ISG Provider Lens™

Cybersecurity – Solutions and Services

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

Customized report courtesy of:

QUADRANT REPORT | JULI 2024 | SCHWEIZ

Inhaltsverzeichnis

Bericht Autor: Frank Heuer, Gowtham Sampath (SSE), and Dr. Maxime Martelli (XDR)

Künstliche Intelligenz und „Swissness" prägen den Schweizer Cybersecurity-Markt

Für Schweizer Unternehmen nehmen Cyberbedrohungen 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 sowie die Umbrüche infolge des Home-Office Booms – 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 verstärkte 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 infolge zu einer zunehmenden Relevanz des Zero-Trust-Ansatzes geführt. Perimetersicherheit reicht nicht mehr aus. Der Grundsatz „never trust, always verify" (nie

Zunehmende **Cyberbedrohungen** treiben die Nachfrage nach externen Services voran.

vertrauen, immer überprüfen) bedeutet unter anderem gegenseitige Authentifizierung und kontinuierliche Überwachung des Netzwerks.

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.

Leider wird nach wie vor 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; besonders gilt dies für quantum-basierende Angriffe. Diese stellen in Zukunft eine neue Qualität bei Angriffen auf die Verschlüsselung von vertraulichen Daten dar. Derzeit spielen quantum-basierende Bedrohungen in der Praxis zwar noch keine Rolle, aber aufgrund der potenziell schwerwiegenden Folgen haben sich erste Dienstleister bereits mit ihrem Consulting darauf eingestellt. 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.

Identity & Access Management (Produkte)

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

Ein weiterer wichtiger Faktor ist die stetig steigende Zahl der Benutzer, Geräte und Dienste. Damit nimmt auch die Anzahl an digitalen Identitäten zu, die zu verwalten sind. Ein zusätzlicher Faktor ist die vermehrte Nutzung des Home Office. Viele Mitarbeitende greifen dadurch remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden.

Strategic Security Services

Angesichts der immer intensiveren und raffinierteren Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. 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

Weiterhin sind Unternehmen und Behörden in der Schweiz angesichts immer raffinierterer Cyberangriffe und des Fachkräftemangels immer häufiger darauf angewiesen, externe Dienstleister in Anspruch zu nehmen, 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

Immer komplexere Cyberattacken fördern besonders auch die Nachfrage nach Managed Security Services von Security Operations Centers (SOCs). Die Knappheit an qualifizierten Experten und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich 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.

Zusammenfassung

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.

Künstliche Intelligenz und Quantumtechnologie bedeuten neue Bedrohungen für Anwender, aber auch neue Chancen für Cybersecurity-Dienstleister. Vorteile haben dabei Serviceanbieter, die „Swissness" vorweisen können und sowohl die Grossunternehmen mit ihren grossen Budgets als auch die Mittelständler mit ihrer dynamisch wachsenden Nachfrage adressieren.

Zusammenfassung

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

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

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

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

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

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

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

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

Trends im Bereich Extended Detection & Response (XDR)

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

Die wichtigsten Trends im XDR-Bereich sind nachstehend aufgeführt:

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

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

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

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

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

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

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

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

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

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

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

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

Zusammenfassung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anbieterpositionierung

Seite 1 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Accenture	Not In	Not In	Not In	Leader	Leader	Leader	Not In
All for One Group	Not In	Not In	Not In	Contender	Contender	Not In	Not In
Aveniq	Not In	Not In	Not In	Contender	Product Challenger	Leader	Leader
Axians	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger
Bechtle	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger	Product Challenger
BeyondTrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Contender	Not In	Not In	Not In	Not In	Not In
BlackBerry	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Broadcom	Product Challenger	Leader	Product Challenger	Not In	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Product Challenger	Not In

Anbieterpositionierung

Seite 2 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Product Challenger	Contender	Contender
Check Point Software	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	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
CyberProof	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In
Deloitte	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In

Anbieterpositionierung

Seite 3 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Deutsche Telekom	Not In	Not In	Not In	Leader	Product Challenger	Leader	Leader
DXC Technology	Not In	Not In	Not In	Leader	Contender	Contender	Not In
Ergon Informatik	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Eviden	Leader	Not In	Not In	Leader	Leader	Leader	Not In
EY	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Fortinet	Contender	Leader	Product Challenger	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Leader	Leader	Leader	Product Challenger

Anbieterpositionierung

Seite 4 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
HPE (Aruba)	Not In	Not In	Contender	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Not In
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
IN Groupe	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
InfoGuard	Not In	Not In	Not In	Leader	Leader	Product Challenger	Leader
Infosys	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In
Intrinsec	Not In	Not In	Not In	Contender	Not In	Not In	Not In
ISPIN	Not In	Not In	Not In	Leader	Product Challenger	Leader	Leader
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Leader	Not In	Not In

Anbieterpositionierung

Seite 5 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Kudelski Security	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Rising Star ★
Kyndryl	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Not In
Lookout	Not In	Not In	Contender	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
ManageEngine	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In
MTF	Not In	Not In	Not In	Contender	Not In	Contender	Contender
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Nevis	Leader	Not In	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

Anbieterpositionierung

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

Anbieterpositionierung

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 8 von 9

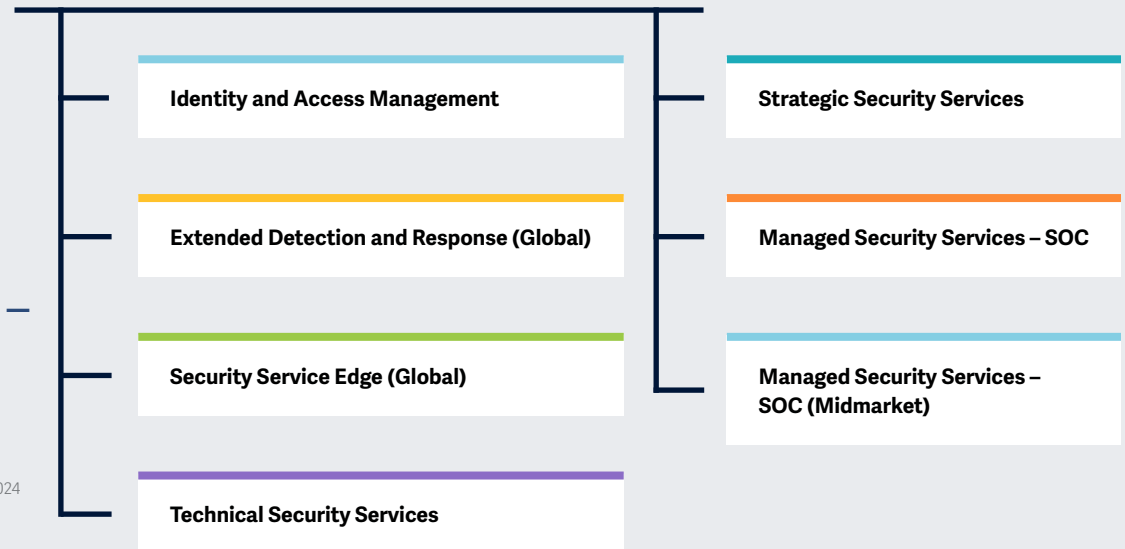
	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
SolarWinds	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Product Challenger	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
Swisscom	Not In	Not In	Not In	Leader	Leader	Leader	Leader
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
terreActive	Not In	Not In	Not In	Not In	Not In	Contender	Contender
Thales	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 9 von 9

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC	Managed Security Services - SOC (Midmarket)
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In	Not In
UMB	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
Unisys	Not In	Not In	Not In	Market Challenger	Contender	Market Challenger	Not In
United Security Providers	Leader	Not In	Not In	Not In	Product Challenger	Leader	Leader
Verizon Business	Not In	Not In	Not In	Not In	Contender	Product Challenger	Not In
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Leader	Leader	Not In
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In

Untersuchte Schwerpunkt-themen der Studie **Cybersecurity – Solutions and Services 2024**.



Vereinfachte Illustration; Quelle: ISG 2024

Definition

Cybersicherheit im Zeitalter der künstlichen Intelligenz

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

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

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

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

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

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

Betrachtungsumfang der Studie

Dieser ISG Provider Lens™-Quadrantenbericht deckt die folgenden 7 Quadranten für Dienstleistungen/Lösungen ab: Identity and Access Management, Technical Security Services, Strategic Security Services, Managed Security Services - SOC, Managed Security Services - SOC (Midmarket). Die Anbieter von Security Service Edge (SSE)-Lösungen sowie von Extended Detection & Response (XDR) werden in dieser Studie in diesem Jahr aus einer globalen Perspektive analysiert und positioniert, nicht aus der Perspektive einzelner Länder und Regionen, da sich diese Märkte derzeit noch im Anfangsstadium und Reifungsprozess befinden.

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

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

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

Klassifizierung der Anbieter

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

Identity and Access Management

Wer diesen Bericht lesen sollte

Dieser Bericht ist für Schweizer Unternehmen von grosser Bedeutung, denn er bietet eine umfassende Bewertung von IAM-Lösungsanbietern und ermöglicht es ihnen, fundierte Entscheidungen entsprechend ihren spezifischen Sicherheitsbedürfnissen zu treffen. Darüber hinaus wird bewertet, wie die einzelnen Anbieter Unternehmen bei der Bewältigung komplexer Sicherheitsherausforderungen im Zusammenhang mit der Sicherung des Benutzerzugangs und von digitalen Identitäten unterstützen.

Unternehmen in der Schweiz erkennen zunehmend, wie wichtig IAM-Lösungen sind. Mit zunehmender Digitalisierung und Remote-Arbeit steigt die Nachfrage nach einem sicheren Zugangsmanagement. Schweizer Unternehmen sehen ein, dass IAM erforderlich ist, um die Einhaltung von Vorschriften zu gewährleisten und die sich entwickelnde Bedrohungslandschaft zu entschärfen.

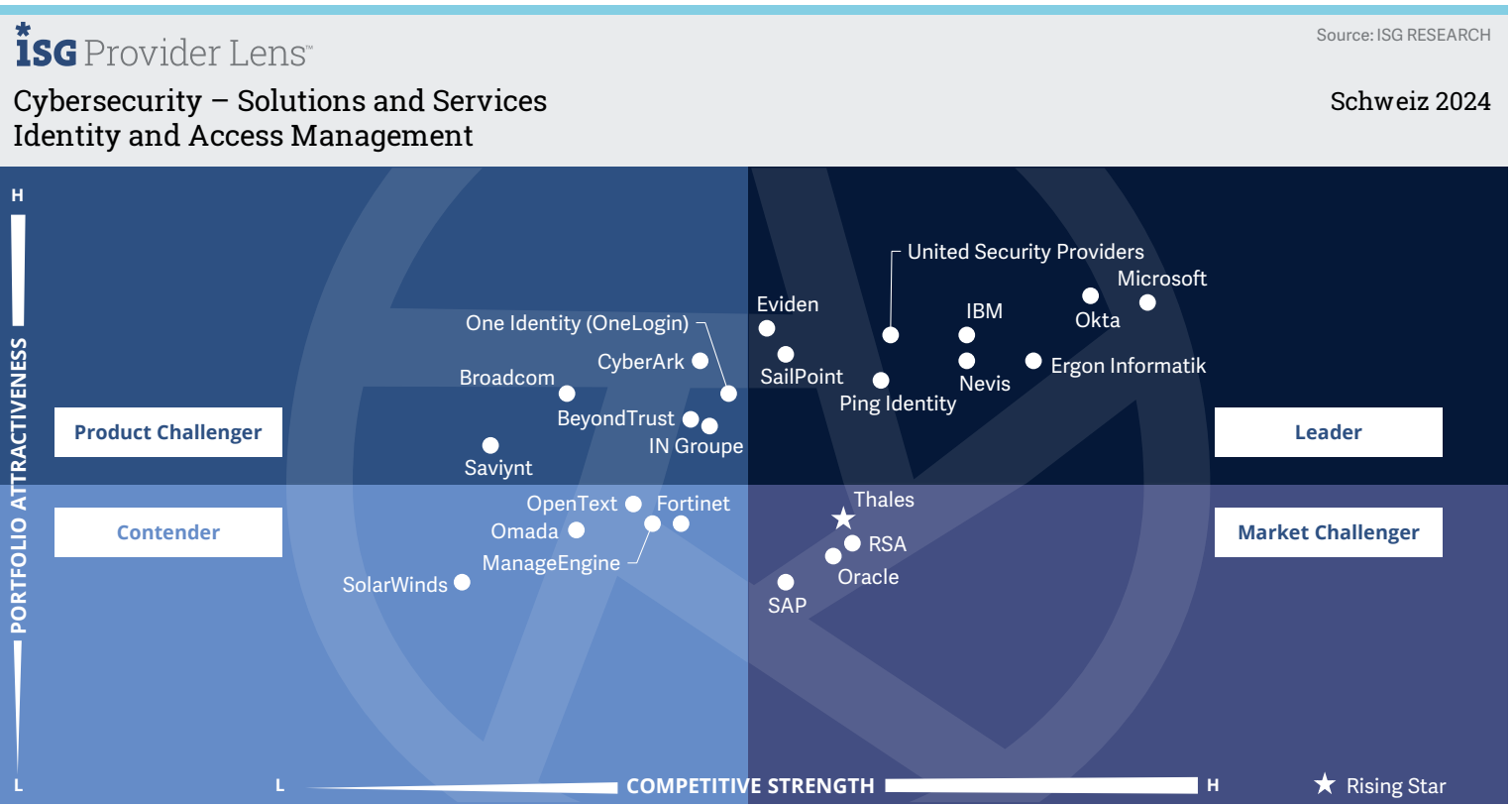
IAM-Anbieter gehen mit skalier- und anpassbaren Lösungen auf die besonderen Anforderungen von Schweizer Unternehmen ein. Sie wissen, wie komplex die Sicherung von Benutzerzugängen und digitalen Identitäten in einem stark regulierten Umfeld wie der Schweiz ist. Die Provider bieten Funktionalitäten wie Multifaktor-Authentifizierung, Single Sign-on und Privileged Access Management an, um die vielfältigen Sicherheitsanforderungen von Schweizer Unternehmen zu erfüllen.

Sie fokussieren sich zudem auf Integrationsmöglichkeiten zur nahtlosen Einbindung ihrer Lösungen in bestehende Infrastrukturen. Dieser Ansatz gewährleistet eine minimale Störung des Betriebs und verbessert gleichzeitig die Sicherheitslage insgesamt. Dank entsprechender Optionen können Schweizer Unternehmen IAM-Lösungen an branchenspezifische Anforderungen und Compliance-Standards anpassen.

Risikomanagement-Experten hilft dieser Bericht, die Effektivität von IAM-Lösungen bei der Bekämpfung von identitätsbezogenen Bedrohungen und Schwachstellen zu bewerten.

Enterprise-Architekten gewinnen aus diesem Bericht ein besseres Verständnis dafür, wie sich IAM-Lösungen in bestehende Systeme und Anwendungen integrieren lassen.

Experten auf der Geschäftsseite erfahren aus diesem Bericht, wie IAM-Lösungen die strategische Entscheidungsfindung und Risikosteuerungsinitiativen unterstützen und so Sicherheitsrisiken mindern und wertvolle digitale Ressourcen schützen.



In diesem Quadranten geht es um die **relevantesten** IAM Provider in der Schweiz, die proprietäre Software anbieten bzw. betreiben. Wichtige Themen sind **SSO, MFA** und **Betrieb in der Schweiz. Passwortlose** Authentifizierung und **KI**-Support gewinnen an Bedeutung.

Frank Heuer

Definition

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

IAM-Lösungen dienen dem Management (Erfassung, Aufzeichnung und Verwaltung) von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets auf Basis von Privileged Access Management (PAM), d.h. des Zugriffs anhand von definierten Policies.

Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungs-Suites im Rahmen von Management Suites zunehmend in sichere Mechanismen, Frameworks und Automatisierung (z.B. der Risikobewertung) eingebunden, um Nutzer- und Attacken-Profiling in Echtzeit durchführen zu können. Von den Lösungsanbietern werden zudem weitere Funktionalitäten für Social Media und mobile Anwendungen erwartet, um deren spezifische Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Dieser Quadrant umfasst auch Machine Identity Management.

Auswahlkriterien

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

Beobachtungen

In der Schweiz ist IAM auch in diesem Jahr ein besonders relevantes Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, so dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern z.B. auch vernetzte Maschinen in der Fertigung (Industrie 4.0). Zudem nimmt die Anzahl zu verwaltender digitaler Identitäten von Nutzern stetig zu. Ein entscheidender Faktor ist dabei der Umzug vieler Mitarbeiter in das Home Office. Durch vermehrte Remote- und mobile Zugriffe auf die Unternehmensressourcen werden die Kontrolle und Regulierung des Zugriffs für IT-Verantwortliche zu einer zunehmend drängenden Aufgabe, was wiederum noch höhere Sicherheits- bei gleichzeitig höheren Komfortanforderungen zur Folge hat. Daher gewinnen Themen wie Single Sign-on (SSO), Multi-Faktor-Authentifizierung (MFA), intuitive Schnittstellen, passwortlose Authentifizierung sowie der Einsatz von Biometrie und künstlicher Intelligenz an Bedeutung.

Wie im Softwaremarkt insgesamt verschiebt sich auch der IAM-Betrieb zunehmend von On-Premise in die Cloud. Die meisten Provider bieten somit sowohl den On-Premise- als auch den Cloudbetrieb an. Auch reine Cloudanbieter treten immer häufiger auf, allen voran Okta. Anbieterseitig ist zudem zu erwähnen, dass Ping Identity den Wettbewerber ForgeRock übernommen und integriert hat, der somit in unserer Analyse nicht mehr dediziert aufgeführt ist. SailPoint ist der Sprung unter die Leader gelungen. Neuer Rising Star ist die Thales Group. ManageEngine ist neu im Quadranten vertreten.

Von den 59 Anbietern, die in dieser Studie bewertet wurden, konnten sich 24 für diesen Quadranten qualifizieren. Dabei erreichten neun eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Ergon Informatik

Ergon Informatik ist ein führender Schweizer IAM-Anbieter, der seine Kunden mit vielseitigen und starken Authentifizierungsmöglichkeiten bei gleichzeitiger Benutzerfreundlichkeit überzeugt.

EVIDEN an atos business

Auch unter neuem Namen ist **Eviden (an Atos Business)** als Leader im Schweizer Markt dank eines vielseitigen IAM-Portfolios erfolgreich aufgestellt.

IBM

IBM überzeugt in der Schweiz mit einer vielseitigen, leistungsfähigen Lösung, kombiniert mit einer hohen Marktpräsenz.

Microsoft

Microsoft gelingt es mit verbesserten Lösungen und nicht zuletzt auch versiertem Marketing, sich im Schweizer IAM-Markt immer mehr durchzusetzen.

Nevis

Nevis überzeugt mit einfacher mobiler Nutzung und besonders auch mit dem Erfolg in anspruchsvollen Anwendersegmenten, insbesondere im Bankensektor.

Okta

Durch den rein cloudbasierten Ansatz kann **Okta** die einfache und schnelle Realisierung von Identity & Access-Management-Lösungen versprechen.

Ping Identity

Ping Identity überzeugt immer mehr Kunden in der Schweiz durch die Vielseitigkeit seiner innovativen Lösung sowie die Balance zwischen Anwenderkomfort und Sicherheit.

SailPoint

SailPoint nutzt künstliche Intelligenz zur Risikominimierung und erleichtert darüber hinaus die IAM-Verwaltung von Multicloud-Umgebungen. So gelingt SailPoint der Sprung unter die IAM-Leader in der Schweiz.

United Security Providers

Mit Swissness und einer breiten Leistungspalette profiliert sich **United Security Providers** im Schweizer Markt für IAM-Lösungen als führender Anbieter.

THALES
Building a future we can all trust

Die **Thales** steigt durch innovative und umfangreiche Authentifizierungsmethoden zum Rising Star für IAM-Lösungen in der Schweiz auf.

Extended Detection and Response (Global)

Wer diesen Bericht lesen sollte

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

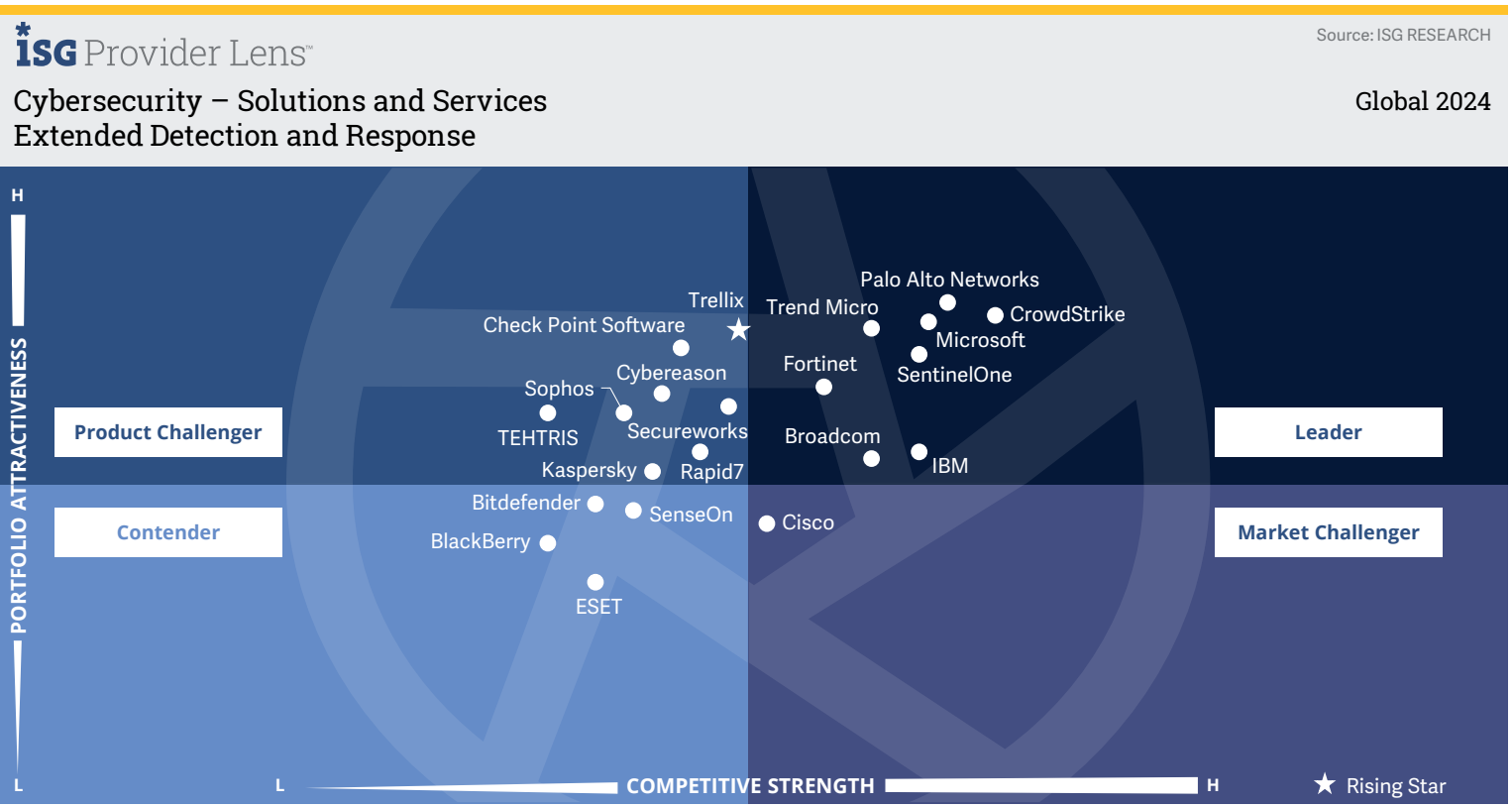
Unternehmen erkennen die Notwendigkeit eines proaktiven Ansatzes zur Erkennung von und Reaktion auf Bedrohungen, der sich auf Data-Science-Techniken und dynamisch aktualisierte Bedrohungsdaten stützt. XDR ermöglicht es Unternehmen jeder Größe und jedes Sicherheitsniveaus, robuste Fähigkeiten zur Erkennung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

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

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

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

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



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

Dr. Maxime Martelli

Definition

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

Auswahlkriterien

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

Beobachtungen

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

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

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

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

Von den 35 Unternehmen, die für diese Studie bewertet wurden, haben sich 21 für diesen Quadranten qualifiziert; acht dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Broadcom

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

CrowdStrike

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

Fortinet

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

IBM

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

Microsoft

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

Palo Alto Networks

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

SentinelOne

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

Trend Micro

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

Trellix

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

Security Service Edge (Global)

Wer diesen Bericht lesen sollte

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

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

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

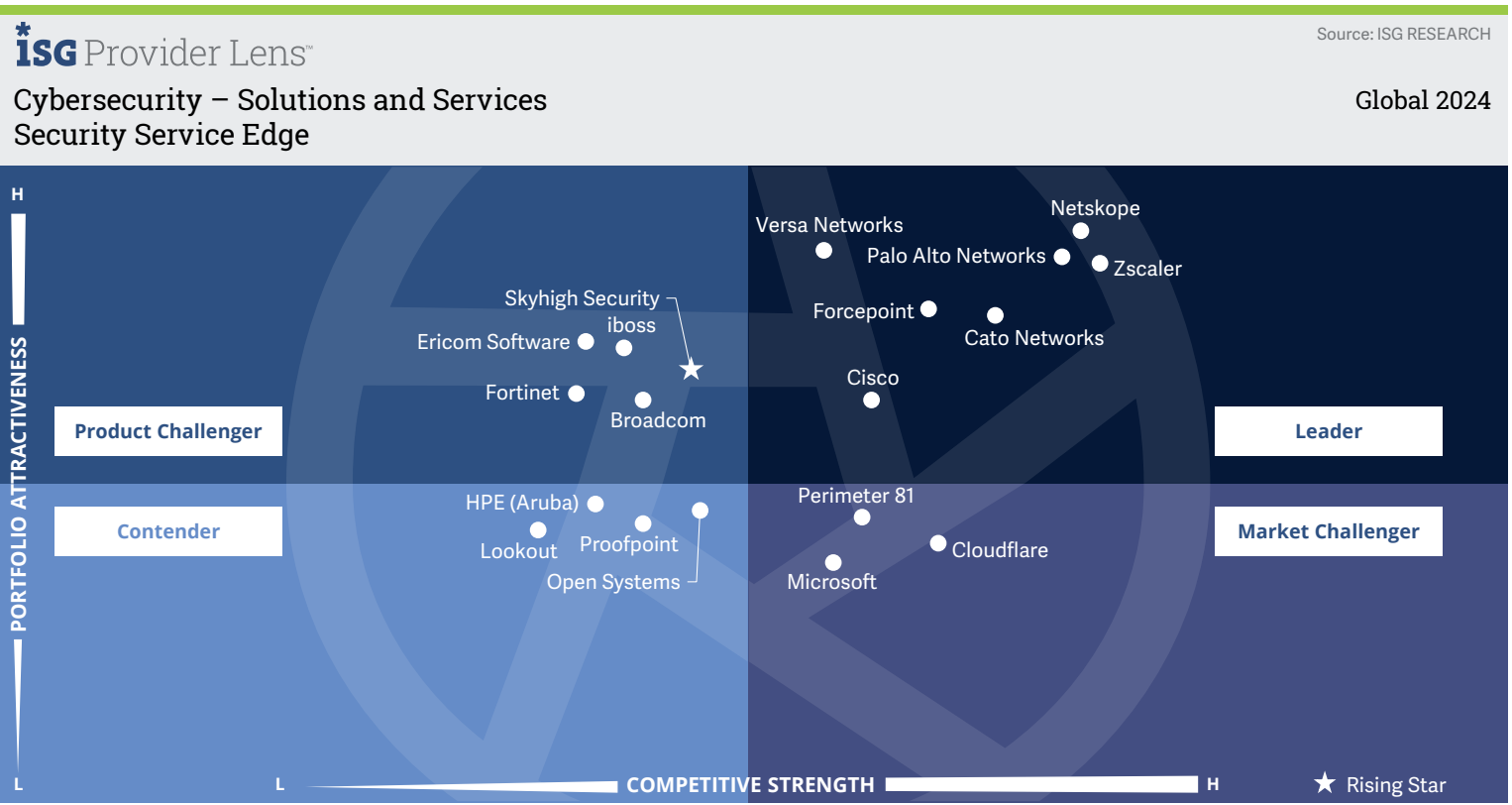
SSE wird eingesetzt, um moderne Sicherheitsherausforderungen zu bewältigen, den Zugang zu vereinfachen und die digitalen Erfahrungen zu verbessern. Von den Anbietern wird gewünscht, dass sie rationalisierte Lösungen, robusten Schutz und Flexibilität in einer sich schnell entwickelnden Landschaft bieten.

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

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

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

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



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

Gowtham Sampath

Definition

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

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

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

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

Auswahlkriterien

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

Beobachtungen

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

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

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

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

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

Anbieterauswahl: Differenzierung im SSE-Markt:

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

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

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

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

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

Von den 35 Unternehmen, die für diese Studie bewertet wurden, haben sich 19 für diesen Quadranten qualifiziert; sieben dieser Anbieter wurden als Leader und einer als Rising Star positioniert.

Cato Networks

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

Cisco

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

Forcepoint

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

Netskope

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

Palo Alto Networks

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

Versa Networks

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

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

Skyhigh Security

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

Technical Security Services

Wer diesen Bericht lesen sollte

Dieser Bericht über TSS ist für in der Schweiz tätige Unternehmen relevant. Er bietet umfassende und wertvolle Einblicke in den aktuellen Markt für Security Services in der Schweiz für diverse Branchen. Der Bericht bewertet die Fähigkeiten von TSS-Anbietern bei der Integration verschiedener Sicherheitsprodukte und -lösungen unterschiedlicher Anbieter und bietet so einen ganzheitlichen Marktüberblick, der über die reine Bewertung proprietärer Angebote hinausgeht.

In der heutigen, sich schnell entwickelnden Bedrohungslandschaft ist es für ein effektives Sicherheitsmanagement entscheidend, über die neuesten Trends, Technologien und Strategien informiert zu sein. Dieser Bericht beleuchtet die Positionierung von TSS-Anbietern, um Unternehmen zu helfen, die Wettbewerbslandschaft zu verstehen und fundierte Entscheidungen bei der Auswahl von Sicherheitspartnern zu treffen.

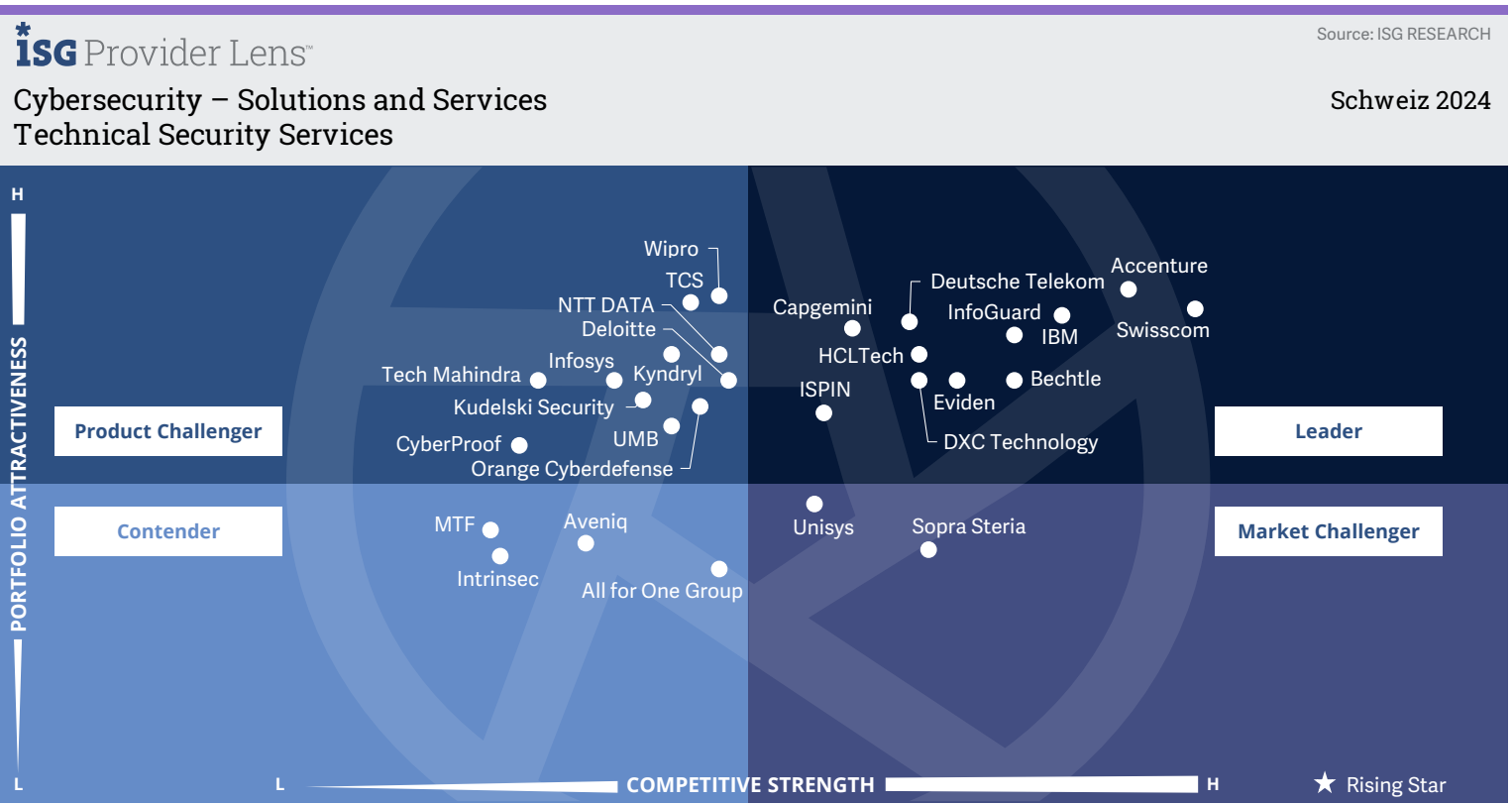
Schweizer Unternehmen nutzen TSS-Lösungen zur Verbesserung ihrer Sicherheitslage. Angesichts der zunehmenden Komplexität und Raffinesse der Sicherheitsbedrohungen erkennen viele Unternehmen, wie wichtig eine Partnerschaft mit spezialisierten TSS-Anbietern ist, um ihre Abwehrmassnahmen zu stärken. Dieser Trend wird durch den Bedarf an umfassenden Sicherheitslösungen vorangetrieben, die ein breites Spektrum an Bedrohungen in digitalen und physischen Bereichen abdecken können.

Die massgeschneiderten Lösungen der TSS Provider kombinieren modernste Technologien mit Security Best Practices. TSS-Anbieter offerieren ein breites Portfolio, um die unterschiedlichen Bedürfnisse ihrer Kunden zu erfüllen, von verwalteten Sicherheitsdiensten bis hin zu Beratungs- und Unterstützungsleistungen. Durch ihr umfassendes Verständnis der Bedrohungslandschaft und der branchenspezifischen Anforderungen helfen diese Provider Unternehmen dabei, proaktive Sicherheitsmassnahmen zu implementieren und effektiv auf neue Bedrohungen zu reagieren.

Strategieexperten erhalten durch diesen Bericht Einblicke in die neuesten Trends, Technologien und Strategien im Bereich der Security Services.

Sicherheitsexperten können sich mit diesem Bericht über neue Bedrohungen, Best Practices und Lösungen im Markt für Sicherheitsdienstleistungen informieren.

Risikomanager gewinnen durch diesen Bericht Einblicke in die sich entwickelnde Bedrohungslandschaft und die Strategien von TSS-Anbietern zur Bewältigung von Sicherheitsherausforderungen.



In diesem Quadranten geht es um die **relevantesten** Dienstleister für technische Security Services, deren Leistungen nicht nur die eigenen Produkte abdecken. Externe Dienstleister helfen, die zunehmenden Cybersecurity-Herausforderungen **zu bewältigen**.

Frank Heuer

Definition

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

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

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

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

Auswahlkriterien

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

Beobachtungen

Schweizer Unternehmen sind mit immer intensiveren wie auch raffinierteren, komplexeren und ständig neuen Cyberattacken konfrontiert, erschwert durch den Mangel an Cybersecurity-Experten. Daher sind sie 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 und zahlreichen hochwertigen Zertifizierungen ihrer Mitarbeiter.

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

Von den 59 Anbietern, die in dieser Studie bewertet wurden, konnten sich 28 für diesen Quadranten qualifizieren. Dabei erreichten elf eine Position als Leader.

accenture

Accenture offeriert ein breites Spektrum an Technical Security Services. Zusammen mit kosteneffizienten Automatisierungsleistungen – unterstützt von der Security Automation Factory – tragen sie zur führenden Position von Accenture im Schweizer Markt bei.

BECHTLE

Im Schweizer Markt für Technical Security Services profitieren **Bechtle** und seine Kunden von ausgeprägter lokaler Präsenz und einem grossen Team. Dies ist besonders im Mittelstandssegment nützlich.

Capgemini

Capgemini versteht es, sich im Markt für Technical Security Services als Anbieter mit innovativen Ansätzen – zum Beispiel Security Automation und künstlicher Intelligenz – hervorzuheben.

Deutsche Telekom Security überzeugt die Kunden mit Cybersecurity-Lösungen aus einem Guss, die höchste Ansprüche an die Zuverlässigkeit und den Schutz von IT-Infrastrukturen erfüllen.

DXC TECHNOLOGY

DXC Technology profitiert von der globalen Präsenz und unterstützt seine Kunden mit Hilfe eines umfassenden Portfolios für Technical Security Services, integrierten Lösungen und weiterentwickelter Automatisierung.

Eviden (an Atos Business) hat sich in der Schweiz mit einem ganzheitlichen Cybersecurity-Ansatz, der auch die Geschäftsrelevanz betont, als ein Leader hinsichtlich Technical Security Services etabliert.

HCLTech

HCLTech überzeugt im Schweizer Markt für Technical Security Services mit einem grossen und tiefen Angebot, das zahlreiche Technologien adressiert, sowie mit globaler Erfahrung und starken Partnerbeziehungen.

Weltweite Präsenz und Erfahrung sowie umfassende Kompetenzen und tiefe technische Skills machen **IBM** zu einem Leader im Schweizer Markt für Technical Security Services.

Im Schweizer Markt für Technical Security Services festigt **InfoGuard** seine Position als Leader durch ein umfassendes, zeitgemässes Angebot und eine ausgewogene Kundenstruktur.

ISPIN profiliert sich als leistungsfähiger Dienstleister, besonders bei dem wichtigen Thema der Netzwerksicherheit, und profitiert von einer Zielgruppe mit grossem Potenzial.

Umfassende Kompetenzen, starke Partnerschaften mit renommierten Herstellern von Cybersecurity-Produkten und eine grosse Reichweite in der Schweiz sind die Basis für die Leader-Position der **Swisscom** im Markt für Technical Security Services.

Leader

"Deutsche Telekom Security überzeugt ihre Kunden mit Cybersecurity-Lösungen aus einem Guss, die höchste Ansprüche erfüllen."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 204.200 Mitarbeitende in über 87 Niederlassungen in mehr als 50 Ländern. Im Geschäftsjahr 2023 erwirtschaftete das Unternehmen einen Umsatz von 112,0 Milliarden €. Telekom Security wurde 2020 in eine eigenständige rechtliche Einheit, die „Deutsche Telekom Security GmbH", (nachfolgend „Deutsche Telekom"), innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security rund 1.700 Mitarbeitende. Der Hauptsitz der Deutschen Telekom in der Schweiz befindet sich in Zollikofen. Neben Managed Security Services und Strategic Security Services werden auch Technical Security Services angeboten.

Stärken

Höchste Anforderungen werden erfüllt: Die Erfahrung der Deutschen Telekom mit hochanspruchsvollen Umgebungen ist beeindruckend. Die Deutsche Telekom 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.

Security-Lösungen aus einem Guss: Die Deutsche Telekom bietet den Kunden lückenlose Technical Security Services, die ein komplettes Spektrum an Themen abdecken. Neben Technical Security Services werden auch Strategic Security Services und Managed Security Services aus einer Hand angeboten, so dass der gesamte Lifecycle eines Security-Projektes aus einem Guss abgedeckt wird. Darüber hinaus ermöglicht die Deutsche Telekom aufgrund der generellen IT-Kompetenz auch IT-Lösungen mit damit verbundener Cybersecurity. Hervorzuheben ist insbesondere auch die das spezielle Know-how hinsichtlich der Kombination von IT-Security und TK-Security.

Umfangreiche Technologiepartnerschaften: 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

Um für weltweit aktive Kunden noch attraktiver zu sein, könnte ein weiterer Ausbau der globalen Präsenz erwägenswert sein. Der Provider ist inzwischen auf drei Kontinenten vertreten, gemessen an anderen international aktiven Anbietern auf dem Leistungsniveau der Deutschen Telekom ist die internationale Präsenz jedoch noch ausbaufähig.

Strategic Security Services

Wer diesen Bericht lesen sollte

Schweizer Unternehmen sind mit zunehmenden Bedrohungen der Cybersicherheit konfrontiert; dadurch steigt der Bedarf an massgeschneiderten Strategien zum Schutz ihres Geschäftsbetriebs. Dieser Bericht ist für Schweizer Unternehmen von grosser Bedeutung, denn er informiert über die Anbieter von strategischen Sicherheitsdiensten, die eine fundierte Entscheidungsfindung ermöglichen.

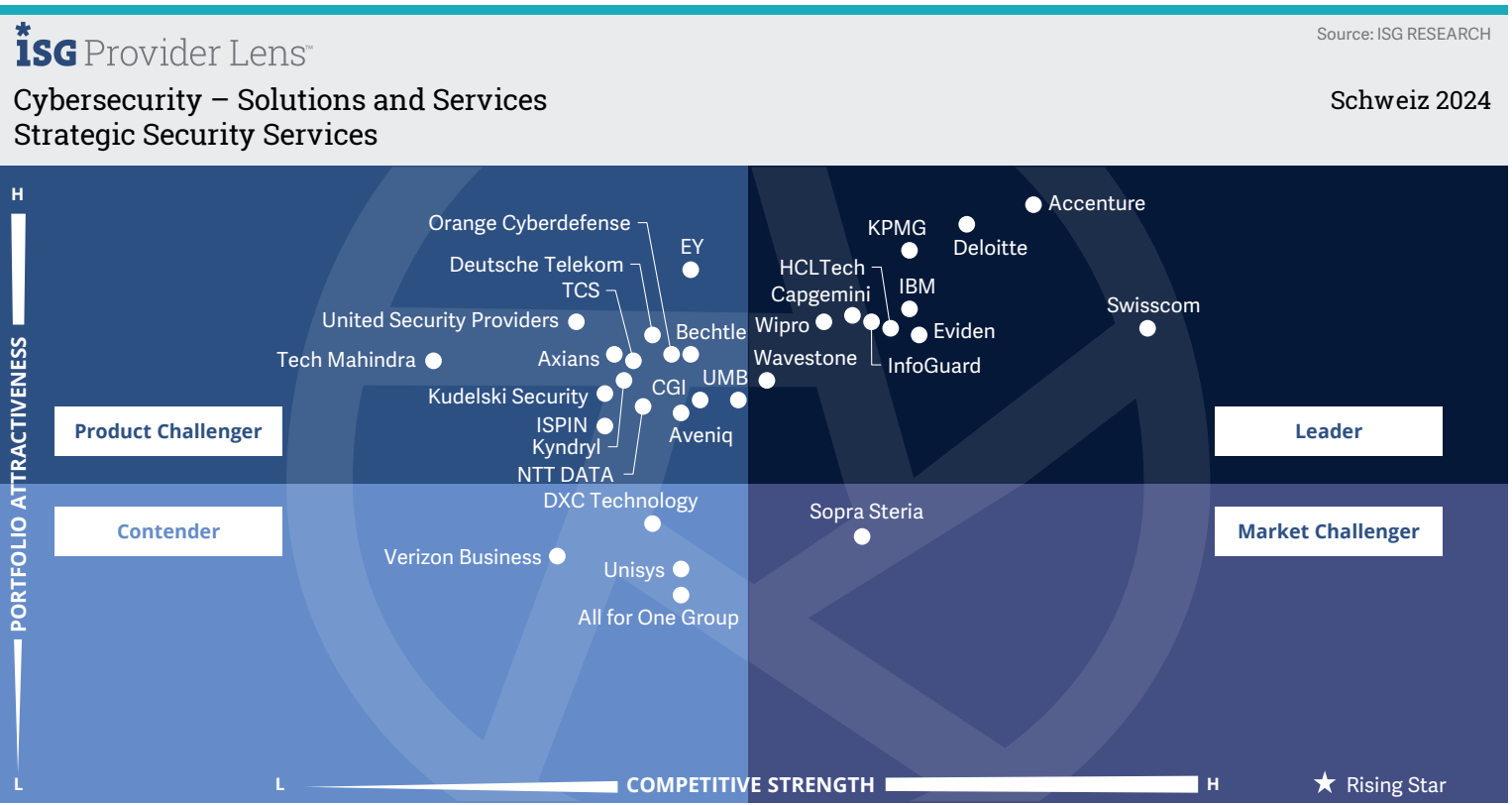
Unternehmen verlassen sich zunehmend auf SSS, um den Sicherheitsreifegrad zu bewerten und massgeschneiderte Cybersicherheitsstrategien zu entwickeln. Angesichts der zunehmenden Digitalisierung und des Drucks von Seiten des Gesetzgebers nehmen Schweizer Unternehmen SSS Provider in Anspruch, um komplexe Sicherheitsherausforderungen zu bewältigen. Diese Anbieter verfügen über spezielles Fachwissen zur Bewertung der Risikosituation und zur Entwicklung proaktiver Sicherheitsmassnahmen, die auf die Unternehmensziele abgestimmt sind.

Die Bedrohungslage verschärft sich, u.a. durch raffinierte Cyberangriffe wie Ransomware, Phishing und Advanced Persistent Threats (APTs). Diese Angriffe gefährden nicht nur sensible Daten, sondern stören auch die Geschäftskontinuität; für Unternehmen ist es deshalb unerlässlich, robuste Security Frameworks aufzubauen und einzusetzen. SSS Provider spielen eine entscheidende Rolle bei der Erkennung von Schwachstellen, der Risikominderung und der Einhaltung neuer rechtlicher Anforderungen.

Compliance-Beauftragte gewinnen durch diesen Bericht ein besseres Verständnis dafür, wie ausgewählte SSS Provider die branchenspezifischen Compliance-Anforderungen erfüllen und die Datenschutzbestimmungen einhalten.

Sicherheitsexperten werden mit diesem Bericht über die Fähigkeiten von SSS-Anbietern informiert, so dass sie ihre Sicherheitsstrategien besser auf die Unternehmensziele abstimmen können.

Strategieexperten hilft dieser Bericht, SSS-Anbieter zu bewerten und fundierte Entscheidungen zur Verbesserung ihrer Cybersicherheitslage zu treffen.



In diesem Quadranten geht es um die **relevantesten** Cybersecurity-Berater in der Schweiz, die Leistungen nicht nur für die eigenen Produkte offerieren. Steigende Cyberbedrohungen sowie Chancen und Risiken neuer Technologien **erhöhen den Beratungsbedarf**.

Frank Heuer

Definition

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

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

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

Auswahlkriterien

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

Beobachtungen

Die Cybersecurity-Gefährdungssituation in der Schweiz nimmt weiterhin zu. Der Ukraine-Krieg ist dabei nur das bekannteste Beispiel für das Anfachen von Bedrohungen. Zusammen mit mangelnden Ressourcen ergibt sich ein zunehmendes Orientierungsbedürfnis hinsichtlich Cybersicherheit. Perspektivisch zeichnen sich zudem neue, technisch ausgefeilte Bedrohungen ab.

Angesichts immer komplexerer Cyberattacken – auch im Zuge geopolitischer Konflikte – sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Hiervon sind schon lange nicht mehr nur die bekannten Schweizer Grossunternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelständische Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin; besonders in mittelgrossen Unternehmen.

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, damit die Strategie bruchlos in die Tat umgesetzt werden kann, im Vorteil; das gilt auch für Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen – gegebenenfalls auch zugehörige neugestaltete Geschäftsprozesse – aus einem Guss anbieten können. Erste Berater stellen sich auf die Abwehr von quantum-basierenden Cyberattacken ein.

Wavestone ist in den Leader-Quadranten aufgestiegen. Secureworks und Zensar sind nicht mehr im Quadranten vertreten.

Von den 59 Anbietern, die in dieser Studie bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten elf eine Position als Leader.

accenture

Accenture setzt durch grosse Kompetenz und Erfahrung Massstäbe in der Cybersecurity-Beratung in der Schweiz und hat Zugang zur Führungsetage seiner Kunden.

Capgemini

Capgemini punktet in der Schweiz mit einem umfassenden und weiter ausgebauten Portfolio für Cybersecurity Consulting sowie mit der praktischen Erfahrung seiner Berater.

Deloitte.

Deloitte profiliert sich mit starker globaler Präsenz sowie mit einem umfassenden Portfolio und Businessverständnis.

EVIDEN
an atos business

Eviden (an Atos Business) bringt mit seinem ganzheitlichen Ansatz gute Voraussetzungen für eine führende Position im Schweizer Markt für Cybersecurity Consulting mit.

HCLTech

HCLTech ist ein führender Berater für Cybersecurity in der Schweiz und baut mit umfassenden Dienstleistungen seine Marktposition weiter aus.

IBM

IBM ist ein Vorreiter bei der Cybersecurity-Beratung mit einem umfassenden, integrierten und innovativen Angebot sowie tiefen technischen Insights.

InfoGuard

Mit umfangreichem Portfolio, Verständnis für zahlreiche Technologien und optimaler Kundenstruktur hat sich **InfoGuard** als ein führender Anbieter im Schweizer Markt für Cybersecurity-Beratung etabliert.

Die führende Position von **KPMG** im Schweizer Markt für Cybersecurity Consulting stützt sich auf die geschickte Synthese von Business- und technischer Beratung mit strategischer Kompetenz.

Mit Umsetzungskompetenz, einem umfangreichen Leistungsspektrum, individuellen End-to-End-Services und ausgeprägter Swissness ist die **Swisscom** ein führender Cybersecurity-Berater.

Wavestone

Wavestone setzt Akzente zur Nachhaltigkeit und ist mit grosser Erfahrung sowie Branchenexpertise in der Schweiz zunehmend erfolgreich, so dass der Sprung unter die führenden Anbieter von Cybersecurity-Beratung gelingt.

Wipro unterstreicht seine führende Position im Schweizer Markt für Cybersecurity Consulting durch ein umfangreiches Portfolio, tiefgehende technische Kompetenz und kundenorientiertes Pricing.

Managed Security Services – SOC

Wer diesen Bericht lesen sollte

Im Rahmen dieses Quadranten wird die Relevanz von MSS für Schweizer Unternehmen bewertet; er bietet wertvolle Einblicke zur Auswahl von MSS-Anbietern, die auf die effektive Bekämpfung von Sicherheitsbedrohungen spezialisiert sind. Angesichts der sich ständig weiterentwickelnden Cyberbedrohungen ist der Bedarf an robusten MSS für den Schutz von Unternehmensressourcen und -daten von entscheidender Bedeutung.

Dieser Bericht gibt Einblicke in die Art und Weise, wie die einzelnen MSS Provider kritische Herausforderungen im Markt angehen. Diese Informationen sind von unschätzbarem Wert für Unternehmen, die ihre Sicherheitsstrategien auf Best Practices und neue Trends abstimmen wollen. Schweizer Unternehmen, die verstehen, wie MSS-Anbieter Herausforderungen wie sich entwickelnde Bedrohungslandschaften, Compliance-Anforderungen und technologische Fortschritte bewältigen, können fundierte Entscheidungen treffen, die ihre Sicherheitslage verbessern.

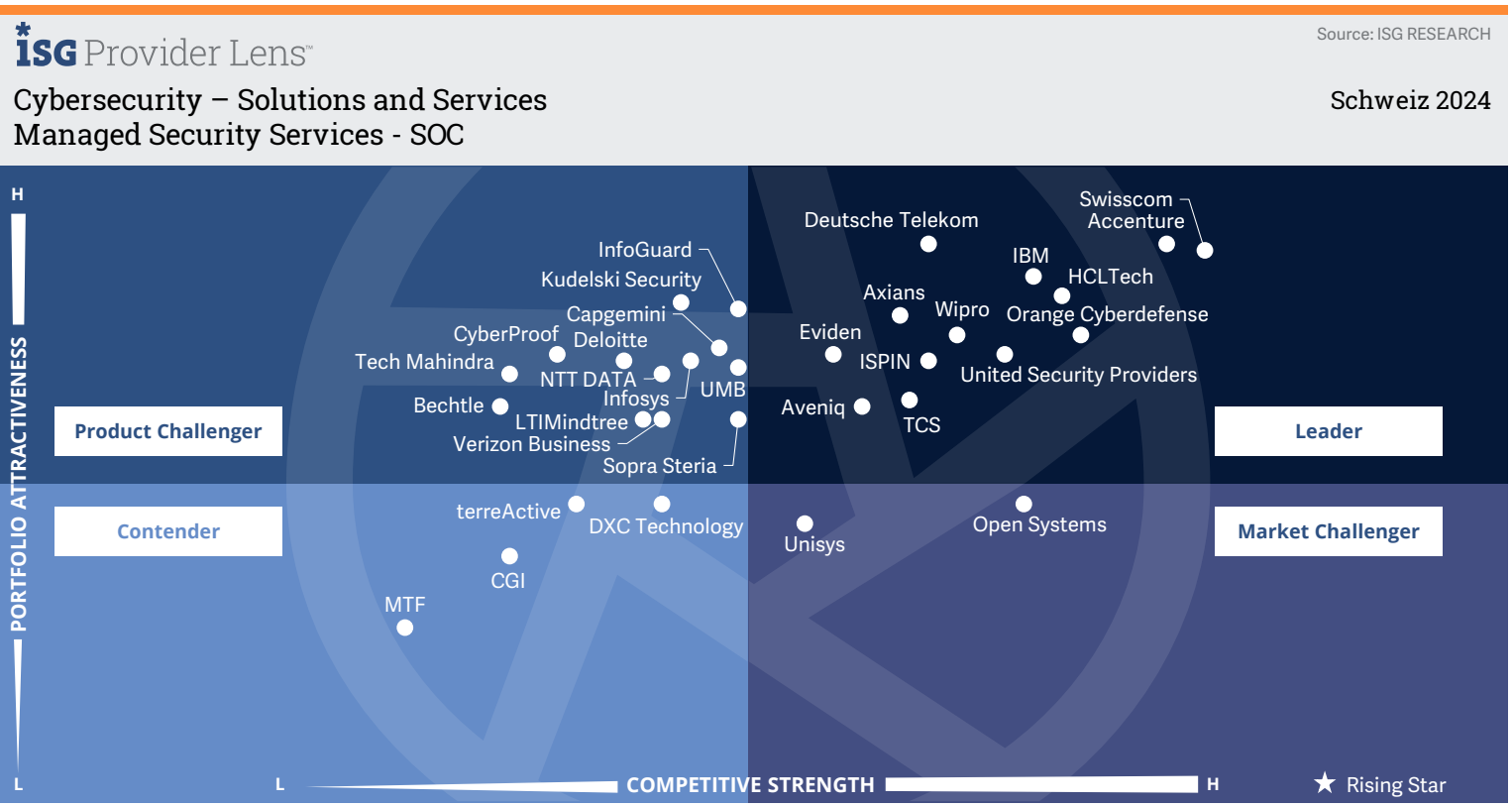
Schweizer Unternehmen setzen zunehmend auf MSS. Cyberbedrohungen werden immer raffinierter und greifen immer mehr um sich; viele Unternehmen erkennen die Grenzen herkömmlicher Sicherheitsmassnahmen und wenden sich für einen umfassenden Schutz an MSS-Anbieter. Dieser Trend spiegelt den wachsenden Bedarf an Fachkenntnissen und proaktiven Sicherheitsmassnahmen zur wirksamen Risikominderung wider.

MSS Provider bieten Schweizer Unternehmen eine Reihe von Leistungen an, die auf ihre spezifischen Bedürfnisse zugeschnitten sind. Zu diesen Services zählen z.B. eine 24/7-Sicherheitsüberwachung, die Erkennung von und Reaktion auf Bedrohungen, Schwachstellenmanagement und Unterstützung bei der Einhaltung von Vorschriften. Mit Hilfe der Expertise und der Ressourcen von MSS-Anbietern können Schweizer Unternehmen sich von der Last der internen Sicherheitsverwaltung befreien, sich auf ihr Kerngeschäft konzentrieren und gleichzeitig auch weiterhin eine robuste Sicherheitslage gewährleisten.

Sicherheitsexperten können anhand der Informationen in diesem Bericht potenzielle MSS-Anbieter bewerten und ihre Fähigkeiten zur wirksamen Bekämpfung von Sicherheitsbedrohungen einschätzen.

Technische Experten können sich mit diesem Bericht über die Landschaft der MSS-Anbieter informieren und Partner identifizieren, die die Sicherheitslage ihres Unternehmens verbessern können.

Beschaffungsexperten hilft dieser Bericht, MSS-Anbieter zu bewerten und fundierte Entscheidungen hinsichtlich der Beschaffung von Managed Security Services zu treffen.



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Managed Security Services aus SOCs** auf dem Schweizer Markt, ohne Dienstleister, die ihre Leistungen nur für eigene Produkte erbringen. Externer Betrieb durch **SOCs** ist stark gefragt.

Frank Heuer

Definition

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

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

Auswahlkriterien

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

Beobachtungen

In der Schweiz wächst die Nachfrage nach Managed Security Services, die von Security Operations Centers (SOCs) erbracht werden, stark an; ISG erwartet, dass das Marktvolumen von SOC Services in der Schweiz 2024 um etwa 18 Prozent auf 424 Mio. CHF zunehmen wird. Dies bedeutet ein durchschnittliches jährliches Marktwachstum zwischen 2021 und 2024 von rund 19 Prozent.

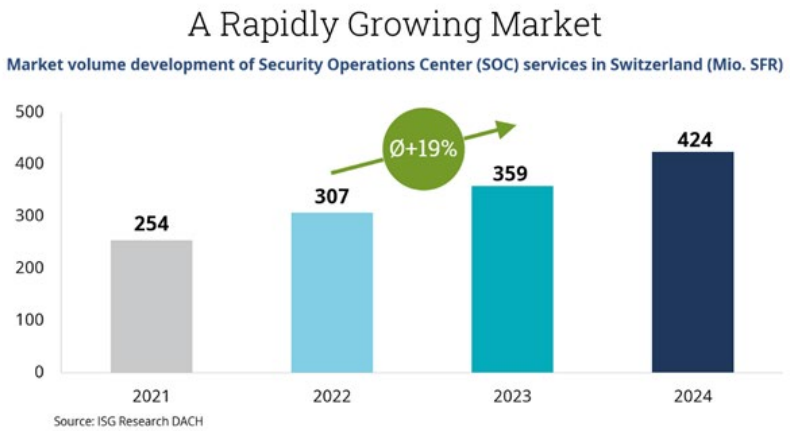
Dieses herausragende Wachstum wird durch immer häufigere, komplexere und wandlungsfähigere Cyberattacken gefördert. Die Knappheit an qualifizierten Fachleuten und das erforderliche stets aktuelle Spezialistenwissen rücken SOC-Dienstleistungen darüber hinaus in den Fokus Schweizer Unternehmen.

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 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.

Von den 59 Anbietern, die in dieser Studie bewertet wurden, konnten sich 32 für diesen Quadranten qualifizieren. Dabei erreichten dreizehn eine Position als Leader.



accenture

Das SOC-Service-Angebot von **Accenture** ist umfassend und deckt alle Security-Themen, einschliesslich OT Security, ab. Dies sowie die globale Präsenz machen den Provider zu einem starken Leader im Schweizer Markt.

AVENIQ

Aveniq profiliert sich mit End-to-End-Leistungen und überzeugender „Swissness" als Leader im Schweizer Markt für Managed Security/SOC Services.

axians

Die Kunden von **Axians IT Services** profitieren von der Delivery aus der Schweiz und kundenorientierten Services, die an die Ansprüche der Klienten anpassbar sind.

Deutsche Telekom Security vereint als Leader erfolgreich umfangreiche Services „made in Switzerland" mit einem grossen Team und Europas grösstem integrierten Cyber Defense & Security Operations Center.

Eviden (an Atos Business) überzeugt seine Kunden mit den innovativen Ansätzen seiner umfassenden Managed Security/SOC Services und SOC-Betrieb in der Schweiz.

HCLTech bekennt sich erfolgreich zum Standort Schweiz und überzeugt mit umfangreichen wie auch kontinuierlich weiterentwickelten Managed Security/SOC Services.

IBM profiliert sich mit globalem Betrieb und umfassenden Managed Security/SOC Services, die auf leistungsstarker eigener Technologie basieren.

Mit kundenorientierten, modularen SOC Services aus der Schweiz und einem umfassenden Ansatz überzeugt **ISPIN** seine Kunden und ist Leader für Managed Security/SOC Services in der Schweiz.

Orange Cyberdefense überzeugt seine internationalen Grosskunden mit globaler und lokaler Präsenz sowie Managed Security/SOC Services, die up to date sind.

Die **Swisscom** überzeugt ihre Kunden mit von einem starken Expertenteam erbrachten Dienstleistungen auf Basis tiefer Insights und steht auf einzigartige Weise für „Swissness". Damit ist die Swisscom ein herausragender Leader für Managed Security/SOC Services.

TCS kombiniert im Rahmen seiner Managed Security/SOC Services erfolgreich kostenoptimierte, leistungsfähige Lösungen für global aktive Kunden, die alle Cybersecurity-Technologien abdecken.

United Security Providers

Als Teil des grössten Cybersecurity-Kompetenzclusters der Schweiz profiliert sich **United Security Providers** mit Security made in Switzerland als Leader für Managed Security/SOC Services.

Mit umfangreichen Services, die Effizienzvorteile bieten, und zunehmender Profilierung gewinnt **Wipro** im Schweizer Markt für Managed Security/SOC Services weitere neue Engagements.

Leader

"Die Deutsche Telekom vereint erfolgreich umfangreiche Services „made in Switzerland" mit einem umfangreichen Team – und ist so Leader für Managed Security/SOC Services in der Schweiz."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 204.200 Mitarbeitende in über 87 Niederlassungen in mehr als 50 Ländern. Im Geschäftsjahr 2023 erwirtschaftete das Unternehmen einen Umsatz von 112,0 Milliarden €. Telekom Security wurde 2020 in eine eigenständige rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom") innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security rund 1.700 Mitarbeiter. Der Hauptsitz der Deutschen Telekom in der Schweiz befindet sich in Zollikofen. Die Deutsche Telekom betreibt ein SOC in der Schweiz.

Stärken

Tiefgehendes Businessverständnis: Die Deutsche Telekom kann umfangreiche Erfahrung aus Mandaten in verschiedenen Branchen vorweisen, besitzt tiefes Verständnis für Businessanforderungen und kann dadurch vielfältige Use Cases bereitstellen. Darüber hinaus verfügt die Deutsche Telekom über differenzierte Erkennungsmuster entsprechend den Anforderungen, individuellen Risiken und Vorgaben der jeweiligen Kunden.

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

Grosses, wachsendes Leistungsprogramm: Die Deutsche Telekom entwickelt das bereits sehr umfassende Angebot kontinuierlich weiter und plant weitere umfangreiche Ergänzungen des Portfolios, um auch zukünftig ein leistungsfähiges Angebot offerieren zu können. Die Roadmap zählt zahlreiche Vorhaben auf.

Herausforderungen

Im Vergleich zu den meisten Wettbewerbern kann die Deutsche Telekom spezielle Kompetenzen hinsichtlich der Anforderungen des Mittelstands vorweisen. Dennoch liegt der Fokus der Managed Security/SOC Services weiterhin Fokus auf Grosskunden, weniger auf dem Mittelstand, dessen Nachfrage überdurchschnittlich wächst.

Managed Security Services – SOC (Midmarket)

Wer diesen Bericht lesen sollte

Im Rahmen dieses Quadranten wird die Relevanz von MSS für Schweizer Mittelständler bewertet; er bietet wertvolle Einblicke zur Auswahl von MSS-Anbietern, die auf die Bekämpfung von Sicherheitsbedrohungen spezialisiert sind. Angesichts der sich ständig weiterentwickelnden Cyberbedrohungen ist der Bedarf an robusten MSS für den Schutz von Unternehmensressourcen und -daten von entscheidender Bedeutung.

Aufgrund des gestiegenen Bewusstseins für Cybersecurity-Risiken, strengerer Vorschriften und der Kosteneffizienz des Outsourcings von Sicherheitsdienstleistungen setzen Schweizer Mittelständler zunehmend auf MSS. Durch die Inanspruchnahme von MSS-Providern können sie sich auf ihre Kernaktivitäten konzentrieren und gleichzeitig die Sicherheitsanforderungen effektiv verwalten.

MSS-Anbieter adressieren diese Nachfrage mit maßgeschneiderten Sicherheitslösungen, die den spezifischen Anforderungen mittelständischer Unternehmen gerecht werden und deren spezifische Risikoprofile und betriebliche Einschränkungen berücksichtigen.

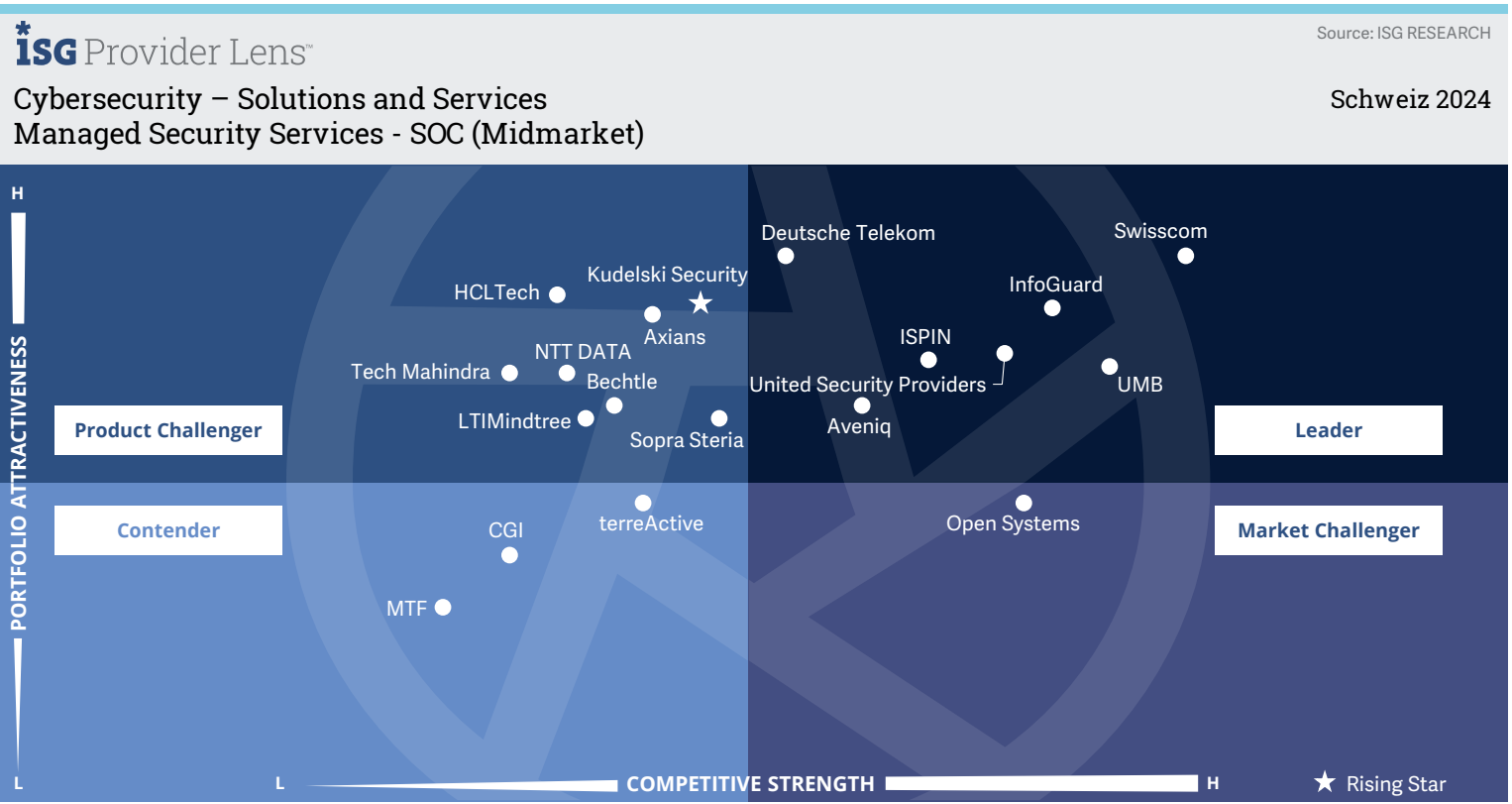
Sie bieten skalierbare Dienste, die mit den Unternehmen mitwachsen und wirksame Sicherheitsmaßnahmen für expandierende Unternehmen beinhalten. Kontinuierliche Überwachungs- und Unterstützungsdienste erkennen Bedrohungen in Echtzeit und reagieren entsprechend darauf, so dass absoluter Schutz gewährleistet ist. Modernste Technologien wie KI und ML verbessern die Erkennung von und Reaktion auf Bedrohungen und wehren so ausgeklügelte Angriffe wirksam ab.

Bei Innovationen auf dem Schweizer MSS-Markt stehen insbesondere die Datensouveränität und der Schutz der Privatsphäre im Mittelpunkt, um die strengen Schweizer Datenschutzgesetze ein- und das Vertrauen erhalten zu können. MSS-Anbieter verfügen über lokales Know-how und kennen die rechtlichen und kulturellen Gegebenheiten in der Schweiz. Sie entwickeln spezielle Lösungen für den Finanzsektor, u.a. mit fortschrittlicher Betrugserkennung und Compliance Management. Schweizer MSS-Anbieter arbeiten auch mit den lokalen für die Cybersecurity zuständigen Behörden zusammen und beteiligen sich an nationalen Initiativen, um ihre Fähigkeiten zum Schutz vor Bedrohungen zu verbessern.

Sicherheitsexperten können anhand der Informationen in diesem Bericht potenzielle MSS-Anbieter bewerten und ihre Fähigkeiten zur wirksamen Bekämpfung von Sicherheitsbedrohungen einschätzen.

Technische Experten können sich mit diesem Bericht über die Landschaft der MSS-Anbieter informieren und Partner identifizieren, die die Sicherheitslage ihres Unternehmens verbessern können.

Beschaffungsexperten hilft dieser Bericht, MSS-Anbieter zu bewerten und fundierte Entscheidungen hinsichtlich der Beschaffung von Managed Security Services zu treffen.



In diesem Quadranten geht es um die **relevantesten** Anbieter von **Managed Security Services aus SOCs** für den Schweizer Mittelstand, ohne Provider, deren Leistungen nur eigene Produkte abdecken. Externer Betrieb mit **„Swissness“** ist zunehmend gefragt.

Frank Heuer

Definition

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

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

Auswahlkriterien

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

Beobachtungen

Der Schweizer Markt für SOC Services wächst insgesamt stark und nimmt besonders im Segment der mittelständischen Unternehmen zu, 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 Managed Security Services durch Security Operations Centers. 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.

Von den 59 Anbietern, die in dieser Studie bewertet wurden, konnten sich 19 für diesen Quadranten qualifizieren. Dabei erreichten sieben eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

AVENIQ

Mit ausgeprägter „Swissness" und starkem Fokus auf die Zielgruppe überzeugt **Aveniq** die mittelständischen SOC-Service-Kunden und profiliert sich als führender Anbieter.

Deutsche Telekom Security schafft es, mit Delivery aus der Schweiz und Verständnis für den Markt als führender Anbieter von Managed Security/SOC-Dienstleistungen für den Schweizer Mittelstand zu überzeugen.

InfoGuard
SWISS CYBER SECURITY

InfoGuard etabliert sich dank grosser Marktreichweite und attraktiver Services als ein führender Anbieter von SOC-Dienstleistungen für mittelständische Unternehmen in der Schweiz.

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

ISPIN erreicht durch einen starken technischen Ansatz sowie die Zusammenführung von Automatisierung und Manpower in Kombination mit „Swissness" eine starke Position im Markt für SOC-Dienstleistungen für den Schweizer Mittelstand.

swisscom

Die **Swisscom** ist mit ausgeprägter „Swissness" der führende Anbieter von Managed Security/ SOC-Dienstleistungen für den Schweizer Mittelstand.

UMB

Dank „Swissness", End-to-End-Services und Fokussierung auf die Zielgruppe erreicht **UMB** eine starke Position im Markt für SOC-Dienstleistungen für Mittelstandskunden in der Schweiz.

United Security Providers

Mit umfangreichen Services und als Teil des grössten Cybersecurity-Clusters der Schweiz zählt **United Security Providers** zu den führenden Anbietern von SOC Services für den Schweizer Mittelstand.

Kudelski Security

Kudelski Security ist mit seinen Lösungen für die reduzierte Komplexität des Security-Managements und seinem Cyber Fusion Center der Rising Star für Managed Security/SOC-Dienstleistungen für den Schweizer Mittelstand.

Leader

"Der Deutschen Telekom gelingt es, mit Verständnis für den Markt auch in der Schweiz als Anbieter von Managed Security/SOC-Dienstleistungen für den Mittelstand zu überzeugen."

Frank Heuer

Deutsche Telekom

Übersicht

Die Deutsche Telekom mit Hauptsitz in Bonn, Deutschland, beschäftigt mehr als 204.200 Mitarbeitende in über 87 Niederlassungen in mehr als 50 Ländern. Im Geschäftsjahr 2023 erwirtschaftete das Unternehmen einen Umsatz von 112,0 Milliarden €. Telekom Security wurde 2020 in eine eigenständige rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom"), innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security rund 1.700 Mitarbeitende. Der Hauptsitz der Deutschen Telekom in der Schweiz befindet sich in Zollikofen. Die Deutsche Telekom betreibt ein SOC in der Schweiz.

Stärken

Services auch aus der Schweiz: Die Deutsche Telekom betreibt Managed Security Services unter anderem in der Schweiz, was besonders von den Mittelstandskunden geschätzt wird. Der Anbieter betreibt zudem hochmoderne Cyber Defense & Security Operations Center und generiert als globaler Carrier umfangreiche Threat Intelligence. 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.

Umfangreiches, wachsendes Portfolio: 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 des Portfolios – die Roadmap zählt zahlreiche Vorhaben auf. Gerade Schweizer Unternehmen legen Wert auf Services, die up-to-date sind. Dies sichert den zukünftigen Erfolg der Deutschen Telekom in der Schweiz.

Ausgeprägtes Geschäftsverständnis: Die Deutsche Telekom verfügt über ein tiefes Verständnis für Businessanforderungen, kann umfangreiche Erfahrung aus Mandaten in verschiedenen Branchen vorweisen und dadurch 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. Das Schwerpunktsegment sind dabei die gehobenen Mittelstandskunden. Mit einem stärkeren Fokus auch auf kleinere Firmenkunden könnte die Deutsche Telekom aufgrund der überdurchschnittlich stark wachsender Nachfrage in diesem Segment noch erfolgreicher sein.

Star of Excellence

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

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

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

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

Durchschnittlicher CX-Wert der Branche

▲ Höchster CX Score: 91.0

▼ Niedrigster CX Score: 64.8

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

Kundenrolle im Unternehmen

▲ **Am zufriedensten**
Information Technology

▼ **Am wenigsten zufrieden**
Human Resources

Region

▲ **Am zufriedensten**
Africa

▼ **Am wenigsten zufrieden**
Eastern Europe

Branche

▲ **Am zufriedensten**
Chemicals

▼ **Am wenigsten zufrieden**
Public sector

Wichtigste CX-Säule

Execution and Delivery

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

Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2024 – Cybersecurity – Solutions and Services" analysiert die entsprechenden Softwareanbieter 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, Dr. Maxime Martelli und Gowtham Sampath

Editor:
Maria Müller-de Haen und Padma Kalyani Mohapatra

Forschungsanalysten:
Monica K

Datenanalysten:
Rajesh Chillappagari und Laxmi Sahebrao

Beratende Berater:
Roger Albrecht

Projektleiter:
Shreemadhu Rai B

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

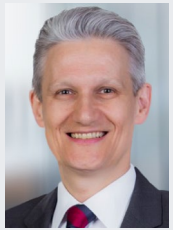
Die in diesem Bericht vorgestellten Marktforschungs- und Analysedaten umfassen Research-Informationen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit.

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

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

Dabei wurde die Studie in folgende Schritte gegliedert:

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



Autor

Frank Heuer
Principal Analyst

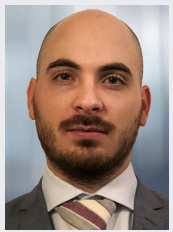
Frank Heuer ist Principal Analyst bei ISG Germany. Sein Schwerpunkt liegt auf den Themen Cybersecurity, Digital Workspace, Communication, Social Business & Collaboration sowie Cloud Computing.

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

Autor (SSE)

Gowtham Kumar Sampath
Assistant Director & Lead Analyst

Gowtham Sampath ist Assistant Director bei ISG Research und verantwortlich für die Erstellung seiner ISG Provider Lens™ Quadrantenberichte für die Bereiche Banking Technology/ Platforms, Digital Banking Services, Cybersecurity sowie Analytics Solutions & Services. Gowtham verfügt über 15 Jahre Marktforschungserfahrung; seine Analysen sollen die Lücke zwischen Datenanalyseanbietern und Unternehmen schließen und gehen auf Marktchancen und Best Practices ein. In dieser Funktion arbeitet er auch mit Beratern zusammen, um branchenübergreifend Ad-Hoc-Anfragen von Unternehmenskunden im Bereich der IT-Services zu adressieren. Darüber hinaus verfasst er Thought Leadership Researcharbeiten, Whitepapers und Artikel über neue Technologien im Bankwesen zu den Themen Automatisierung, Digital und User Experience (DX bzw. UX) sowie über die Auswirkungen der Datenanalyse in diversen Branchen.



Autor (XDR)

Dr. Maxime Martelli

Consulting Manager und Sicherheitsanalyst

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

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

Unternehmenskontext und globaler Überblick

Monica K

Assistant Manager, Lead Research Specialist

Monica K. ist Assistant Manager und Lead Research Specialist und eine Digitalexpertin bei ISG. Sie hat Inhalte für die Provider Lens™-Studien sowie Inhalte aus der Unternehmensperspektive erstellt und ist die Autorin des globalen zusammenfassenden Berichts für den Cybersecurity-, ESG- und Nachhaltigkeitsmarkt. Monica K. verfügt über mehr als ein Jahrzehnt an Erfahrung und Fachwissen in den Bereichen Technologie, Wirtschaft und Marktforschung für ISG-Kunden.

Zuvor war sie bei einem Forschungsunternehmen tätig, wo sie sich auf aufkommende Technologien wie IoT und Produktentwicklung, Anbieterprofile und Talent Intelligence spezialisierte. Zu ihrem Aufgabenbereich gehörte das Management umfassender Forschungsprojekte und die Zusammenarbeit mit internen Stakeholdern bei verschiedenen Beratungsinitiativen.

Sponsor der Studie

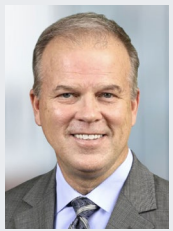
Heiko Henkes

Direktor und leitender Analyst

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

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

IPL-Produktverantwortlicher



Jan Erik Aase

Partner und globaler Leiter - ISG Provider Lens™

Herr Aase verfügt über umfangreiche Erfahrungen bei der Implementierung und Erforschung der Dienstleistungsintegration und des Managements von IT- und Geschäftsprozessen. Mit mehr als 35 Jahren Erfahrung ist er hochqualifiziert in der Analyse von Trends und Methoden der Vendor Governance, der Identifizierung von Ineffizienzen in aktuellen Prozessen und der Beratung der Branche. Jan Erik hat Erfahrungen auf allen vier Seiten des Sourcing- und Vendor-Governance-Lebenszyklus - als Kunde, Branchenanalyst, Dienstleister und Berater. Als Partner und globaler Leiter von ISG Provider Lens™ ist er nun sehr gut positioniert, um den Zustand der Branche zu bewerten, darüber zu berichten und Empfehlungen sowohl für Unternehmen als auch für Kunden von Dienstleistern auszusprechen.

ISG Provider Lens™

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

ISG Research™

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

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

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

ISG

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

Weitere Informationen unter isg-one.com.

ISG Provider Lens™

JULI, 2024

BERICHT: CYBERSECURITY – SOLUTIONS AND SERVICES