ISG Provider Lens™

Cyber Security – Solutions & Services

Switzerland 2021

Quadrant Report

Eine Untersuchung der Information Services Group Germany GmbH

Juni 2021

Customized report courtesy of:

axians

Über diesen Bericht

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 in diesem Bericht zusammengestellten Daten beruhen auf zuletzt im April 2021 aktualisierten Informationen. Zwischenzeitliche Fusionen und Akquisitionen und die damit zusammenhängenden Veränderungen sind in diesem Bericht nicht berücksichtigt.

Der Lead Author für diesen Bericht ist Frank Heuer. Die Research-Analystin ist Monica K und der Data Specialist ist Rajesh C. Die Analystin für den Unternehmenskontext und die globale Zusammenfassung ist Monica K.

ISG Provider Lens™

ISG Provider Lens™

Das ISG Provider Lens™ Programm bietet marktführende, handlungsorientierte Studien, Berichte und Consulting Services, bei denen es insbesondere um die Stärken und Schwächen von Technologieanbietern und Dienstleistern sowie deren Positionierung im Wettbewerbsumfeld geht. Diese Berichte bieten maßgebliche Einsichten, die von unseren Advisors im Rahmen ihrer Beratungstätigkeit bei Outsourcing-Verträgen genutzt werden, aber auch von vielen ISG-Unternehmenskunden, die potentiell als Outsourcer auftreten (z.B. FutureSource).

Weitere Informationen zu unseren Studien sind über ISGLens@isg-one.com, Tel.+49 (0) 561-50697524 oder auf unserer Website unter ISG Provider Lens™ erhältlich.

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.

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 erhältlich.

EXECUTIVE SUMMARY

Allgemeine Trends: Die Covid-19-Pandemie wird sich auch weiterhin auf die Cybersicherheit in der Schweiz auswirken

Sowohl der langfristige Trend zur Digitalisierung als auch die raschen Umbrüche durch die COVID-19-Pandemie haben in der Schweiz zu vergrösserten Angriffsflächen für Cyberangriffe geführt, die entsprechender Gegenmassnahmen bedürfen.

Im Rahmen der Digitalisierung werden Geschäftsprozesse immer mehr in die IT verlagert. Auch geistiges Eigentum der Unternehmen wird immer mehr digital dargestellt. Mit der zunehmenden Notwendigkeit, IT- und Kommunikationssysteme in Unternehmen zu schützen, hat sich IT-Sicherheit zur Unternehmenssicherheit gewandelt. Aktuell bedeutet die Corona-Krise auch weiterhin eine Herausforderung für die IT-Sicherheit, da mit der verstärkten Home-Office-Nutzung – und der dadurch bedingten externen Anbindung der Mitarbeiter – die IT-Systeme leichter angreifbar sind. Da auch nach dem Ende der Pandemie nicht zu erwarten ist, dass alle Arbeitsplätze wieder in die Unternehmen zurückverlagert werden, wird diese Herausforderung voraussichtlich langfristig bestehen.

Cyberkriminelle realisieren in immer kürzeren Abständen neue, raffiniertere und komplexere Methoden, um die Cyberverteidigungssysteme von Unternehmen und Behörden zu überwinden. In den letzten zwölf Monaten waren wieder einige spektakuläre Cyberattacken zu verzeichnen; aber auch nicht so prominente Angriffe – etwa durch Ransomware – machen immer mehr Unternehmen zu schaffen. Entsprechend müssen die Cybersecurity-Massnahmen der Unternehmen und Behörden lückenlos auf dem neuesten Stand sein. Damit sind immer mehr Unternehmen und Behörden nicht zuletzt durch den IT-Fachkräftemangel – speziell im Cybersecurity-Markt – überfordert. Somit wenden sich IT-Verantwortliche und Führungskräfte verstärkt an externe Dienstleister, zum Beispiel Anbieter von Managed Security Services. Diese sowie 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.

Neben dem Eigenschutz zwingen auch gesetzliche Regelungen Unternehmen dazu, stärkere Sicherheitsmassnahmen umzusetzen, um Cyberattacken vorzubeugen. Gerade für mittelständische Unternehmen stellt dies immer noch eine grosse Herausforderung dar.

Der Mittelstand ist andererseits ein interessantes Marktsegment für Cybersecurity-Anbieter. Da Mittelständler insgesamt gesehen weniger ausgereifte IT-Sicherheitssysteme als Grossunternehmen besitzen, aber durch die oben beschriebenen Faktoren zu Nachrüstungen gezwungen sind, haben sie einen grossen Nachholbedarf und verzeichnen dementsprechend eine überdurchschnittlich stark wachsende Nachfrage nach Cybersecurity-Lösungen. Noch vorteilhafter für Anbieter ist eine ausgewogene Kundenstruktur aus Mittelstand und Grossunternehmen, um auch von den grossen Budgets der Large Accounts profitieren zu können.

Trotz der grossen Bedeutung von Cybersicherheit kämpfen IT-Verantwortliche oft mit der Aufgabe, Investitionen in IT-Sicherheit gegenüber Stakeholdern des Unternehmens zu legitimieren, besonders gegenüber dem CFO. Im Unterschied zu anderen IT-Projekten ist es nicht immer möglich, die Rentabilität der Investitionen nachzuweisen; es ist auch nicht einfach, Bedrohungsrisiken zu quantifizieren. Allerdings haben auch immer mehr Führungskräfte erkannt, dass Cyberattacken zu massiven, unter Umständen existenziellen finanziellen und Imageschäden führen können. Somit gewinnt Cybersicherheit in Unternehmen an Bedeutung, und Führungskräfte werden verstärkt in das Cyberrisikomanagement eingebunden.

Auf der anderen Seite liegt das Problem oft nicht (allein) auf der technischen Seite; viele 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.

Trends im Markt für Identity & Access Management (Produkte)

IAM ist aktuell und auch in Zukunft ein besonders wichtiges Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch Maschinen und bestimmte Unternehmensbereiche (Industrie 4.0). Darüber hinaus nimmt die Anzahl der Benutzer, Geräte und Dienste stetig zu und damit auch die Anzahl von digitalen Identitäten, die zu verwalten sind. Ein weiterer Faktor ist der Umzug vieler Mitarbeiter in das Home Office in Folge der Pandemie. Viele Mitarbeiter greifen nun remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden. Auch Themen wie intuitive Schnittstellen, passwortlose Authentifizierung, Einsatz von Biometrie und künstliche Intelligenz gewinnen unter anderem durch die zunehmende Nutzung mobiler Endgeräte an Bedeutung.

Wie im Softwaremarkt insgesamt ist auch hinsichtlich IAM-Lösungen eine Verschiebung vom On-Premise-Betrieb in die Cloud festzustellen. Die meisten Anbieter haben sich darauf eingestellt und bieten sowohl den On-Premise- als auch den Cloudbetrieb (Identity as a Service) an. Auch reine Cloudanbieter treten immer häufiger auf. Darüber hinaus spielen Bundling und Integration eine zunehmende Rolle.

24 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für das Identity & Access Management in der Schweiz identifiziert. Davon konnten sich neun als Leader positionieren: Atos, Ergon, IBM, Microsoft, NEVIS, Okta, Ping Identity, RSA und United Security Providers.

Trends im Markt für Data Leakage / Loss Prevention (Produkte)

Das Interesse in der Schweiz an DLP-Lösungen hat in den letzten Jahren weiter deutlich zugenommen. Dazu tragen verschiedene Faktoren bei, welche die Sicherheit der Daten im Unternehmen berühren. So haben sich Daten und geistiges Eigentum zu immer

wichtigeren und teilweise existentiell bedeutsamen Unternehmens-Assets entwickelt. Immer mehr Cyberkriminelle setzen an diesem Punkt an, um Informationen zu stehlen. Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar (gerade auch während der gegenwärtigen Pandemiesituation), da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen.

Neben der Mobilität und Funktionsvielfalt bei den Endgeräten sind es die IT-Trends Big Data, Social Business und Cloud Computing, die eine Kontrolle der Datenbewegungen deutlich erschweren und hohe Anforderungen an DLP-Lösungen stellen. Soziale Netzwerke und andere Social-Media-Plattformen eröffnen neue Kommunikationskanäle, über die Daten abfliessen können; hinzu kommen die Risiken durch Datentransfers via E-Mail. Aber nicht nur ungewollt können Daten durch das Verschulden von internen Akteuren abfliessen; auch vor ungetreuem Verhalten interner Beteiligter müssen sich Unternehmen schützen können.

Wie im Softwaremarkt insgesamt ist auch hinsichtlich DLP-Lösungen eine Verschiebung vom On-Premise-Betrieb in die Cloud festzustellen. Die meisten Anbieter haben sich darauf eingestellt und bieten sowohl den On-Premise- als auch den Cloudbetrieb an. Darüber hinaus spielen Bundling und Integration eine zunehmende Rolle.

23 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für DLP in der Schweiz identifiziert. Davon konnten sich acht als Leader positionieren: Broadcom, Forcepoint, IBM, Ivanti MobileIron, Matrix42, McAfee, Microsoft und Trend Micro.

Trends im Markt für Advanced Endpoint Threat Protection, Detection & Response (Produkte)

Zum Schutz der Endpoints in Unternehmen vor komplexer werdenden Bedrohungen sollen Lösungen für Advanced Endpoint Threat Protection, Detection & Response dienen. Im Gegensatz zu herkömmlichen Sicherheitslösungen – wie klassischen Antivirus-Lösungen – beruhen sie nicht auf Signaturen, sondern sind proaktiv gegen potenzielle Bedrohungen ausgerichtet, indem sie Verhaltensanalysen sowie Machine Learning beziehungsweise künstliche Intelligenz zur Anwendung bringen. Des Weiteren ist eine kontinuierliche Überwachung der Endpoints möglich.

Die zunehmende Nutzung von Clouddaten und -anwendungen ist bereits seit mehreren Jahren ein zu beobachtender Trend. Gerade aber durch die Pandemie hat sich diese Entwicklung verstärkt; viele Mitarbeiter arbeiten inzwischen von zu Hause aus – und damit ausserhalb der gesicherten Unternehmenssysteme. Damit hat sich die Bedrohungslage zusätzlich verschärft. Dementsprechend interessieren sich immer mehr Unternehmen in der Schweiz für proaktiv und umfassender schützende Advanced-Endpoint-Threat-Protection-, Detection- & Response-Lösungen.

16 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für Advanced Endpoint Threat Protection, Detection &

Response in der Schweiz identifiziert. Davon konnten sich acht als Leader positionieren, und zwar Broadcom, Check Point, CrowdStrike, Kaspersky, Microsoft, Sophos, Trend Micro, VMware Carbon Black.

Trends im Markt für Strategic Security Services

Auch und besonders in diesem Jahr – durch die Corona-Situation und die damit verbundene Arbeitsplatzverlegung in das Home Office – sind Unternehmen in der Schweiz vor vielfältige Herausforderungen gestellt, welche die IT-Sicherheit und den Datenschutz betreffen. Die weiter zunehmende Gefährdungssituation bewirkt zusammen mit mangelnden Ressourcen ein zunehmendes Bedürfnis nach Orientierung hinsichtlich dieser wichtigen Themen. Angesichts der immer intensiveren wie auch 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 im Bereich IT-Security haben gerade die mittelgrossen Unternehmen zu leiden. Der Mittelstand ist damit ein überdurchschnittlich wachsendes – und entsprechend zunehmend attraktives – Marktsegment.

Dienstleister, die ihren Kunden neben Strategic Security Services auch Technical Security Services und Managed Security Services anbieten können, damit die Strategie bruchlos in die Tat umgesetzt werden kann, sind hier im Vorteil. Auch die Fähigkeit, integrierte IT- und dazugehörige Security-Lösungen aus einem Guss anbieten zu können, kann eine höhere Kundenpräferenz bewirken.

ISG Provider Lens™

29 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Dienstleister hinsichtlich Strategic Security Services in der Schweiz identifiziert. Davon konnten sich elf als Leader positionieren: Accenture, Atos, Capgemini, Deloitte, DXC, EY, HCL, IBM, KPMG, PwC und Swisscom.

Trends im Markt für Technical Security Services

Auch 2021 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. Auch unbedachtes Verhalten von Anwendern wird von Kriminellen verstärkt ausgenutzt, z.B. bei Trojaner- und Phishing-Angriffen; es sind auch immer mehr Ransomware-Angriffe zu beobachten. Neben einem zeitgemässen Security Equipment spielen daher auch Schulungen für die Anwender nach wie vor eine wichtige Rolle im Cybersecurity-Konzept von Unternehmen und Behörden. Über diese grundsätzlichen Faktoren hinaus bewirkt die Corona-Pandemie auch weiterhin zusätzlichen externen Unterstützungsbedarf.

IT-Security-Projekte sind häufig anspruchsvoll und vielfältig angelegt. Daher sind hier insbesondere Dienstleister im Vorteil, die ein breites Leistungsspektrum an Technical Security Services aus einer Hand bieten. Auch Partnerschaften mit renommierten Technologieanbietern, zahlreiche hochwertige Zertifizierungen, End-to-End Security Services, integrierte Angebote aus IT- und zugehöriger Security-Lösung sowie – speziell für

Grosskunden – internationale Erfahrung und international vertretene Teams sind von Vorteil.

Mittelständische Unternehmen zeigen nach wie vor besonderen Nachholbedarf hinsichtlich der Modernisierung ihrer IT-Security-Systeme. Diese Situation, verschärfte gesetzliche Regelungen und Fachkräftemangel fördern die Nachfrage nach externer Unterstützung. Mittelständler wissen darüber hinaus häufig die lokale Präsenz der Dienstleister für kurze Wege und unkomplizierte, schnelle Unterstützung zu schätzen.

25 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Dienstleister hinsichtlich Technical Security Services in der Schweiz identifiziert. Davon konnten sich zehn als Leader positionieren: Accenture, Atos, Bechtle, Capgemini, DXC, HCL, IBM, ISPIN, Swisscom und T-Systems.

Trends im Markt für Managed Security Services

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken – sowie die zusätzlichen Herausforderungen durch die Pandemie – fördern besonders auch die Nachfrage nach Managed Security Services. Knappe qualifizierte Ressourcen und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich in den Fokus der Schweizer Unternehmen.

Grosse wie auch mittelständische Kunden wissen Security Operations Centers (SOCs) mit Schweizer Standort aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen. Für beide Zielgruppen sind darüber hinaus auch End-to-End Security Services, integrierte Lösungen aus IT- und zugehöriger Security-Lösung, die Sicherung der Zuverlässigkeit der

Managed Security Services sowie eine hohe Innovationskraft wichtig, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Erweiterung der SOCs hin zu Cyber Defense Centers, indem zunehmend komplexeren Bedrohungen auch mit künstlicher Intelligenz und Automatisierung begegnet wird. Ergänzende Cyber Fusion Centers helfen dabei, das Cybersecurity Management zielgerichtet und zukunftsgerecht auszubauen.

Für grosse Unternehmen spielen aufgrund deren häufig internationaler Präsenz global verteilte SOCs eine besondere Rolle. Diese grossen Firmen legen aufgrund ihrer meist komplexen IT-Security-Systeme oft auch Wert auf ein breites Security-Themenspektrum, das von den Managed Security Services Providern abgedeckt werden muss. Speziell für mittelständische Kunden spielen Ansprechpartner, die die Schweizer Landessprachen beherrschen, in den SOCs eine wichtige Rolle.

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.

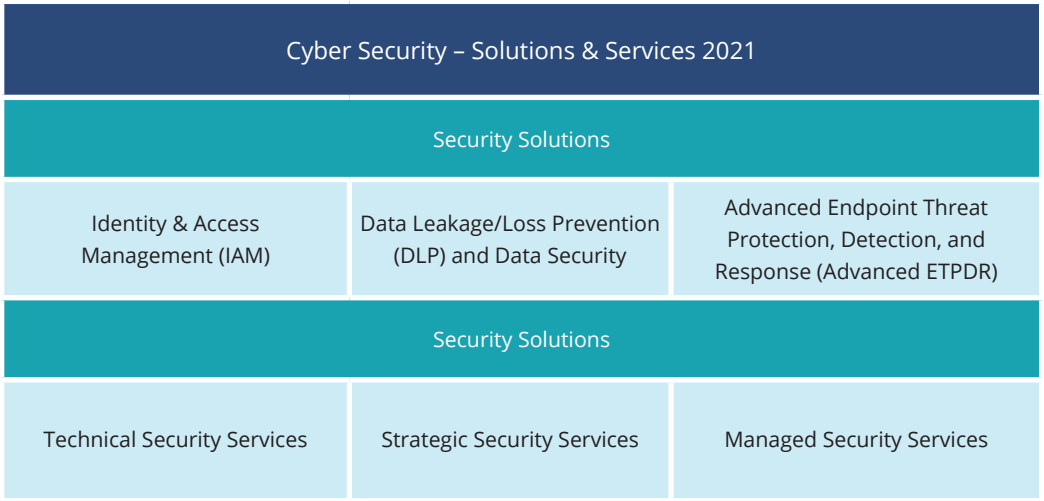
33 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für Managed Security Services in der Schweiz identifiziert. Davon konnten sich vierzehn als Leader positionieren: Accenture, Atos, Aveniq (Avectris), Axians, Capgemini, HCL, IBM, ISPIN, Orange Cyberdefense, Swisscom, T-Systems, TCS, United Security Providers und Wipro.

Einleitung

Marktüberblick

Unternehmen in der Schweiz setzen zügig neue Technologien ein, um die digitale Transformation voranzutreiben, wettbewerbsfähig zu bleiben und den sich ständig ändernden Anforderungen der Endbenutzer gerecht werden zu können. Die zunehmende Verbreitung dieser Technologien sowie neue Tools, die für mehr Effizienz und Geschwindigkeit sorgen, haben zu einer erhöhten Gefährdung und einer wachsenden Angriffsfläche geführt. Ransomware, Advanced Persistent Threats und Phishing-Angriffe stellten sich 2020 als die schlimmsten Cyber-Bedrohungen heraus. Führende Unternehmen, darunter Experian, SolarWinds, Zoom, Magellan Health, Finastra und Marriott, sahen sich im letzten Jahr Cyberangriffen durch Hacking, bösartigen Code und Ransomware ausgesetzt.

Simplified illustration



Source: ISG 2021

Definition

Betrachtungsumfang der Studie

Im Rahmen der ISG Provider Lens™-Studie „Cybersecurity - Solutions & Services 2021“ werden die folgenden Regionen in sechs Quadranten analysiert:

	USA	UK	Nordische	Deutschland	Schweiz	Frankreich	Brasilien	Australien
Identity and Access Management (IAM)	✓	✓	✓	✓	✓	✓	✓	✓
Data Leakage/Loss Prevention (DLP) and Data Security	✓	✓	✓	✓	✓	✓	✓	✓
Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	✓	✓	✓	✓	✓	✓	✓	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	✓	✓	✓
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓
Managed Security Services (MSS)	✓	✓	✓	✓	✓	✓	✓	✓

Definition

Die vorliegende Studie untersucht sechs Themenbereiche im Schweizer Markt für Cybersecurity. Die wesentliche Unterscheidung hinsichtlich der in dieser Studie untersuchten Themen betrifft die Differenzierung von Security Solutions und Security Services.

Die Security Solutions umfassen in dieser Studie Software und Cloud Services von Produktanbietern auf Basis eigener Software. Die betrachteten Themen sind Identity & Access Management (IAM), Data Leakage/Loss Prevention (DLP) sowie Advanced Endpoint Threat Protection, Detection & Response. IAM-Lösungen dienen der Erfassung, Aufzeichnung und Verwaltung von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets, einschliesslich Privileged Access Management. DLP-Lösungen sind in der Lage, sensible Daten zu erkennen, Richtlinien durchzusetzen, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern. Lösungen für Advanced Endpoint Threat Protection, Detection & Response gehen über einen reinen signaturbasierten Schutz hinaus und bieten Schutz vor Angriffen wie Ransomware, Advanced Persistent Threats und Malware; zu diesem Zweck werden Vorfälle über alle Endpunkte hinweg untersucht.

Security Services betreffen Dienstleistungen für Security-Lösungen, die sich nicht ausschliesslich auf die jeweiligen proprietären Produkte konzentrieren. Diese Kategorie umfasst Strategic Security Services, Technical Security Services und Managed Security Services. Strategic Security Services umfassen in erster Linie die Beratung für IT-Sicherheit. Technical Security Services beinhalten Integration, Wartung und Support von IT-Sicherheitsprodukten oder -lösungen. Unter Managed Security Services fallen Betrieb und Management von IT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center.

ISG Provider Lens™ Kategorien

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 der Unternehmenskunden und das Spektrum der auf dem lokalen Markt tätigen IT-Anbieter ausreichend groß ist, erfolgt eine weitere Differenzierung der IT-Anbieter nach Leistung 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 ihres Schwerpunktes positioniert. Im Ergebnis wird gegebenenfalls zwischen zwei Kundengruppen unterschieden, die wie folgt definiert werden:

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

ISG Provider Lens™ Kategorien

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.

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

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.

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.

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.

ISG Provider Lens™ Kategorien

der Quadrant einer ISG Provider Lens™ Studie kann auch einen Anbieter beinhalten, der nach Meinung von ISG großes Potential hat, eine Leader-Position zu erreichen, und als „Rising Star" klassifiziert werden kann. Anzahl Anbieter pro Quadrant: ISG bewertet und positioniert die wichtigsten Anbieter entsprechend des Betrachtungsumfangs der jeweiligen Studie; die Anzahl der pro Quadrant positionierten Anbieter ist auf 25 begrenzt (Ausnahmen sind möglich).

Rising Star

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.

Bewertung nach Kategorien 1 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	Not in	Contender	Not in	Not in	Not in	Not in
Accenture	Not in	Not in	Not in	Leader	Leader	Leader
All for One Group	Not in	Not in	Not in	Market Challenger	Contender	Not in
Atos	Leader	Not in	Not in	Leader	Leader	Leader
Aveniq (Avectris)	Not in	Not in	Not in	Contender	Product Challenger	Leader
Axians	Not in	Not in	Not in	Product Challenger	Product Challenger	Leader
Bechtle	Not in	Not in	Not in	Leader	Contender	Product Challenger
Bitdefender	Not in	Not in	Product Challenger	Not in	Not in	Not in
BlackBerry Cylance	Not in	Not in	Contender	Not in	Not in	Not in
Brainloop	Not in	Product Challenger	Not in	Not in	Not in	Not in
Broadcom	Product Challenger	Leader	Leader	Not in	Not in	Not in
Capgemini	Not in	Not in	Not in	Leader	Leader	Leader
CGI	Not in	Not in	Not in	Product Challenger	Product Challenger	Contender
Check Point	Not in	Not in	Leader	Not in	Not in	Not in
Cisco	Not in	Not in	Contender	Not in	Not in	Not in

Bewertung nach Kategorien 2 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Clearswift	Not in	Market Challenger	Not in	Not in	Not in	Not in
Cognizant	Not in	Not in	Not in	Contender	Product Challenger	Product Challenger
CoSoSys	Not in	Market Challenger	Not in	Not in	Not in	Not in
CrowdStrike	Not in	Not in	Leader	Not in	Not in	Not in
CyberArk	Product Challenger	Not in	Not in	Not in	Not in	Not in
Cybereason	Not in	Not in	Product Challenger	Not in	Not in	Not in
CyberProof	Not in	Not in	Not in	Not in	Not in	Product Challenger
Deloitte	Not in	Not in	Not in	Product Challenger	Leader	Product Challenger
DeviceLock	Not in	Product Challenger	Not in	Not in	Not in	Not in
Digital Guardian	Not in	Product Challenger	Not in	Not in	Not in	Not in
DXC	Not in	Not in	Not in	Leader	Leader	Product Challenger
Ergon	Leader	Not in	Not in	Not in	Not in	Not in
ESET	Not in	Not in	Contender	Not in	Not in	Not in
EY	Not in	Not in	Not in	Not in	Leader	Not in
FireEye	Not in	Not in	Product Challenger	Not in	Not in	Not in

Bewertung nach Kategorien 3 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Forcepoint	Not in	Leader	Not in	Not in	Not in	Not in
ForgeRock	Product Challenger	Not in	Not in	Not in	Not in	Not in
Fortinet	Contender	Not in	Not in	Not in	Not in	Not in
GBS	Not in	Product Challenger	Not in	Not in	Not in	Not in
Google DLP	Not in	Contender	Not in	Not in	Not in	Not in
HCL	Not in	Not in	Not in	Leader	Leader	Leader
IBM	Leader	Leader	Not in	Leader	Leader	Leader
InfoGuard	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger
Infosys	Not in	Not in	Not in	Contender	Not in	Not in
ISPIN	Not in	Not in	Not in	Leader	Product Challenger	Leader
Ivanti MobileIron	Not in	Leader	Not in	Not in	Not in	Not in
Kaspersky	Not in	Not in	Leader	Not in	Not in	Not in
KPMG	Not in	Not in	Not in	Not in	Leader	Not in
Kudelski	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger
Lumen	Not in	Not in	Not in	Not in	Not in	Product Challenger

Bewertung nach Kategorien 4 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Matrix42	Market Challenger	Leader	Product Challenger	Not in	Not in	Not in
McAfee	Not in	Leader	Product Challenger	Not in	Not in	Not in
Micro Focus	Product Challenger	Not in	Not in	Not in	Not in	Not in
Microsoft	Leader	Leader	Leader	Not in	Not in	Not in
Netskope	Not in	Product Challenger	Not in	Not in	Not in	Not in
NEVIS	Leader	Not in	Not in	Not in	Not in	Not in
Nexus	Product Challenger	Not in	Not in	Not in	Not in	Not in
NTT	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger
Okta	Leader	Not in	Not in	Not in	Not in	Not in
One Identity	Contender	Not in	Not in	Not in	Not in	Not in
OneLogin	Product Challenger	Not in	Not in	Not in	Not in	Not in
Open Systems	Not in	Not in	Not in	Not in	Not in	Market Challenger
OpenText	Not in	Product Challenger	Not in	Not in	Not in	Not in
Oracle	Market Challenger	Not in	Not in	Not in	Not in	Not in
Orange Cyberdefense	Not in	Not in	Not in	Market Challenger	Product Challenger	Leader

Bewertung nach Kategorien 5 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Palo Alto Networks	Not in	Not in	Contender	Not in	Not in	Not in
Ping Identity	Leader	Not in	Not in	Not in	Not in	Not in
Proofpoint	Not in	Market Challenger	Not in	Not in	Not in	Not in
PwC	Not in	Not in	Not in	Not in	Leader	Not in
RSA	Leader	Not in	Not in	Not in	Not in	Not in
SailPoint	Product Challenger	Not in	Not in	Not in	Not in	Not in
SAP	Market Challenger	Not in	Not in	Not in	Not in	Not in
Saviynt	Product Challenger	Not in	Not in	Not in	Not in	Not in
SecureTrust	Not in	Product Challenger	Not in	Not in	Not in	Not in
Secureworks	Not in	Not in	Not in	Not in	Product Challenger	Product Challenger
Solarwinds	Contender	Not in	Not in	Not in	Not in	Not in
Sophos	Not in	Not in	Leader	Not in	Not in	Not in
Sopra Steria	Not in	Not in	Not in	Not in	Market Challenger	Product Challenger
Swisscom	Not in	Not in	Not in	Leader	Leader	Leader
TCS	Not in	Not in	Not in	Product Challenger	Product Challenger	Leader

Bewertung nach Kategorien 6 von 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
terreActive	Not in	Not in	Not in	Not in	Not in	Contender
Thales	Contender	Not in	Not in	Not in	Not in	Not in
Trend Micro	Not in	Leader	Leader	Not in	Not in	Not in
Trustwave	Not in	Not in	Not in	Not in	Not in	Product Challenger
T-Systems	Not in	Not in	Not in	Leader	Not in	Leader
UMB	Not in	Not in	Not in	Not in	Not in	Product Challenger
Unisys	Not in	Not in	Not in	Market Challenger	Market Challenger	Market Challenger
United Security Providers	Leader	Not in	Not in	Not in	Not in	Leader
Varonis	Not in	Product Challenger	Not in	Not in	Not in	Not in
Verizon	Not in	Not in	Not in	Not in	Product Challenger	Product Challenger
VMware Carbon Black	Not in	Not in	Leader	Not in	Not in	Not in
WatchGuard	Not in	Product Challenger	Not in	Not in	Not in	Not in
Wipro	Not in	Not in	Not in	Product Challenger	Product Challenger	Leader
Zensar	Not in	Not in	Not in	Contender	Contender	Contender
Zscaler	Not in	Contender	Not in	Not in	Not in	Not in

Cyber Security – Solutions & Services Quadrants

ENTERPRISE CONTEXT

Identity & Access Management (IAM)

Dieser Bericht ist für Unternehmen aller Branchen in der Schweiz relevant und bewertet die Leistungen von Lösungsanbietern im Hinblick auf Software und zugehörige Dienstleistungen, die die besonderen Anforderungen an die sichere Verwaltung von Benutzeridentitäten und Geräten in Unternehmen erfüllen.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von IAM-Anbietern in der Schweiz dargelegt und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen. Durch die zunehmende Nutzung des Bring-Your-Own-Device-Modells können Kriminelle leichter auf Geräte zugreifen, was entsprechende Sicherheitsrisiken nach sich zieht. Daher bevorzugen Unternehmen IAM-Lösungen, die einen hohen Automatisierungsgrad aufweisen und dabei helfen, auf Basis von ML-Algorithmen eine vorfallbasierte Rangfolge auszulösen und zu verwalten.

Da auch Unternehmen in der Schweiz für einen erfolgreichen Handel mit EU-Ländern die EU-Vorschriften einhalten müssen, nutzen sie gerne fertige Richtlinien-Templates, die die EU-Datenschutzbestimmungen besser gewährleisten.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Anbieter identifizieren und evaluieren:

IT- und Technologie-Verantwortliche gewinnen durch diesen Bericht ein klares Verständnis der relativen Positionierung und der Fähigkeiten von IAM-Lösungsanbietern und -Dienstleistern. Der Bericht vergleicht auch die technischen Leistungen verschiedener Provider im Markt.

Sicherheitsexperten sollten diesen Bericht lesen, um zu verstehen, wie Anbieter und ihre IAM-Tools die Sicherheits- und regionalen Gesetze einhalten und wie diese Akteure miteinander verglichen werden können.

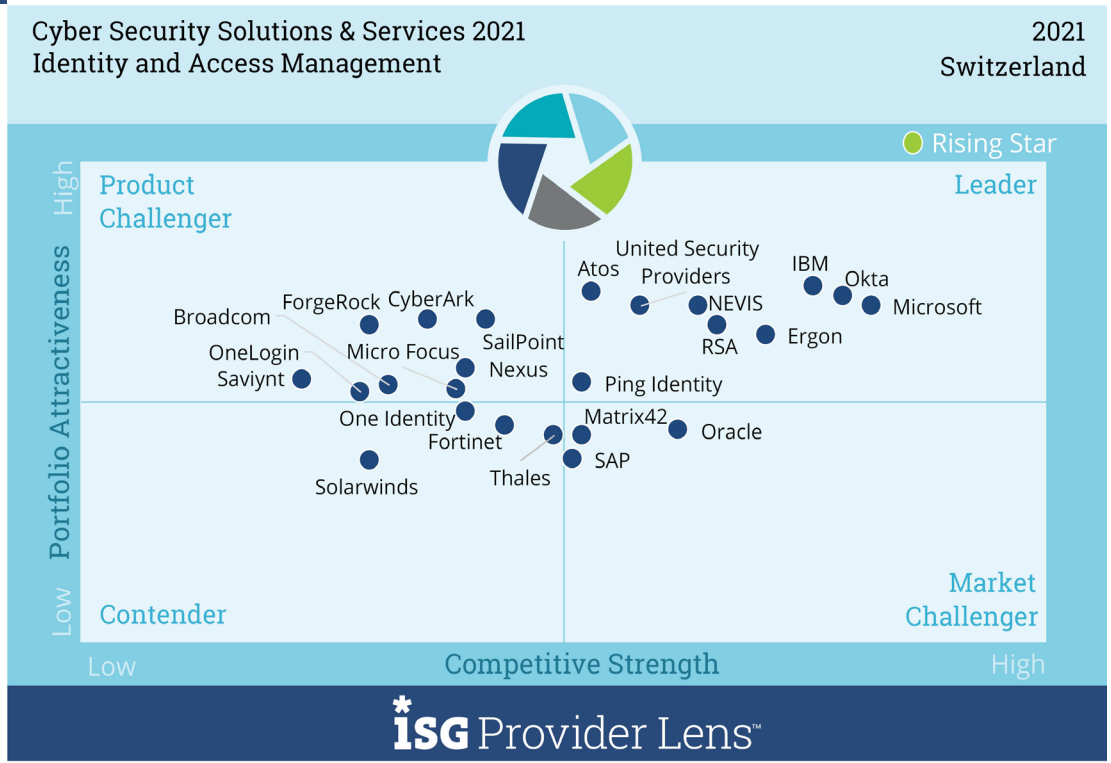
Compliance- und Governance-Verantwortliche hilft dieser die IAM-Landschaft zu verstehen, da sie sich direkt auf die Einhaltung der daten- und datenschutzrechtlichen Vorschriften der Region auswirkt.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Definition

IAM-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die spezifische und sichere Verwaltung von Benutzeridentitäten und -geräten in Unternehmen. Dieser Quadrant umfasst auch Software-as-a-Service Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine IAM-Produkte (on-premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. Entsprechend der individuellen Unternehmensanforderungen können diese den auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in der Cloud (vom Kunden verwaltet), auf Basis eines as-a-Service-Modells oder in Form einer kombinierten Lösung.

IAM-Lösungen dienen der Erfassung, Aufzeichnung und Verwaltung von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets, einschliesslich Privileged



Source: ISG Research 2021

IDENTITY AND ACCESS MANAGEMENT (IAM)

Definition

Access Management (PAM). Sie stellen sicher, dass die Zugriffsrechte entsprechend definierten Richtlinien gewährt werden. Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungen 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 Features im Zusammenhang mit Social Media und mobilen Anwendern erwartet, um deren Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen.

Auswahlkriterien

- Relevanz (Umsatz und Anzahl der Kunden) als IAM-Produktanbieter in der Schweiz
- IAM-Angebote sollen auf proprietärer Software und nicht auf Software von Drittanbietern beruhen.
- Die Lösung sollte entweder vor Ort, in der Cloud, als Identity as a Service (IDaaS), in einem verwalteten Modell (eines Drittanbieters) oder in einer Kombination davon eingesetzt werden können.
- Die Lösung sollte die Authentifizierung anhand von Single Sign-on (SSO), Multifaktor-Authentifizierung (MFA), risiko- und kontextbasierten Modellen oder einer Kombination aus diesen Ansätzen unterstützen.
- Die Lösung sollte rollenbasierten Zugriff und Privileged Access Management (PAM) unterstützen.
- Der IAM-Anbieter sollte Zugriffsmanagement für eine oder mehrere Unternehmensanforderungen wie Cloud, Endpunkte, mobile Geräte, Anwendungsprogrammierschnittstellen (APIs) und Webanwendungen offerieren.
- Die Lösung sollte einen oder mehrere ältere und neuere IAM-Standards unterstützen, einschliesslich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM.
- Zur Unterstützung durch einen sicheren Zugriff sollte das Portfolio eine oder mehrere der folgenden Möglichkeiten bieten: Directory-Lösungen, Dashboard- oder Self-Service-Management und Lifecycle Management (Migration, Synchronisierung und Replizierung).

IDENTITY AND ACCESS MANAGEMENT (IAM)

Beobachtungen

IAM präsentiert sich in der Schweiz auch 2021 als ein besonders wichtiges Cybersecurity-Thema und wird weiterhin ein bedeutendes Thema sein. Hierfür sprechen mehrere Gründe.

Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch Maschinen und bestimmte Unternehmensbereiche (Schlagwort: Industrie 4.0). Die Sicherung der Identität wird in Zukunft die Grundlage darstellen, um überhaupt digitale Systeme und die Vernetzung untereinander sicherzustellen. Darüber hinaus nimmt die Anzahl der Benutzer, Geräte und Dienste stetig zu und damit auch die Anzahl von digitalen Identitäten, die zu verwalten sind. Dabei ist es in Zeiten der permanenten Bedrohung der Daten durch Cyberangriffe umso wichtiger, eine wirksame und effiziente Kontrolle des Identitätsmanagements zu gewährleisten. Digitale Identitäten sind dabei der Schlüssel zu Daten, Geräten und Diensten, deshalb müssen diese besonders gesichert werden.

Ein weiterer Faktor ist eine aktuelle Situation, die sicherlich auch langfristige Auswirkungen haben wird. In Folge der COVID-19-Pandemie sind viele Mitarbeiter in das Home Office umgezogen und greifen nun remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden. Mit der verstärkten Arbeit aus dem Home Office wurde auch der Zugriff von mobilen Endgeräten nochmals forciert; dies resultiert in nochmals grösseren Sicherheits- bei gleichzeitig höheren Komfortanforderungen. Daher gewinnen Themen wie intuitive Schnittstellen, passwortlose Authentifizierung sowie der Einsatz von Biometrie und künstlicher Intelligenz an Bedeutung.

Darüber hinaus werden Unternehmensanwendungen und -daten immer mehr in die Cloud migriert. Dies erfordert IAM-Lösungen, die auch Cloudanwendungen absichern können.

Wie im Softwaremarkt insgesamt ist auch hinsichtlich IAM-Lösungen eine Verschiebung vom On-Premise-Betrieb in die Cloud festzustellen. Die meisten Anbieter haben sich darauf eingestellt und offerieren sowohl den On-Premise- als auch den Cloudbetrieb (Identity as a Service) an. Auch reine Cloudanbieter treten immer häufiger auf, allen voran der US-amerikanische Anbieter Okta. Oktas zunehmender Erfolg auch in der Schweiz zeigt, dass die Kunden immer mehr den bequemen Betrieb auch von Security-Lösungen aus der Cloud zu schätzen wissen. Ein wesentlicher Faktor ist dabei die Erschliessung neuer Zielgruppen; die IAM-Nutzung ist durch den Betrieb in der Cloud auch für kleine und mittelständische Unternehmen, die mit dem Eigenbetrieb häufig überfordert wären, problemlos möglich geworden.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Beobachtungen

Darüber hinaus spielen Bundling und Integration eine zunehmende Rolle. Microsoft setzt dieses Rezept seit einigen Jahren auch erfolgreich im IAM-Markt um und hat seine Marktposition inzwischen deutlich ausgebaut.

24 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für das Identity & Access Management in der Schweiz identifiziert. Davon konnten sich neun als Leader positionieren.

- Die Lösung von **Atos** bietet eine hohe Performance. Zudem überzeugt das vielseitige und flexible Portfolio von Atos für Identity- & Access-Management-Lösungen viele Anwender.
- **Ergon** offeriert vielseitige Authentifizierungsmöglichkeiten und profiliert sich mit einer leistungsfähigen Lösung sowie IAM „made in Switzerland“.
- **IBM** verfügt über eine hohe Marktpräsenz und kann mit hoher Performance, einem breiten Funktionsspektrum und hoher Integrationsfähigkeit punkten.
- **Microsofts** IAM-Lösungen lassen sich sehr gut in bestehende Microsoft-IT-Landschaften integrieren. Darüber hinaus baut Microsoft seine Position im IAM-Markt mit bewährten Marketingrezepten, aber auch technologischen Verbesserungen aus.
- **NEVIS** überzeugt unter anderem mit seiner Swissness auch anspruchsvollste Kunden.
- Mit seinem cloudbasierten Ansatz baut **Okta** seine Position im Schweizer Markt für Identity & Access Management immer weiter aus. Zudem gab der Anbieter Im März 2021 die Übernahme des Mitbewerbers Auth0 bekannt.
- **Ping Identity** baut seine Marktpräsenz auch in der Schweiz weiter aus und schafft so der Sprung unter die führenden IAM-Anbieter.
- **RSA** besitzt weiterhin einen starken Footprint im Schweizer Markt für IAM-Lösungen. Von der hohen Leistungsfähigkeit der RSA SecurID Suite profitieren zudem RSA und seine Kunden.
- **United Security Providers** bietet Swissness und eine umfangreiche IAM-Lösung, die den Kunden eine grosse Auswahl an Betriebsmodellen offeriert.

ENTERPRISE CONTEXT

Data Leakage/Loss Prevention (DLP) & Data Security

Dieser Bericht ist für Unternehmen aller Branchen in der Schweiz relevant, um Anbieter von DLP- und Datensicherheits-Produkten zu bewerten.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern dargelegt, die DLP-Produkte für Schweizer Unternehmenskunden offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen.

Durch die COVID-19-Pandemie ist das Arbeiten von zu Hause aus zur neuen Normalität geworden. Infolgedessen ist es von entscheidender Bedeutung, eine sichere mobile Belegschaft zu gewährleisten, Sicherheit in Bring-Your-Own-Device-Umgebungen (BYOD) durchzusetzen sowie Daten auf entfernten Cloud-Systemen zu sichern.

Unternehmen sind auf der Suche nach DLP-Lösungen, die Schutz und Compliance für personenbezogene Daten, Schutz des geistigen Eigentums und Datentransparenz bieten können. Bei diesen Enterprise-DLP-Lösungen handelt es sich um umfassende Softwarepakete für physische und virtuelle Lösungen. Die steigende Anzahl digitaler Assets in Unternehmen hat zu einem massiven Anstieg an strukturierten und unstrukturierten Daten geführt. Daher investieren große Unternehmen aktiv in DLP-Lösungen. Die Funktionalitäten der digitalen DLP-Lösungen werden auf die Cloud und den erweiterten Schutz vor Bedrohungen ausgeweitet.

In der Schweiz ist der Markt für Cybersecurity ausgereift und wird von globalen wie auch lokalen Akteuren umkämpft. Der Einsatz von DLP-Lösungen wächst mit der Notwendigkeit, Daten in Übereinstimmung mit Datenschutzregeln wie der General Data Protection Regulation (GDPR) zu sichern.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Anbieter identifizieren und evaluieren:

Chief Information Security Officers (CISOs) erhalten durch diesen Bericht ein besseres Verständnis der Produkte von DLP-Anbietern und ihrer relativen Position sowie individuellen Stärken, um so die Informations- und Datensicherheit des Unternehmens zu gewährleisten.

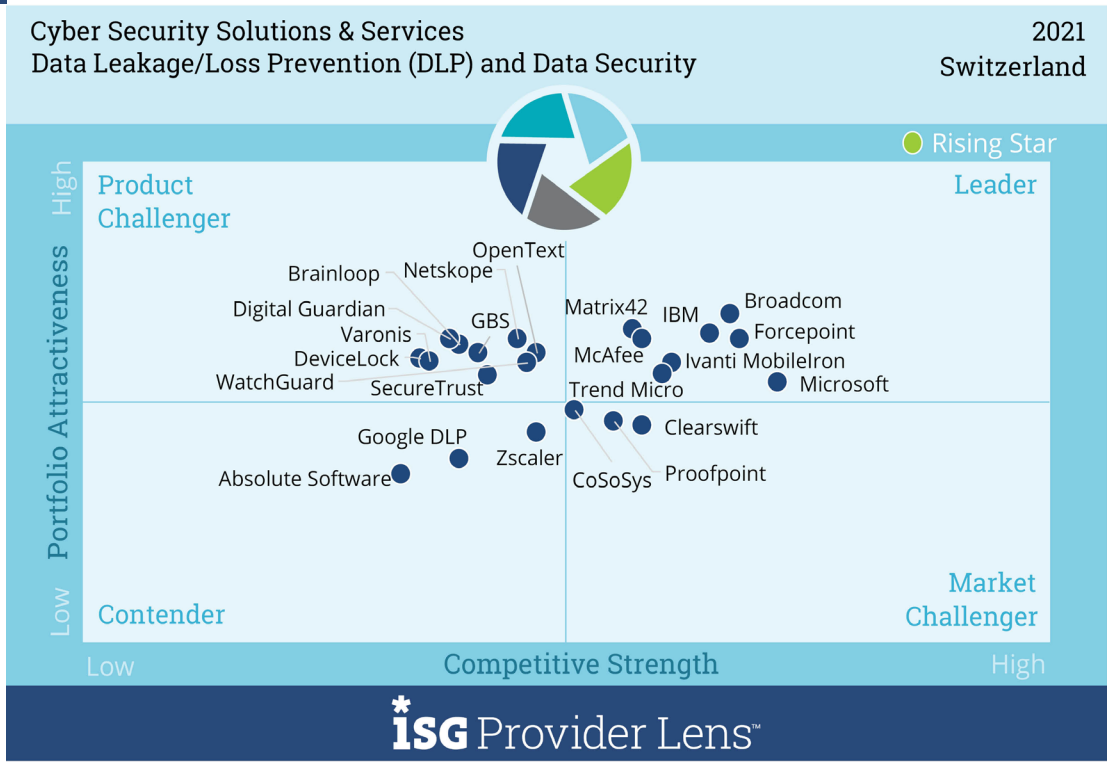
Chief Security Officers (CSOs) werden mit diesem Bericht über die relative Positionierung und die Fähigkeiten von Anbietern informiert, so dass sie bei der Planung und Auswahl einer DLP-Lösung effektiv vorgehen können. Der Bericht zeigt zudem auf, wie Produkt- und Marktfähigkeiten eines Anbieters im Vergleich zum Mitbewerb dastehen.

Sicherheitsarchitekten sollten diesen Bericht lesen, um zu verstehen, wie Anbieter von DLP-Lösungen im Vergleich zu anderen Anbietern zu ihren Initiativen und Bedürfnissen passen.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition

DLP-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine DLP-Produkte (on-premise oder cloudbasiert) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. DLP-Lösungen sind Angebote, die sensible Daten identifizieren und überwachen können, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste verhindern. Die Lösungen der Anbieter in diesem Markt bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf anderen Geräten gewährleisten.



Source: ISG Research 2021

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition

Diese Lösungen sollten in der Lage sein, sensible Daten zu erkennen, Richtlinien durchzusetzen, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern. Sie gewinnen erheblich an Bedeutung, da es für Unternehmen schwieriger geworden ist, Datenbewegungen und -übertragungen zu kontrollieren. Die Zahl der Geräte, auch der mobilen, die zur Datenspeicherung genutzt werden, nimmt in Unternehmen zu. Sie sind meistens mit einer Internetverbindung ausgestattet und können Daten senden und empfangen, ohne diese über ein zentrales Internet-Gateway zu leiten. Die Geräte sind mit einer Vielzahl von Schnittstellen für den Datenaustausch ausgestattet, z.B. USB-Ports, Bluetooth, Wireless Local Area Network (WLAN) und Near-Field Communication (NFC). Datensicherheitslösungen schützen Daten vor unberechtigtem Zugriff, Offenlegung oder Diebstahl.

Auswahlkriterien

- Relevanz (Umsatz und Anzahl der Kunden) als DLP-Produktanbieter in der Schweiz
- DLP-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
- Die Lösung sollte DLP über eine beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt unterstützen.
- Die Lösung sollte sensible Daten schützen, egal ob es sich dabei um strukturierte oder unstrukturierte Daten, Text- oder Binärdaten handelt.
- Die Lösung sollte mit grundlegendem Management-Support angeboten werden, einschliesslich, aber nicht nur, Reporting, Richtlinienkontrolle, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Beobachtungen

Das Interesse der Unternehmen in der Schweiz an DLP-Lösungen hat in den letzten Jahren weiter deutlich zugenommen. Dazu tragen verschiedene Faktoren bei, welche die Sicherheit der Daten im Unternehmen berühren. Daten und geistiges Eigentum sind immer wichtigere und teilweise existentiell bedeutsame Assets von Unternehmen geworden. Der Verlust und das Durchsickern von Daten können schwerwiegende Folgen für den Ruf und das Bestehen eines Unternehmens haben. Immer mehr Cyberkriminelle setzen an diesem Punkt an, um Informationen zu stehlen.

Die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar – zunehmend gerade auch während der gegenwärtigen Pandemiesituation. Diese Clients entziehen sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration und dürfen teilweise auch aus rechtlichen Gründen (Datenschutz) nicht umfassend betrieblich überwacht werden. DLP-Lösungen müssen diese Einschränkungen bei der Kontrolle berücksichtigen, ohne betriebliche Sicherheitslücken zuzulassen.

Neben der Mobilität und Funktionsvielfalt bei den Endgeräten sind es die IT-Trends Big Data, Social Business und Cloud Computing, die eine Kontrolle der Datenbewegungen deutlich erschweren und hohe Anforderungen an DLP-Lösungen stellen. Die enorm wachsende Menge an Daten macht leistungsfähige DLP-Lösungen erforderlich, die die Daten schnell aufspüren, klassifizieren und entsprechend ihrem Schutzbedarf vor unerlaubten Aktionen wie Kopieren oder Verschieben schützen. Cloudspeicherlösungen und Cloud Apps führen dazu, dass Daten bei der Verarbeitung unter Umständen ungewollt das Firmennetzwerk verlassen. Dabei besteht auch die Gefahr, dass betriebliche Daten in private Cloudspeicherdienste übertragen werden. Soziale Netzwerke und andere Social-Media-Plattformen eröffnen neue Kommunikationskanäle, über die Daten abfliessen können; hinzu kommen die Risiken durch Datentransfers via E-Mail. Aber nicht nur ungewollt können Daten durch das Verschulden von internen Akteuren abfliessen; auch vor ungetreuem Verhalten interner Beteiligter müssen sich Unternehmen schützen können.

23 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für DLP in der Schweiz identifiziert. Davon konnten sich acht als Leader positionieren.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Beobachtungen

- **Broadcom** unterstützt seine Kunden durch Zentralisierung und Vereinheitlichung. Zur Spitzenposition von Broadcom im Schweizer DLP-Markt trägt auch die umfangreiche und innovative Lösung des Anbieters bei.
- Francisco Partners hat im Januar 2021 **Forcepoint** übernommen. Offenbar wurde auch das Private-Equity-Unternehmen von den Leistungen Forcepoints – wie der effektiven Entlastung der Kunden bei Data-Leakage- und Data-Loss-Themen – überzeugt.
- Die DLP-Lösung von **IBM** zeichnet sich durch ihre hohe Integrationsfähigkeit aus. Darüber hinaus vereint IBM seine zukunftsweisende Data-Loss-/ Data-Leakage-Prevention-Lösung mit hoher Marktpräsenz.
- Im Dezember 2020 hat Ivanti die Akquise von MobileIron abgeschlossen Die Spezialisierung auf das zukunftsweisende Thema mobile Datensicherheit hat MobileIron offenbar von dem nun **Ivanti MobileIron** genannten Unternehmen überzeugt.
- **Matrix42** offeriert einen umfassenden professionellen Service und Support. Darüber hinaus bietet Matrix42 eine anwenderfreundliche und effiziente DLP-Lösung an, die über ein sehr breites Funktionsspektrum verfügt.
- Im März 2021 hat **McAfee** den Verkauf seiner Geschäftskundensparte an die Symphony Technology Group angekündigt. Möglicherweise überzeugte das Private-Equity-Unternehmen auch das vielseitige Delivery und das breite Leistungsspektrum des McAfee DLP-Angebots.
- Auch im DLP-Markt profitiert **Microsoft** von seiner grossen Marktpräsenz, und mit geschicktem Marketing gelingt es dem Anbieter, seine Position im Markt für DLP-Lösungen weiter auszubauen.
- In der Schweiz verfügt **Trend Micro** über viele Vertriebspartner. Zum Erfolg im DLP-Markt tragen auch die Integrierbarkeit sowie die einfache Einführung und Anwendung seiner DLP-Lösung bei.

ENTERPRISE CONTEXT

Advanced Endpoint Threat Protection, Detection & Response

Dieser Bericht ist für Unternehmen jeglicher Branchen in der Schweiz relevant, um Anbieter von hoch entwickelten Endpoint Threat Protection, Detection & Response Produkte zu evaluieren.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern dargelegt, die hoch entwickelte Endpoint Threat Protection, Detection & Response Produkte für Schweizer Unternehmenskunden offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen.

Unternehmen von heute benötigen einen hohen Schutz gegen immer raffiniertere Bedrohungen. Zusätzlich zur Erkennung von und Reaktion auf Bedrohungen an den Endpunkten umfassen fortschrittliche Endpunkt-Sicherheitslösungen künstliche Intelligenz (KI), maschinelles Lernen (ML), Sicherheitsanalysen und Echtzeit-Bedrohungsdaten.

Laut Aussagen von Schweizer Unternehmen und Organisationen haben Cyberangriffe zugenommen; in Reaktion auf die eskalierende Bedrohungslage sind höhere Ausgaben für die Cyberabwehr geplant. Der Fachkräftemangel ist eine große Herausforderung für Unternehmen. Die Integration in Security Operations Centers, Security Information and Event Management (SIEM)-Lösungen und Security Orchestration, Automation & Response (SOAR)-Prozesse ist keineswegs trivial, sondern eine anspruchsvolle Aufgabe.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Anbieter identifizieren und evaluieren:

Chief Information Security Officers (CISOs) erhalten durch diesen Bericht ein besseres Verständnis der Produkte von Anbietern für fortschrittliche Endpunkt-Sicherheit und ihrer relativen Position sowie individuellen Stärken, um so die Informations- und Datensicherheit des Unternehmens zu gewährleisten.

Chief Security Officers (CSOs) werden mit diesem Bericht über die relative Positionierung und die Fähigkeiten von Anbietern informiert, so dass sie bei der Planung und Auswahl einer hochentwickelten Unified Endpoint Management Lösung effektiv vorgehen können. Der Bericht zeigt zudem auf, wie Produkt- und Marktfähigkeiten eines Anbieters im Vergleich zum Mitbewerb dastehen.

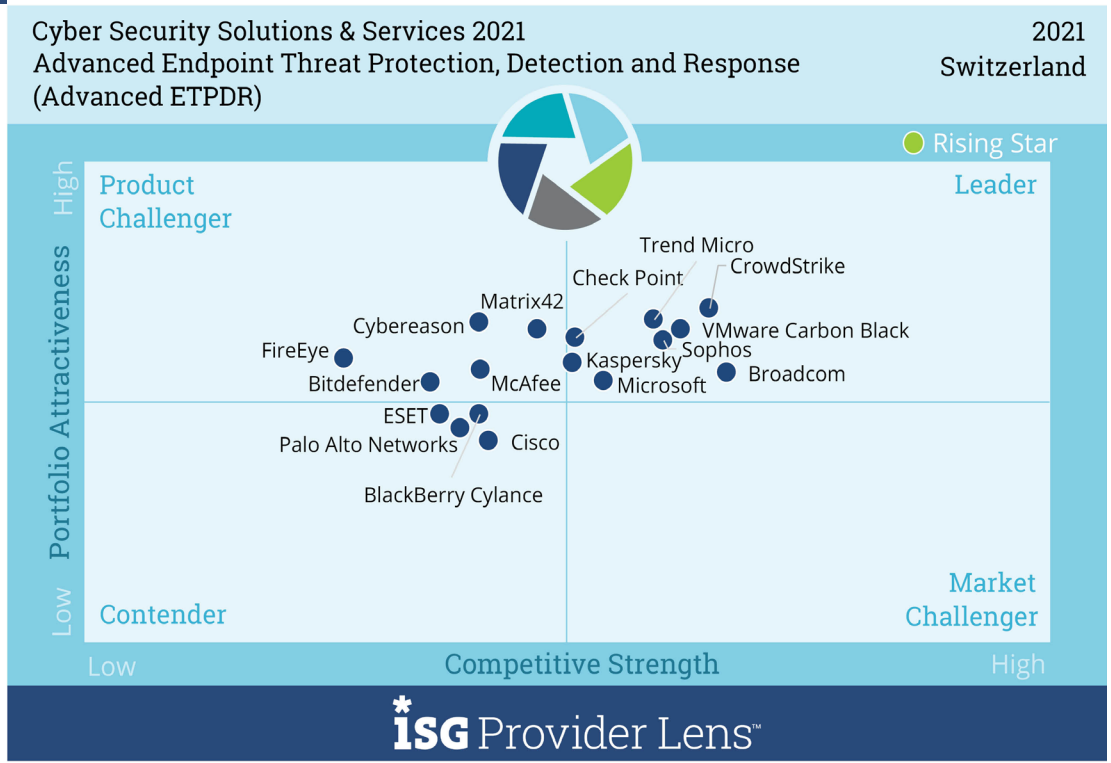
Chief Technology Officers (CTOs) hilft dieser Bericht zu entscheiden, welche Technologien sie am Arbeitsplatz einführen und nutzen wollen.

Sicherheitsarchitekten sollten diesen Bericht lesen, um zu verstehen, wie Anbieter von fortschrittlichen Endpunktlösungen im Vergleich zu anderen Anbietern zu ihren Initiativen und Bedürfnissen passen.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Definition

Anbieter von Advanced-Endpoint-Threat-Protection-, Detection- & Response- (ETPDR-) -Produkten und -Lösungen offerieren eigenentwickelte, proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service-Angebote auf Basis von proprietärer Software. Reine Dienstleister, die kein auf eigenentwickelter Software basierendes Advanced-ETPDR-Produkt (vor Ort oder in der Cloud) anbieten, werden hier nicht analysiert. Im Rahmen dieses Quadranten werden Anbiete bewertet, die Produkte für die kontinuierliche Überwachung und vollständige Transparenz aller Endpunkte bieten und hochentwickelte Bedrohungen analysieren, verhindern und darauf reagieren können.



Source: ISG Research 2021

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Definition

Diese Lösungen gehen über einen reinen signaturbasierten Schutz hinaus und bieten Schutz vor Angriffen wie Ransomware, Advanced Persistent Threats (APTs) und Malware; zu diesem Zweck werden Vorfälle über alle Endpunkte hinweg untersucht. Die Lösung sollte in der Lage sein, den infizierten Endpunkt zu isolieren und die notwendigen Korrekturmassnahmen/Reparaturen durchzuführen. Solche Lösungen bestehen aus einer Datenbank, in der die vom Netzwerk und den Endpunkten gesammelten Informationen aggregiert, analysiert und untersucht werden, und einem Agenten, der im Hostsystem residiert und die Überwachungs- und Reporting-Funktionen für die Vorfälle bereitstellt.

Auswahlkriterien

- Relevanz (Umsatz und Anzahl der Kunden) als Advanced-ETPDR-Produktanbieter in der Schweiz
- Advanced-ETPDR-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
- Umfassende und vollständige Abdeckung und Visibilität aller Endpoints im Netzwerk
- Nachweisliche effektive Abwehr von komplexen Bedrohungen wie Advanced Persistent Threats, Ransomware und Malware
- Nutzung und Analyse von Bedrohungsdaten sowie Echtzeiteinblicke in Bedrohungen, die von den Endpunkten ausgehen

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Beobachtungen

Cyberangriffe nehmen in der Schweiz sowohl in ihrer Quantität als auch besonders hinsichtlich ihrer Gefährlichkeit immer weiter zu. Zudem wandeln sich die Attacken immer schneller. Lösungen für Advanced Endpoint Threat Protection, Detection & Response sollen Unternehmen vor diesen komplexer werdenden Bedrohungen schützen.

Herkömmliche Sicherheitslösungen – wie klassische Antivirus-Lösungen - sind im immer dynamischer werdenden Bedrohungsumfeld zunehmend überfordert, da sie auf Signaturen beruhen. Lösungen für Advanced Endpoint Threat Protection, Detection & Response hingegen sind proaktiv gegen potenzielle Bedrohungen ausgerichtet, da sie Verhaltensanalysen und Machine Learning beziehungsweise künstliche Intelligenz zur Anwendung bringen. Des Weiteren ermöglichen diese fortschrittlichen Sicherheitslösungen eine kontinuierliche Überwachung der Endpoints.

Nicht nur die Entwicklung auf der Angreiferseite führt zu einer zunehmenden Nachfrage nach Lösungen für Advanced Endpoint Threat Protection, Detection & Response, sondern – speziell in jüngster Zeit – auch die veränderte Situation der Anwenderunternehmen und ihrer Mitarbeiter. Die zunehmende Nutzung von Clouddaten und -anwendungen ist bereits seit mehreren Jahren ein zu beobachtender Trend. Gerade durch die Pandemie hat sich diese Entwicklung verstärkt – viele Mitarbeiter arbeiten inzwischen von zu Hause aus – und damit ausserhalb der gesicherten Unternehmenssysteme. Damit hat sich die Bedrohungslage zusätzlich verschärft. Dementsprechend interessieren sich immer mehr Unternehmen für proaktiv und umfassender schützende Advanced-Endpoint-Threat-Protection-, Detection- & Response-Lösungen.

16 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Hersteller im Markt für Advanced Endpoint Threat Protection, Detection & Response in der Schweiz identifiziert. Davon konnten sich acht als Leader positionieren.

- Die Lösung von **Broadcom** ist in der Lage, ein breites Spektrum an Endpoints abzudecken. Darüber hinaus überzeugt Broadcom seine Kunden mit flexiblen, individualisierbaren Schutzmassnahmen.
- Die neue Lösung **Check Point** Harmony ist für eine Vielzahl an Plattformen geeignet und punktet mit einem flexiblen Bereitstellungsmodell und automatisierter Unterstützung.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Beobachtungen

- **CrowdStrike** arbeitet aktiv mit Drittanbietern zum Vorteil seiner Kunden zusammen und wartet im Markt für Advanced Endpoint Threat Protection, Detection & Response mit einem leistungsfähigen Angebot auf.
- **Kasperskys** Kunden profitieren von dem globalen Sensornetzwerk des Anbieters. Darüber hinaus profiliert sich Kaspersky mit der grossen Leistungsfähigkeit seiner Lösung und mit einem hohen Grad an Transparenz.
- **Microsoft** kann umfangreiche Bedrohungsdaten vorweisen, versteht es aber auch, seine Präsenz im Softwaremarkt auch im Markt für Advanced Endpoint Threat Protection, Detection and Response zu nutzen.
- **Sophos** nutzt künstliche Intelligenz zum Vorteil seiner Kunden und überzeugt nicht nur seine bestehenden Kunden mit dem integrierten Management seiner Security-Lösungen auch für Endpoints.
- **Trend Micro** verfügt über eine grosse Markteichweite und bietet eine sehr umfassende Lösung für Advanced Endpoint Threat Protection, Detection & Response an.
- **VMware Carbon Blacks** Lösung eignet sich sehr gut für das Threat Hunting. VMware Carbon Black kann auch generell eine sehr leistungsfähige und zugleich benutzerfreundliche Lösung vorweisen.

ENTERPRISE CONTEXT

Technical Security Services

Dieser Bericht ist für Unternehmen aller Branchen in der Schweiz relevant, um Anbieter zu bewerten, die sich nicht ausschließlich auf ihre jeweiligen proprietären Produkte konzentrieren, sondern Produkte oder Lösungen anderer Anbieter implementieren und integrieren können. TSS umfassen Integration, Wartung und Support von IT-Sicherheitsprodukten oder -lösungen.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern dargelegt, die Technical Security Services für Schweizer Unternehmenskunden offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen. Der Bericht bewertet Anbieter, die sich auf die Integration von Sicherheitsprodukten und -lösungen sowie auf Wartungs- und Supportangebote spezialisiert haben. Diese Provider helfen Organisationen, ihre sensiblen Informationen, Daten und andere digitale Werte vor den wachsenden digitalen Bedrohungen zu schützen.

Unternehmen suchen nach Dienstleistern, die Services für alle Branchen anbieten können. Außerdem werden Anbieter bevorzugt, die branchenspezifische Lösungen für die Integration und Implementierung anbieten. Darüber hinaus ist Fachwissen gefragt, speziell in den Bereichen kundenspezifische Codeentwicklung, ML-basierte Entwicklung, Sicherheitsautomatisierung und Plattform-Engineering.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Dienstleister identifizieren und evaluieren:

Marketing- und Vertriebsleiter hilft dieser Bericht, die relative Positionierung und die Fähigkeiten von Servicepartnern zu verstehen, die ihnen beim effektiven Entwickeln und Aufsetzen von Cybersecurity-Strategien mit den erforderlichen Auswertungen für entsprechende Systeme und unter die Arme greifen können.

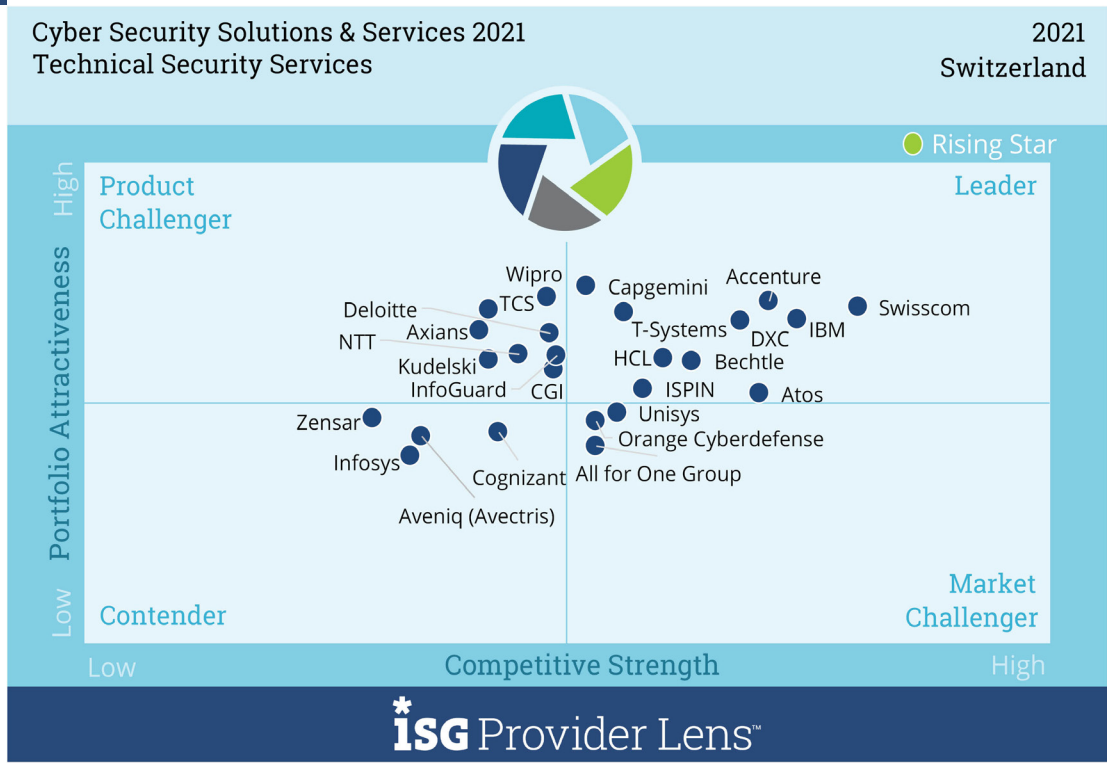
Chief Strategy Officers sollten diesen Bericht lesen, um die relative Positionierung und die Fähigkeiten von Servicepartnern zu verstehen, mit denen sie zusammenarbeiten und eine effektive Cybersecurity-Strategie entwickeln können.

Sicherheits- und Datenexperten gewinnen durch diesen Bericht ein besseres Verständnis dahingehend, wie Anbieter die Einhaltung der Sicherheits- und Datenschutzgesetze in der Schweiz gewährleisten.

TECHNICAL SECURITY SERVICES

Definition

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschliesslich auf ihre jeweiligen proprietären Produkte konzentrieren und Produkte oder Lösungen anderer Anbieter implementieren und integrieren können. TSS umfassen Integration, Wartung und Support von IT-Sicherheitsprodukten oder -lösungen. Sie adressieren alle Sicherheitsprodukte, einschliesslich Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpoint Security, Unified Threat Management und andere.



Source: ISG Research 2021

TECHNICAL SECURITY SERVICES

Auswahlkriterien

- Nachweisliche Erfahrung in der Implementierung von Sicherheitslösungen für Unternehmen in der Schweiz
- Kein ausschliesslicher Fokus auf firmeneigene Produkte
- Autorisierung von Anbietern, deren Sicherheitslösungen zu vertreiben und zu unterstützen
- Zertifizierte Experten zur Unterstützung der jeweiligen Sicherheitstechnologien
- Potenzielle Mitgliedschaft in lokalen Sicherheitsverbänden und Zertifizierungsstellen (wünschenswert, aber nicht zwingend)

Beobachtungen

Auch 2021 stellen die immer intensiveren wie auch raffinierteren, komplexeren und ständig neuen Cyberattacken Unternehmen in der Schweiz vor die Herausforderung, ihre IT-Systeme vor Schaden zu bewahren. Die Erreichung dieses Ziels wird auch weiterhin durch der Mangel an IT-Fachkräften erschwert, unter denen die Cybersecurity-Experten besonders knapp sind. Daher sind Firmen immer häufiger darauf angewiesen, externe Dienstleister in Anspruch zu nehmen, um ihre IT-Security-Systeme auf dem laufenden Stand zu halten. Auch unbedachtes Verhalten von Anwendern wird von Kriminellen immer mehr ausgenutzt, z.B. bei Trojaner- und Phishing-Angriffen; hinzu kommen immer mehr Ransomware-Angriffe. Neben einem zeitgemässen Security Equipment spielen daher auch Schulungen für die Anwender weiterhin eine wichtige Rolle im Cybersecurity-Konzept von Unternehmen und Behörden.

Mittelständische Unternehmen zeigen nach wie vor besonderen Nachholbedarf hinsichtlich der Modernisierung ihrer IT-Security-Systeme, da diese Unternehmen besonders häufig unter dem IT-Fachkräftemangel, fehlendem Know-how, Überforderung oder mangelndem Kapital leiden. Die zunehmenden, komplexeren Sicherheitsbedrohungen und die verschärften gesetzlichen Regelungen bewegen diese Firmen jedoch immer häufiger dazu zu handeln, wofür in vielen Fällen externe Unterstützung erforderlich ist. Mittelständler wissen darüber hinaus häufig die lokale Präsenz der Dienstleister für kurze Wege und unkomplizierte, schnelle Unterstützung zu schätzen.

TECHNICAL SECURITY SERVICES

Beobachtungen

Über die oben beschriebenen grundsätzlichen Faktoren hinaus bewirkt die Corona-Pandemie auch weiterhin zusätzlichen externen Unterstützungsbedarf hinsichtlich sicherer IT-Landschaften, da durch die verstärkte Home-Office-Nutzung – und die dadurch bedingte externe Anbindung der Mitarbeiter – die IT-Systeme leichter angreifbar sind.

IT-Security-Projekte sind häufig anspruchsvoll und vielfältig angelegt. Daher sind hier insbesondere Dienstleister im Vorteil, die ein breites Spektrum an Technical Security Services aus einer Hand bieten und dabei möglichst zahlreiche IT-Security-Lösungen adressieren. In diesem Zusammenhang können sich auch Dienstleister positiv abheben, die mit renommierten Technologieanbietern kooperieren und deren Mitarbeiter viele hochwertige Zertifizierungen vorweisen können. Partnerschaften mit zahlreichen renommierten Technologieanbietern ermöglichen individuell zugeschnittene Leistungen auf hohem Niveau.

Um darüber hinaus im anspruchsvollen Markt der Technical Security Services für Grosskunden erfolgreich zu sein, müssen die Anbieter grosse, auch internationale Erfahrung in diesem Marktsegment sowie ein breit angelegtes Lösungsspektrum vorweisen können. Schlagkräftige, häufig auch international vertretene Teams sollten zur Unterstützung bereitstehen.

Grossunternehmen – und grosse Behörden – zählen aufgrund ihrer komplexen IT (Security)-Landschaften und -Projekte weiterhin zu den wichtigsten Nachfragern von Technical Security Services. Aus den oben beschriebenen Gründen nehmen auch mittelständische Firmen diese Leistungen zunehmend in Anspruch und sind damit eine Zielgruppe mit überdurchschnittlichem Marktwachstum. 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 im Vorteil, die ihren Kunden neben Technical Security Services auch Strategic Security Services und Managed Security Services anbieten können, damit Projekte End-to-End umgesetzt werden können. Einen ähnlichen Vorteil geniessen Provider, die neben Technical Security Services auch zugehörige IT-Lösungen aus einem Guss anbieten können.

25 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Anbieter von Technical Security Services in der Schweiz identifiziert. Davon konnten sich zehn als Leader positionieren.

TECHNICAL SECURITY SERVICES

Beobachtungen

- **Accenture** besitzt grosse Erfahrung und Kompetenz. Darüber hinaus offeriert der Anbieter ein breites Leistungsspektrum aus einer Hand und erspart seinen Kunden auf innovative Art Kosten bei ihrer Cybersecurity-Lösung.
- **Atos** verfügt über zahlreiche Zertifizierungen und profiliert sich im Schweizer Markt mit seinem ganzheitlichen End-to-End-Ansatz.
- **Bechtle** wartet mit einem umfangreichen Portfolio für Technical Security Services auf und überzeugt nicht nur seine mittelständischen Kunden mit umfangreichen Technical Security Services und lokaler Präsenz.
- **Capgemini** besitzt ein grosses internationales Team für Technical Security Services und kann sich mit seinem Angebot an Technical Security Services als innovativer Dienstleister profilieren.
- **DXC** treibt die Automatisierung von Security-Lösungen voran und versteht es, seine Cybersecurity- und Digitalisierungs-Kompetenzen versiert in integrierten Lösungen zu kombinieren.
- **HCL** ist in der Schweiz überdurchschnittlich erfolgreich. Dazu trägt bei, dass HCL seine Kunden mit einem umfassenden Angebot und einem grossen Team für Technical Security Services überzeugen kann.
- **IBM** setzt interessante Akzente bei Support und Collaboration und ist zudem ein integrierter Cybersecurity-Anbieter, der hochentwickelte, innovative Sicherheitslösungen bietet.
- **ISPIN** konnte zahlreiche Kunden gewinnen und schafft so der Sprung unter die führenden Anbieter von Technical Security Services in der Schweiz.
- Die **Swisscom** profitiert unter anderem von ihren grossen Cross-Selling-Möglichkeiten und profiliert sich mit ihren umfangreichen Leistungen für Technical Security Services und ihren starken Technologiepartnerschaften.
- **T-Systems** verfügt über umfangreiche Technologiepartnerschaften und ist in der Lage, mit einem kompletten Portfolio auch anspruchsvollste, integrierte Security-Projekte zu bewältigen.

ENTERPRISE CONTEXT

Strategic Security Services

Dieser Bericht ist für Unternehmen aller Branchen in der Schweiz relevant, um Anbieter von strategischen Security Services zu bewerten.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern von strategischen Cybersecurity Services in der Schweiz dargelegt und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen. Strategische Dienstleistungen helfen Unternehmen bei der Transformation von Sicherheitsprogrammen in relevante, nachhaltige und umsetzbare Ansätze anhand von Auswertungen und der Entwicklung von Programmen. Anstatt sich auf die Reaktion auf Vorfälle zu konzentrieren, legen wirklich effiziente Strategien vor allem Wert auf die Prävention von Cyberangriffen. Daher wenden sich große Unternehmenskunden gerne an Dienstleister, die über eine große und hochqualifizierte Belegschaft, hoch entwickelte Fähigkeiten und Portfolios sowie eine globale Präsenz verfügen.

Ein hohes Schutzniveau und eine geringe Anzahl von Vorschriften bei erstklassiger Infrastruktur machen Cybersecurity zu einer der Top-Prioritäten in der Schweiz. Daher arbeiten die meisten Unternehmen mit verschiedenen Beratungsorganisationen zusammen, um ihre Strategie zu entwickeln und ihr Ökosystem zu transformieren. Da Großunternehmen über die komplexesten IT-Infrastrukturen verfügen, arbeiten sie weiterhin mit globalen oder multinationalen Dienstleistern zusammen.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Dienstleister identifizieren und evaluieren:

Marketing- und Vertriebsleiter hilft dieser Bericht, die relative Positionierung und die Fähigkeiten von Servicepartnern zu verstehen, die ihnen beim effektiven Entwickeln und Aufsetzen von Cybersecurity-Strategien mit den erforderlichen Auswertungen für entsprechende Systeme unter die Arme greifen können.

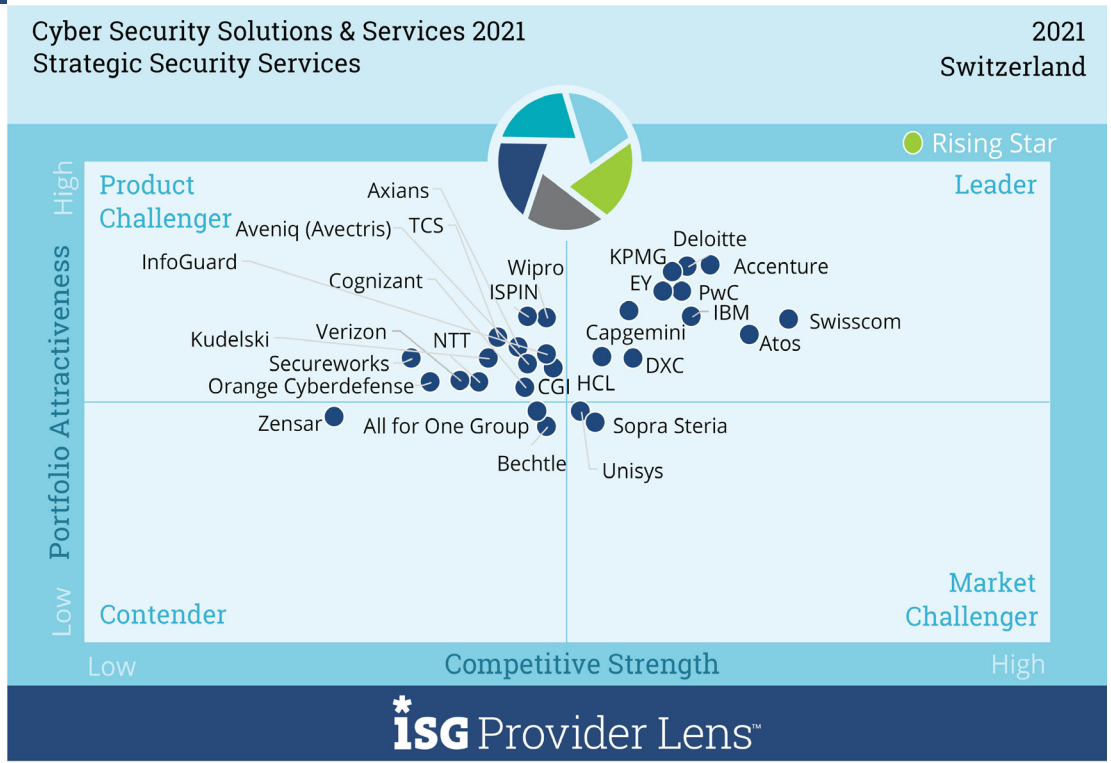
Chief Strategy Officers sollten diesen Bericht lesen, um die relative Positionierung und die Fähigkeiten von Servicepartnern zu verstehen, mit denen sie zusammenarbeiten und eine effektive Cybersecurity-Strategie entwickeln können.

Sicherheits- und Datenexperten gewinnen durch diesen Bericht ein besseres Verständnis dahingehend, wie Anbieter die Einhaltung der Sicherheits- und Datenschutzgesetze in der Schweiz gewährleisten.

STRATEGIC SECURITY SERVICES

Definition

Strategic Security Services umfassen in erster Linie das Consulting für IT-Sicherheit. Einige der in diesem Quadranten abgedeckten Services beinhalten Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zur Architektur von Sicherheitslösungen sowie Training und Schulungen. Diese Services dienen der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition der Cybersicherheitsstrategie für Unternehmen. In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschliesslich auf eigene Produkte oder Lösungen konzentrieren. Die hier analysierten Services decken alle Sicherheitstechnologien ab.



Source: ISG Research 2021

STRATEGIC SECURITY SERVICES

Auswahlkriterien

- Nachweis von Leistungen hinsichtlich Strategic Security Services wie Evaluierung, Assessments, Anbieterauswahl, Architekturberatung und Risikoberatung
- Angebot von mindestens einem der oben genannten Strategic Security Services in der Schweiz
- Die Durchführung von Sicherheitsberatungen unter Verwendung von Frameworks ist von Vorteil.
- Kein ausschliesslicher Fokus auf proprietäre Produkte oder Lösungen

Beobachtungen

Auch und besonders in diesem Jahr sind Schweizer Unternehmen vor vielfältige Herausforderungen gestellt, welche die IT-Sicherheit und den Datenschutz betreffen. Die weiter zunehmende Gefährdungs-situation bewirkt zusammen mit mangelnden Ressourcen ein zunehmendes Bedürfnis nach Orientierung hinsichtlich dieser wichtigen Themen.

Angesichts der immer intensiveren wie auch raffinierteren Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Die Beweggründe für Cybercrime sind beispielsweise Diebstahl von geistigem Eigentum, politische Ziele und immer mehr auch Erpressung durch Ransomware. 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 im Bereich IT-Security haben gerade die mittelgrossen Unternehmen zu leiden. Im Wettbewerb um Fachleute und Talente ziehen sie oft gegenüber den grösseren Firmen, die zum Beispiel meist bessere Konditionen bieten können, den Kürzeren.

Darüber hinaus sind die Anforderungen durch den Gesetzgeber weiterhin oft ein Thema, das den Verant-wortlichen Kopfzerbrechen bereitet, z.B. hinsichtlich Datensicherheit und Datenschutz, deren Umsetzung nicht nur für viele Mittelständler eine grosse Herausforderung darstellt.

STRATEGIC SECURITY SERVICES

Beobachtungen

Diese Faktoren bewirken, dass Unternehmen zunehmend externe Unterstützung benötigen. Am Anfang steht hierbei häufig die Beratung dahingehend, mit welchen Strategien, Lösungen und Technologieanbietern den Security- und Datenschutzanforderungen begegnet werden kann. Über diese grundsätzliche Entwicklung hinaus bewirkt auch die Corona-Krise noch immer zusätzlichen Beratungsbedarf, da durch die verstärkte Home-Office-Nutzung – und die dadurch bedingte externe Anbindung der Mitarbeiter – die IT-Systeme leichter angreifbar sind.

Grossunternehmen – und auch grosse Behörden – zählen aufgrund ihrer komplexen IT- (Security-) Landschaften und -Projekte weiterhin zu den wichtigsten Nachfragern von Strategic Security Services. Aus den oben beschriebenen Gründen nehmen auch mittelständische Firmen diese Leistungen zunehmend in Anspruch und sind damit eine Zielgruppe mit überdurchschnittlichem Marktwachstum. 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 im Vorteil, die ihren Kunden neben Strategic Security Services auch Technical Security Services und Managed Security Services anbieten können, damit die Strategie bruchlos in die Tat umgesetzt werden kann. Einen ähnlichen Vorteil geniessen Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen aus einem Guss anbieten können.

Die Dienstleister in diesem Marktsegment setzen sich vor allem aus zwei Gruppen zusammen: zum einen aus IT-Security-Dienstleistern, zu deren Portfolio auch Security-Beratung zählt, und zum anderen aus Beratungshäusern, wobei die „Big Four" – die Wirtschaftsprüfer Deloitte, EY, KPMG und PwC – erneut eine herausragende Rolle spielen, da sie neben technischer auch Businesskompetenz mitbringen.

29 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Anbieter von Strategic Security Services in der Schweiz identifiziert. Davon konnten sich elf als Leader positionieren.

- **Accenture** offeriert ein sehr breites Serviceportfolio. Accentures Cybersecurity-Einheit expandiert darüber hinaus sehr stark und erhöht damit deutlich die bereits hohe Marktpräsenz.

STRATEGIC SECURITY SERVICES

Beobachtungen

- **Atos** verfolgt einen ganzheitlichen Ansatz in seiner Cybersecurity-Beratung und überzeugt mit seinem globalen Sicherheitsexpertennetzwerk, seinem umfangreichen Angebot und seinen Zertifizierungen.
- **Capgemini** kann ein erfahrenes Security Team vorweisen. Kompetente Cybersecurity-Beratung und -Umsetzung aus einem Guss – das ist eine weitere Stärke von Capgemini.
- **Deloitte** ist ein Cybersecurity-Berater mit starker globaler Präsenz. Deloitte hat sein Cybersecurity-Portfolio zudem stark ausgebaut und profitiert im Rahmen der IT-Security-Beratung von seiner tiefen Businesskompetenz.
- **DXC** kann ein grosses und erfahrenes Team für Cybersecurity vorweisen. Darüber hinaus bietet DXC End-to-End-Security-Dienstleistungen und kann seinen Kunden integrierte IT- und Cybersecurity-Lösungen offerieren.
- **EY** zeichnet sich durch besondere Kundenorientierung aus. Eine bemerkenswerte Zusatzleistung des Beratungshauses ist die Bewertung der Auswirkungen von möglichen Cyberattacken auf den Unternehmenswert.
- **HCL** ist in der Schweiz überdurchschnittlich erfolgreich und schafft so in der Eidgenossenschaft der Sprung unter die führenden Anbieter von Strategic Security Services.
- **IBM** pflegt engen Kontakt zu seinen Kunden. Zudem kann sich IBM im Markt für Cybersecurity-Beratung durch sein umfangreiches und innovatives Dienstleistungsportfolio sowie die tiefen technischen Kenntnisse profilieren.
- **KPMG** verbindet Business- und technisches Verständnis, zeigt zudem Stärken in der strategischen Beratung und zeichnet sich durch gute Zusammenarbeit aus.
- Die Berater von **PwC** überzeugen ihre Kunden durch ihr Kompetenzspektrum. Eine weitere grosse Stärke von PwC ist die Unterstützung der Kunden durch den geschickten Einsatz seiner verschiedenen Kompetenzen bei der Entwicklung von Cybersecurity-Fähigkeiten.
- Die **Swisscom** profitiert von ihrer ausgewogenen Kundenstruktur. Der Anbieter kombiniert zudem erfolgreich ein breites Beratungsportfolio mit End-to-End-Security-Leistungen und einem tiefen Verständnis für die speziellen Belange Schweizer Unternehmen.

ENTERPRISE CONTEXT

Managed Security Services

Dieser Bericht ist für Unternehmen aller Branchen in der Schweiz relevant, um Anbieter von Managed Security Services zu bewerten.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern dargelegt, die Managed Security Services für Schweizer Unternehmenskunden offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen.

Ohne den entsprechenden Managed IT-Support sind IT-Systeme anfällig für Angriffe. Immer mehr wichtige Prozesse werden in die Cloud verlagert, und Cyberkriminelle gehen immer raffinierter vor; deshalb besteht ein noch größerer Bedarf an einer intelligenteren Möglichkeit zur Verbesserung der Sicherheit. Infolgedessen ist die Nachfrage nach Cloud-Sicherheit, Security Operations Center (SOC) Services, Internet of Things (IoT) und Operational Technology (OT) Security sowie Zero Trust Security in den letzten Jahren gestiegen.

Managed Security Service Provider (MSSPs) haben in der Region eigene, dedizierte, gemeinsam gemanagte oder virtuelle SOCs eingerichtet, um entsprechende Services leisten zu können. Der Markt für Managed Security Services (MSS) in der Schweiz wird vor allem durch den wachsenden Bedarf an Sicherheitslösungen in verschiedenen Endabnehmerbranchen angetrieben. Das Bankwesen treibt aufgrund der Kritikalität des Bankenbetriebs die Nachfrage nach Sicherheitslösungen in der Schweiz an. Die Region ist ein ausgereifter Markt in Bezug auf Sicherheitsdienstleistungen für große Unternehmen, das Potenzial für den Mittelstand muss allerdings noch gehoben werden. Beim Outsourcing von Services steigt die Nachfrage nach MSS aufgrund des Mangels an Cybersecurity-Experten. Große Konzerne benötigen häufig umfangreiche Sicherheitsdienstleistungen. Laut ISG berücksichtigen Unternehmen in der Schweiz bei der Wahl eines Anbieters insbesondere dessen Fähigkeit, spezialisierte und hochqualifizierte Ressourcen vor Ort als Teil eines Service-Auftrags offerieren zu können.

Die nachfolgend aufgeführten Rollen können anhand dieses Berichtes Dienstleister identifizieren und evaluieren:

Chief Information Officers (CIOs) hilft dieser Bericht zu verstehen, wie aktuelle Prozesse und Vorgaben sich auf die vorhandenen Systeme im Unternehmen auswirken, und welche Sicherheitsbedarfe es bei der Einführung und Integration von neuen Möglichkeiten unter Umständen zu berücksichtigen gilt.

Chief Technology Officers (CTOs), die für den Betrieb und die Serviceerbringung zuständig sind, erfahren mehr über neue Technologien und Lösungen, um eine strategische Orientierung zu gewinnen, und können sich über Optionen für Partnerschaften mit entsprechenden Dienstleistern informieren. CTOs können auch dafür sorgen, dass geeignete Sicherheitsplattformen und -lösungen zum Einsatz kommen, und so Wettbewerbsvorteile schaffen.

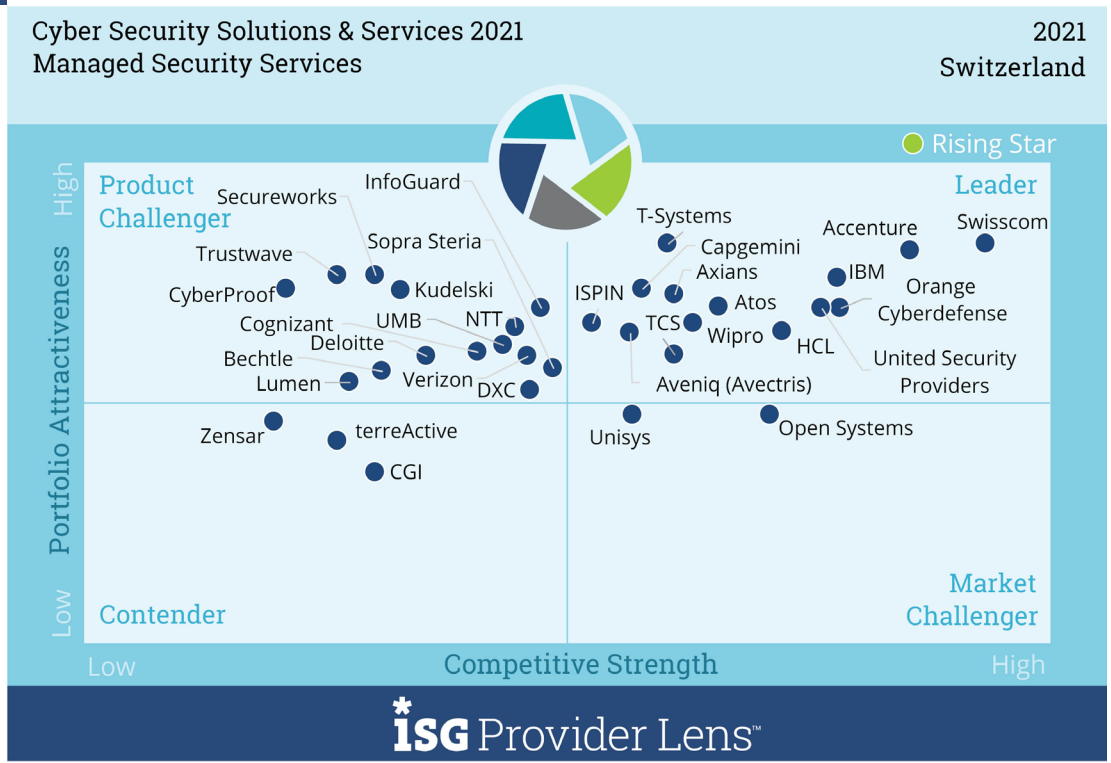
Sicherheits-Verantwortliche gewinnen durch diesen Bericht ein klares Verständnis der relativen Positionierung und der Fähigkeiten von MSSPs. Der Bericht vergleicht auch die technischen Leistungen verschiedener Serviceanbieter im Markt.

ISG Provider Lens™

MANAGED SECURITY SERVICES

Definition

Unter Managed Security Services fallen Betrieb und Management von IT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). Zu den typischen Dienstleistungen gehören Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmassnahmen, Penetrationstests, Firewall-Betrieb, Antivirus-Betrieb, IAM-Betriebsservice, DLP-Betrieb und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Dieser Quadrant untersucht Dienstleister, die sich nicht ausschliesslich auf proprietäre Produkte konzentrieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Lösung von Problemen.



Source: ISG Research 2021

MANAGED SECURITY SERVICES

Auswahlkriterien

- Angebot von Sicherheitsdiensten wie Erkennung und Vorbeugung, Security Information & Event Management (SIEM) sowie Sicherheitsberatern und Audits, per Fernzugriff oder vor Ort beim Kunden.
- Relevanz (Umsatz und Anzahl der Kunden) als Anbieter von Managed Security Services in der Schweiz
- Kein ausschliesslicher Fokus auf proprietäre Produkte, sondern Management- und Betriebsleistungen für Best-of-Breed Security-Tools
- Akkreditierungen von Anbietern von Sicherheitstools
- Security Operations Center sind idealerweise im Besitz und unter der Leitung des Anbieters und nicht überwiegend von Partnern.
- Zertifizierte Mitarbeiter

Beobachtungen

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken – sowie die zusätzlichen Herausforderungen durch die Pandemie – fördern besonders auch die Nachfrage nach Managed Security Services. Knappe qualifizierte Ressourcen und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich in den Fokus der Schweizer Unternehmen.

Im Segment der grossen Unternehmen spielen aufgrund der häufig internationalen Präsenz dieser Unternehmen global verteilte Security Operations Center (SOCs) eine besondere Rolle. Aber auch SOCs mit Schweizer Standort wissen Grossunternehmen aufgrund des wichtiger gewordenen Datenschutzaspektes – aufgrund unternehmensinterner Compliance oder gesetzlicher Regelungen – zu schätzen. Die grossen Firmen legen aufgrund ihrer meist komplexen IT-Security-Systeme häufig Wert auf ein breites Security-Themenspektrum, das von den Managed Security Services Providern abgedeckt wird.

Aber gerade auch mittelständische Unternehmen – die noch mehr als die Grossunternehmen vom Cybersecurity-Fachkräftemangel betroffen sind – sind immer mehr auf die Unterstützung externer Dienstleister angewiesen, um diese zunehmenden Herausforderungen zu meistern. So interessiert sich inzwischen auch der Mittelstand verstärkt für Managed Security Services, mit denen die Kunden umfassend beim Handling der Security-Systeme entlastet werden. In diesem Zusammenhang sind SOCs in der Schweiz ein Pluspunkt im Kundensegment der mittelständischen Unternehmen, da dieser Klientel der Betrieb in der Schweiz besonders wichtig ist; auch Ansprechpartner, welche die Heimatsprache beherrschen, spielen für diese Kundengruppe eine wichtige Rolle. Anbieter mit einer ausgewogenen

MANAGED SECURITY SERVICES

Beobachtungen

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

Unabhängig von der Unternehmensgrösse ist den Kunden die Sicherung der Zuverlässigkeit der Managed Security Services wichtig. Das heisst, die flankierenden Dienstleistungen zur Sicherung der Verfügbarkeit und Vertraulichkeit – z.B. physischer Schutz der SOCs, redundante Systeme, hochklassige SLAs und eine hochverfügbare Hotline – dürfen keine Wünsche offenlassen.

Darüber hinaus erwarten Kunden von den Managed Security Service Providern eine hohe Innovationskraft, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Erweiterung der SOCs in Richtung eines Cyber Defense Centers, indem zunehmend komplexeren Bedrohungen auch mit künstlicher Intelligenz und Automatisierung begegnet wird. Virtualisierung und Software-Defined Perimeter ermöglichen es SOCs, ihren Kunden Skalierbarkeit und Anpassung an ihre individuellen Anforderungen zu bieten. Da auch Cyberkriminelle sich zunehmend künstlicher Intelligenz bedienen, sind Cyber Fusion Center als Ergänzung zu den bestehenden SOCs entstanden, um den Bereich des Cyber Security Managements zielgerichtet und zukunftsgerecht auszubauen.

Des Weiteren sind Dienstleister im Vorteil, die ihren Kunden neben Managed Security Services auch Strategic Security Services und Technical Security Services anbieten können, damit Projekte End-to-End umgesetzt werden können. Einen ähnlichen Vorteil geniessen Provider, die neben Managed Security Services auch zugehörige IT-Lösungen aus einem Guss anbieten können.

33 Unternehmen wurden im Rahmen dieser Anbieteruntersuchung als besonders relevante Anbieter von Managed Security Services in der Schweiz identifiziert. Davon konnten sich vierzehn als Leader positionieren.

- **Accenture** überzeugt mit seinen sehr umfangreichen Managed Security Services. Dies und die weitere Expansion tragen zur zunehmenden Marktpräsenz bei.
- **Atos** bietet Multi-Vector Detection und punktet darüber hinaus mit umfassenden Managed Security Services, die seine Kunden optimal unterstützen – und auch für international aktive Unternehmen attraktiv sind.
- Die Managed Security Services von **Aveniq (Avectris)** überzeugen mit umfangreichen End-to-End-Dienstleistungen auf Basis seines integrierten Portfolios und mit „Swissness". Avectris wurde im Dezember 2020 an die GIA Informatik AG verkauft. Die beiden Unternehmen treten seit dem 1. Juni 2021 unter dem Namen Aveniq auf.

MANAGED SECURITY SERVICES

Beobachtungen

- **Axians** profitiert von seinem besonderen Verständnis für den Mittelstand und kombiniert erfolgreich lokales Delivery und Verständnis für die speziellen Anforderungen seiner Kunden.
- Die Managed Security Services von **Capgemini** bedienen auch hohe Kundenanforderungen aus einer Hand. Darüber hinaus entwickelt Capgemini seine Managed Security Services weiter und gewinnt so eine höhere Marktpräsenz, weltweit und in der Schweiz.
- **HCL** zeigt mit seinen Managed Security Services sehr grosses Engagement in der Schweiz und ist dadurch in der Eidgenossenschaft überdurchschnittlich erfolgreich.
- **IBM** bietet seinen Kunden globalen Betrieb und versteht es, mit seinen leistungsfähigen Managed Security Services zu überzeugen, die ein breites Technologiespektrum abdecken.
- **ISPIN** kombiniert vorteilhaft Manpower mit Automatisierung. Damit und mit seiner Swissness gelingt ISPIN der Sprung unter die führenden Anbieter von Managed Security Services in der Schweiz.
- Die Managed Security Services von **Orange Cyberdefense** unterstützen zahlreiche Cybersecurity-Themen. Und auch mit der globalen Präsenz seiner Managed Security Services überzeugt Orange Cyberdefense seine Kunden.
- Als Schweizer Netzbetreiber ist die **Swisscom** in der Lage, sicherheitsrelevante Vorfälle in der Schweiz früher zu erkennen und somit schneller zu reagieren. Dies und unter anderem auch das umfangreiche Angebot machen die Swisscom zum führenden Anbieter von Managed Security Services in der Schweiz.
- **T-Systems** punktet mit umfangreichen Branchen-Insights und baut seine Managed Security Services kontinuierlich aus.
- **TCS** deckt mit seinen Managed Security Services ein breites Spektrum ab. Des Weiteren beherrscht TCS die Mischung aus globaler und lokaler Präsenz und steigt so in den Leader-Quadranten für Managed Security Services in der Schweiz auf.
- **United Security Providers** und Swisscom bilden eine starke Vereinigung der Kräfte. Darüber hinaus profiliert sich United Security Providers mit umfangreichen Ressourcen und Managed Security Services „made in Switzerland".
- **Wipro** ist in der Schweiz überdurchschnittlich erfolgreich und schafft so der Sprung in den Leader-Quadranten für Managed Security Services in der Schweiz.

AXIANS

Überblick

Axians Cyber Security & BI (nachfolgend „Axians“) ist der Cyber-Security-Experte der Axians-Unternehmensgruppe, die Teil des französischen Unternehmens VINCI Energies ist. In der Schweiz ist Axians Cyber Security & BI in Rotkreuz, Basel und Zürich vertreten. Axians Cyber Security & BI betreibt ab Oktober 2021 in der Schweiz ein dediziertes Security Operations Center in Basel.

Stärken

Die Kunden von Axians können aus einem umfangreichen Angebot an Managed Security Services wählen: Axians bietet im Rahmen seiner Managed Security Services ein breites Spektrum an Services und gemanagten Security-Themen an. Dabei wird nicht nur die IT-Sicherheit, sondern auch der Themenkomplex OT adressiert.

Axians bietet den Betrieb von Security Operations Centern auch in der Schweiz: Axians betreibt Security Operations Center unter anderem auch in der Schweiz. Dies entspricht insbesondere den Erwartungen vieler mittelständischer Anwenderunternehmen – aber durchaus auch von grösseren Unternehmen, die Wert auf den Betrieb im eigenen Land legen.

Axians profitiert von seinem besonderen Verständnis für den Mittelstand: Der Kundenschwerpunkt von Axians hinsichtlich seiner Managed Security Services in der Schweiz liegt vor allem auf den mittelständischen Kunden. Damit kann Axians vom überdurchschnittlichen Wachstum des Mittelstandssegments profitieren, das angesichts steigender Security-Anforderungen und des häufig begrenzten eigenem Know-hows zunehmend auf die Unterstützung durch externe Dienstleister zurückgreift.

Axians besitzt Verständnis für Geschäftsanforderungen und regulierte Branchen: Axians demonstriert Verständnis für die Herausforderungen seiner Kunden im Zusammenhang mit ihren Geschäftsanforderungen. Besonders sind hier auch regulierte Wirtschaftszweige zu nennen. Axians verfügt über tiefes Know-how hinsichtlich stark regulierter Branchen, wie zum Beispiel in der Pharmaindustrie.

Herausforderungen

Die Awareness im Schweizer Markt bietet noch Ausbaupotenzial: Axians konnte seine Leader-Position im Schweizer Markt für Managed Security Services gegenüber dem vergangenen Jahr erkennbar ausbauen. Allerdings wird der Anbieter bisher von Anwenderunternehmen häufig noch nicht unter den ersten Anbietern genannt, wenn es um Managed Security Services geht.

2021 ISG Provider Lens™ Leader

Axians kombiniert erfolgreich lokales Delivery und Verständnis für die speziellen Anforderungen seiner Kunden.

Methodik

METHODIK

Im Rahmen des Projektes „ISG Provider Lens™ 2021 – Cyber Security Services & Solutions“ wurden in einem mehrstufigen Research- und Analyseprozess die relevanten Dienstleister im Schweizer Markt untersucht und nach dem Research-Prozess der Studie positioniert. Dabei gliederte sich das Projekt in folgende Schritte:

1. Definition Zielmarkt Cyber Security Services & Solutions
2. Umfrage zu Dienstleistern/Anbietern zu allen Trendthemen
3. Interaktive Diskussionen mit Dienstleister/Anbietern über ihre Leistungsfähigkeit und Use Cases
4. Nutzung der ISG-internen Datenbanken sowie des Know-hows und der Erfahrung der ISG Advisor (soweit möglich)
5. Detaillierte Analyse und Evaluierung von Services und entsprechenden Dokumentationen auf Basis der von den Anbietern zur Verfügung gestellten Daten und Zahlen sowie anderer Quellen
6. Auswertung auf Basis der folgenden Kriterien:
   - Strategie und Vision
   - Innovation
   - Markenbekanntheitsgrad und Marktpräsenz
   - Vertriebs- und Partnerlandschaft
   - Breite und Tiefe des Service-Angebots
   - Technologische Weiterentwicklungen

Autor und Editor

Frank Heuer, Autor

Principal Analyst

Frank Heuer ist Principal Analyst bei der ISG Germany. Sein Schwerpunkt liegt auf den Themen Cyber Security, 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.

Monica K, Analyst für Unternehmenskontext und Globaler Überblick

Senior Forschungsanalyst

Monica K ist Research Analystin für Studien zum Internet der Dinge und zur digitalen Unternehmenstransformation im Rahmen des ISG Provider Lens™ Programms. Sie hat auch Erfahrung in der Erforschung von Technologien wie Robotic Process Automation, Blockchain und künstlicher Intelligenz. Monica arbeitet seit einem Jahr mit ISG zusammen und beteiligt sich aktiv an der Mobilisierung von Serviceanbieterinformationen durch Primär- und Sekundärforschung. Darüber hinaus bearbeitet sie Ad-hoc-Anfragen von Anbietern und Beratern.

Autor und Editor

Heiko Henkes, Editor

Director Advisor

Heiko Henkes ist Director und Principal Analyst bei ISG und in seiner Rolle als Global IP Content Lead verantwortlich für das strategische Business Management und die Leitung des ISG Research Advisor Teams. Seine Kernkompetenzen liegen in den Bereichen der Definition von Ableitungen für alle Arten von Unternehmen im Rahmen ihrer IT-basierten Geschäftsmodelltransformation. Er schlägt die Brücke zwischen IT-Trendthemen und fungiert als Keynote Speaker zu aktuellen und zukünftigen IT-Trends. Hr. Henkes verfügt über fast 15 Jahre Erfahrung in der IT-Beratung sowie in der Primär- und Sekundärmarkt-Research und mit Anbieter-GTM-Strategien.

Seine Research-Schwerpunkte sind Digital Business Transformation, Cloud und Edge Computing, Mobile Business, Change Management und Mixed Reality.

ISG Provider Lens™ | Quadrant Report
Juli 2021

ISG (Information Services Group) (ISG), (NASDAQ: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 700 Kunden, darunter die 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 digitalen Transformation, inklusive Automatisierung, Cloud und Daten-Analytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzwerkbetrieb, Design von Technologie-Strategie und -Betrieb, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.300 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 Branchen- und Technologie-Expertise sowie weltweit führende Marktforschungs- und Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren.