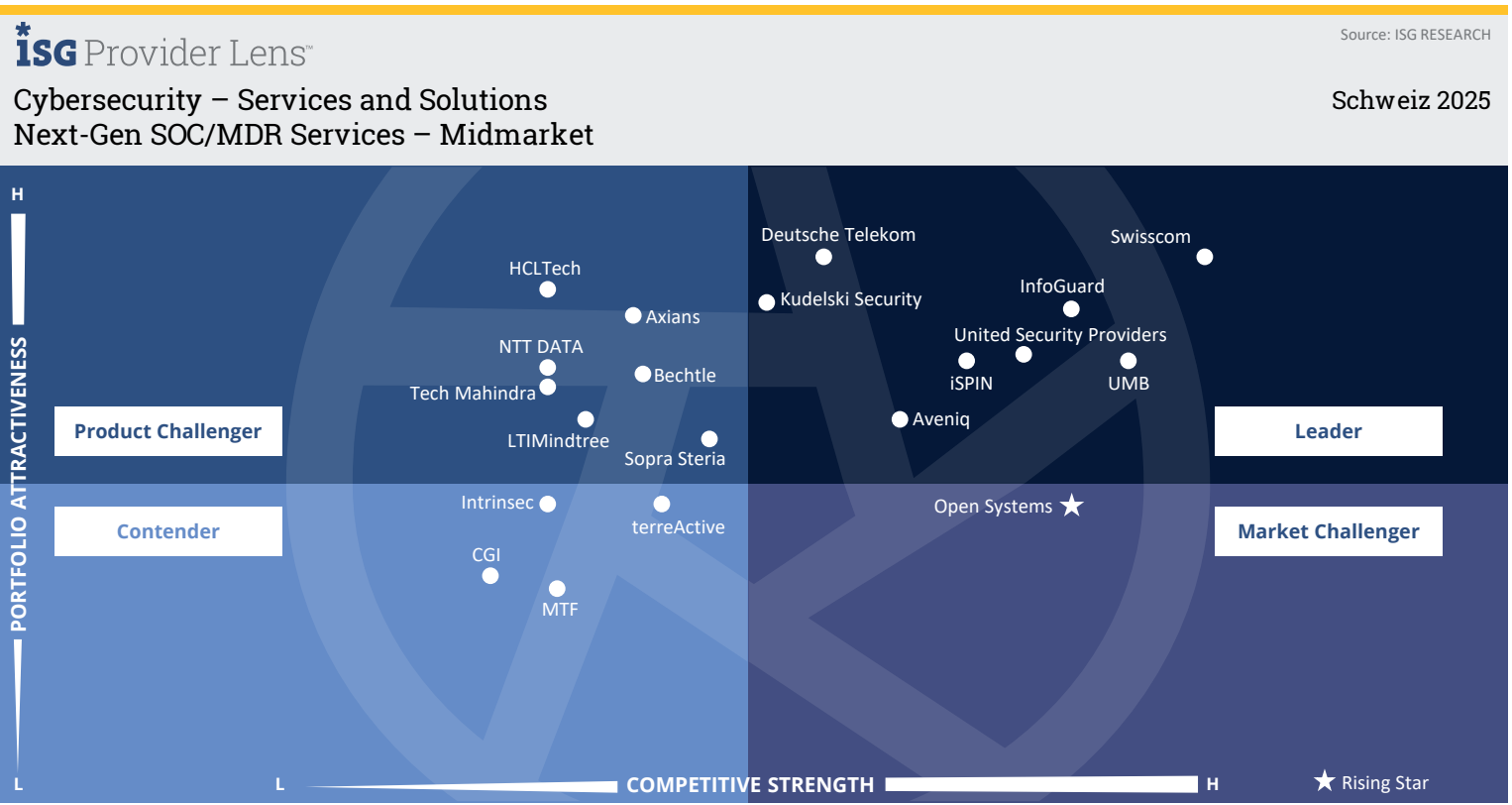
gewinnen aus diesem Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht sowie praktische Lösungen zur Reduzierung der Komplexität gefunden werden können und die Effizienz gesteigert werden kann.

Cybersicherheits-Experten

werden in diesem Bericht über sich abzeichnende Trends und unmittelbaren Bedrohungen informiert, was bei der strategischen Entscheidungsfindung hilft, die Produktivität steigert und die Komplexität der Sicherheitsmassnahmen reduziert.

Technologieexperten

erhalten mit diesem Bericht Einblicke in sich abzeichnende Trends und massgeschneiderte Sicherheitsplattformen und können strategische Ziele und die sich verändernde Sicherheitslandschaft aufeinander abstimmen.



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Next-Gen SOC/MDR Services** für Schweizer 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 der Schweizer Markt für SOC-/MDR-Dienste insgesamt wächst das Segment der mittelständischen Unternehmen, da diese einen besonders hohen Nachholbedarf haben. Mittelständler sind noch mehr als Grossunternehmen vom Fachkräftemangel insbesondere für Cybersecurity betroffen. Gleichzeitig sind auch sie mit immer mehr, immer neuen und immer komplexeren Sicherheitsherausforderungen konfrontiert, und Cyberkriminelle greifen verstärkt auch mittelständische Firmen an, da sie in ihnen wenig wehrhafte Opfer vermuten. Daher ist auch diese Zielgruppe zunehmend auf die Unterstützung externer Dienstleister angewiesen, um diese wachsenden Herausforderungen zu meistern. Im Zuge dieser Entwicklung steigt ihr Interesse an MDR Services und Diensten von Security Operations Centers. MDR-Dienstleister und SOCs bieten das erforderliche stets aktuelle Spezialistenwissen und die Ausrüstung für eine laufende Überwachung der Kundensysteme.

Schweizer Betrieb und Herkunft – kurz als „Swissness" bezeichnet – werden von vielen Mittelständlern geschätzt. Zudem wird von den Anbietern eine hohe Innovationskraft erwartet, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählen unter anderem künstliche Intelligenz und Automatisierung sowie proaktive Leistungen zur Vorbeugung. Für Industriekunden ist die Einbeziehung von OT Security zur Absicherung vernetzter Fertigungsanlagen zunehmend interessant.

Kudelski Security steigt vom Rising Star zum Leader auf. Neuer Rising Star ist Open Systems. Intrinsec ist neu im Quadranten vertreten.

Von den 38 Anbietern, die in dieser Studie dediziert in der Schweiz bewertet wurden, konnten sich 20 für diesen Quadranten qualifizieren. Dabei erreichten acht eine Position als Leader, ein Anbieter wurde als Rising Star identifiziert.

AVENIQ

Im Schweizer Markt der Next-Gen SOC/MDR Services für Mittelstandskunden profitiert **Aveniq** von den End-to-End-Services und der „Swissness".

Mit umfangreichen und zunehmend auf mittelständische Bedürfnisse zugeschnittenen Next-Gen SOC/MDR Services sowie tiefem Marktverständnis überzeugt die **Deutsche Telekom** Schweizer Mittelstandskunden.

InfoGuard
SWISS CYBER SECURITY

InfoGuard ist dank grosser Marktreichweite und attraktiver Next-Gen SOC/MDR Services mit „Swissness" ein führender Anbieter für mittelständische Kunden in der Schweiz.

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

In seinen Next-Gen SOC/MDR Services für den Mittelstand kombiniert **iSPIN** Swissness erfolgreich mit bedarfsgerechten Lösungen und einem umfassenden Ansatz.

Kudelski Security

Durch seinen zunehmenden Erfolg gelingt dem letztjährigen „Rising Star" **Kudelski Security** der Sprung unter die führenden Anbieter von Next-Gen SOC/MDR für den Schweizer Mittelstand.

swisscom

Ihre leistungsfähigen Services sowie ausprägte Swissness tragen zur eindeutigen Leader-Position der **Swisscom** im Schweizer Markt der Next-Gen SOC/MDR Services für den Mittelstand bei.

UMB

UMB gewinnt dank End-to-End-Services und Swissness zunehmend mehr Schweizer Mittelstandskunden für seine Next-Gen SOC/MDR Services.

United Security Providers

United Security Providers überzeugt Schweizer Mittelstandskunden mit umfangreichen Services, die von einer starken Organisation erbracht werden, und Delivery aus der Schweiz.

Open Systems

Open Systems steigt mit neuem Eigentümer und innovativen Investitionen zum „Rising Star" für Managed Security Services in der Schweiz auf.

Leader

„Die Deutsche Telekom überzeugt Schweizer Mittelstandskunden mit tiefem Marktverständnis sowie umfangreichen und zunehmend auf mittelständische Bedürfnisse zugeschnittene Next-Gen SOC/MDR Services."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt 198.194 Mitarbeitende in mehr als 50 Ländern. Im GJ24 erwirtschaftete das Unternehmen einen Umsatz von 115,8 Mrd. €, wobei Services das grösste Segment sind. Telekom Security wurde 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt die Deutsche Telekom in ihren Geschäftskundenbereichen Deutschland, Europa und T-Systems mehr als 2.600 Mitarbeitende im Bereich Cybersecurity. Das Unternehmen hat seinen Schweizer Hauptsitz in Zollikofen und betreibt ein Security Operations Center in der Schweiz.

Stärken

Umfassendes, weiterentwickeltes Leistungsspektrum: Um auch zukünftig ein leistungsfähiges Portfolio anbieten zu können, entwickelt die Deutsche Telekom das bereits sehr umfassende Angebot kontinuierlich weiter und plant weitere umfangreiche Ergänzungen – die Roadmap zählt zahlreiche Vorhaben auf. Die Deutsche Telekom bietet inzwischen ein speziell für den Mittelstand angepasstes Portfolio (MDR Pro) an, welches eine Vielzahl von Domänen anbietet, wie Endpoint, Identity, Connectivity, Cloud und OT. Gerade Schweizer Unternehmen legen Wert auf Services, die up-to-date sind. Dies sichert den zukünftigen Erfolg der Deutschen Telekom in der Schweiz.

SOC-Betrieb auch in der Schweiz: Die Deutsche Telekom betreibt unter anderem ein Security Operations Center in der Schweiz, was besonders von den Mittelstandskunden geschätzt wird. Mit „Security made in Switzerland" kann die Deutsche Telekom speziell angesichts der Datenschutzdiskussion – und besonders in der Zielgruppe des Mittelstandes – punkten. Speziell in diesem Marktsegment trifft das Datenhandling in der Schweiz auf positive Resonanz.

Technisches wie auch Business-Verständnis: Die Deutsche Telekom verfügt über ein tiefes Verständnis der Businessanforderungen und kann umfangreiche Erfahrung aus Mandaten in verschiedenen Branchen vorweisen sowie vielfältige Use Cases bereitstellen. Ausserdem verfügt die Deutsche Telekom über differenzierte Erkennungsmuster entsprechend den individuellen Risiken, Anforderungen und Vorgaben der jeweiligen Kunden.

Herausforderungen

Die Deutsche Telekom ist insgesamt erfolgreich im Schweizer Mittelstandsmarkt aktiv, der Schwerpunkt der Managed Security Services liegt aber nach wie vor noch auf Grosskunden. Es ist empfehlenswert, den Weg in den Mittelstandsmarkt auch weiterhin mit geeigneten Angeboten fortzusetzen, um ihn noch besser zu adressieren.

Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2025 – Cybersecurity – Services and Solutions" analysiert die entsprechenden Softwareanbieter und Dienstleister im Schweizer 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)

Editorin:
Maria Müller-de Haen

Forschungsanalysten:
Monica K und Sandya Kattimani

Datenanalysten:
Rajesh Chillappagari und Laxmi Sahebrao

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.

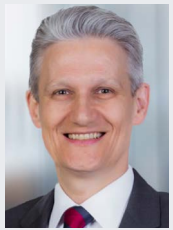
Die in dieser Studie vorgestellten Marktforschungs- und Analysedaten stammen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen 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. Er 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

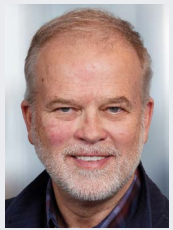
Heiko Henkes

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 ISC 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.

IPL Product Owner



Jan Erik Aase

Partner und globaler Leiter - ISG Provider Lens™

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

Als Partner und globaler Leiter von ISG Provider Lens™ ist er nun sehr gut positioniert, um den Zustand der Branche zu bewerten, darüber zu berichten und Empfehlungen sowohl für Unternehmen als auch für Kunden von Dienstleistern auszusprechen.

ISG Provider Lens™

Die ISG Provider Lens™ Quadranten-Reports bieten Bewertungen von Dienstleistern und kombinieren als einzige Studien dieser Art datengestützte Forschung und Marktanalysen mit praktischen Erfahrungen und Beobachtungen, gestützt auf das globale ISGBeraterteam. Unternehmen erhalten eine Fülle detaillierter Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Sourcing- Partner helfen; die ISG-Berater wiederum nutzen die Berichte, um ihre Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG abzugeben. Die Studien decken derzeit Provider mit Angeboten in mehreren Regionen weltweit ab. Weitere Informationen über die ISG Provider Lens Studien finden Sie auf dieser Webseite.

ISG Research™

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

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

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

ISG

ISG (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