ISG Provider Lens™

Cybersecurity – Solutions and Services

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

Customized report courtesy of:

sure[secure]

QUADRANT REPORT | JUNI 2023 | DEUTSCHLAND

Inhaltsverzeichnis

Bericht Autor: Frank Heuer

Aktuelle Krisen und das Mittelstandssegment treiben den deutschen Cybersecurity-Markt.

Im Zusammenhang mit Cybersecurity sind die Verantwortlichen in den Unternehmen aktuell vor verschiedene Herausforderungen gestellt. Die verstärkten Cyberbedrohungen im Rahmen des Ukraine-Kriegs sowie die Umbrüche als Folge der im Wesentlichen überwundenen COVID-Pandemie – und selbstverständlich auch der langfristige Trend hin zur Digitalisierung – haben in Deutschland zu vergrößerten Angriffsflächen für Cyberattacken geführt, die entsprechender Gegenmaßnahmen bedürfen. Andererseits führt die Abschwächung der Konjunktur zu finanziellen Herausforderungen.

Im Rahmen der Digitalisierung werden Geschäftsprozesse zunehmend in die IT verlagert. Auch geistiges Unternehmenseigentum wird immer mehr digital dargestellt. Mit der steigenden Notwendigkeit, IT- und Kommunikationssysteme zu schützen, hat sich IT-Sicherheit zur Unternehmenssicherheit gewandelt. Die Corona-Krise hat Herausforderungen für die IT-Sicherheit mit sich gebracht, 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.

Der Fachkräftemangel fördert die Nachfrage nach externen Cybersecurity-Dienstleistern in Deutschland.

Neben der vermehrten Remote- und Hybrid-Arbeit hat die zunehmende Bereitstellung von Ressourcen aus der Cloud zu einer größeren Angreifbarkeit der IT-Systeme und infolge zu einer gewachsenen Relevanz des Zero-Trust-Ansatzes geführt. Der Grundsatz „Never trust,

Die **Cybersecurity-Herausforderungen** nehmen für die Unternehmen in jeder Hinsicht zu.

always verify" (nie vertrauen, immer überprüfen) bedeutet unter anderem gegenseitige Authentifizierung und kontinuierliche Überwachung des Netzwerks.

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 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 immer öfter an externe Dienstleister, zum Beispiel Anbieter von Managed Security Services. Diese sowie auch viele IT-Security-Produktanbieter setzen, um selbst mit den Bedrohungen mithalten zu können, verstärkt auf proaktive statt reaktive Methoden, die zum Beispiel auf künstlicher Intelligenz basieren.

Künftig müssen Cybersecurity-Dienstleister ihre Kunden auch für die Abwehr von quantum-basierenden Angriffen wappnen können.

Neben dem Eigenschutz des Unternehmens zwingen auch gesetzliche Regelungen, wie die Datenschutz-Grundverordnung (DSGVO) in der EU, 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 zu profitieren. Die abflauende Konjunktur lässt auch die Nachfrage nach Cybersecurity-Lösungen nicht unberührt, so dass der Mittelstand mit seiner überdurchschnittlich wachsenden Nachfrage zu einem immer attraktiveren Marktsegment wird, das aber auch adäquat adressiert werden will. Es reicht nicht aus, mittelständischen Kunden einfach einen Service für Großkunden anzubieten Vielmehr muss der gesamte Go-to-Market – Produkte, Preise und Kommunikation – an diese Kunden angepasst werden. Kommunikation und kulturelle Aspekte sind besonders wichtig, um vom Mittelstand als Anbieter akzeptiert zu werden, der dieses Segment ernst nimmt.

Trotz der großen Bedeutung von Cybersicherheit kämpfen IT-Verantwortliche wieder vermehrt mit der Aufgabe, Investitionen in IT-Sicherheit gegenüber Stakeholdern des Unternehmens zu legitimieren, besonders gegenüber dem CFO. Anders als bei anderen IT-Projekten ist es nicht immer möglich, die Rentabilität der Investitionen nachzuweisen; auch Bedrohungsrisiken zu quantifizieren ist nicht einfach. Allerdings erkennen auch Führungskräfte zunehmend, dass Cyberattacken zu massiven, unter Umständen existenziellen finanziellen und Imageschäden führen können. Somit gewinnt Cybersicherheit in Unternehmen an Bedeutung, und die Führungsetage wird 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.

Trotzdem muss in der Zukunft das Augenmerk auch auf technische Bedrohungen gelegt werden. Quantum-basierende Angriffe stellen

eine neue Qualität bei Angriffen auf die Verschlüsselung von vertraulichen Daten dar. Erste Dienstleister haben sich mit ihrer Beratung bereits darauf eingestellt.

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 die gestiegene Nutzung des Home Offices infolge der Pandemie. Viele Mitarbeiter greifen remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden.

Data Leakage/Loss Prevention & Data Security (Produkte)

Das Interesse in Deutschland 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 existenziell bedeutsamen Unternehmens-Assets entwickelt.

Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen.

Extended Threat Detection & Response (Produkte)

Lösungen für Extended Threat Detection & Response (XDR) haben in den letzten zwei Jahren an Bedeutung gewonnen und sich durchgesetzt. Unternehmen wollen die Informationen, die sie aus der breiten Palette der in ihrer IT-Infrastruktur eingesetzten Sicherheitstools gewinnen, besser verstehen und im Zusammenhang betrachten (korrelieren). Automatisierung spielt dabei eine zentrale Rolle.

Führende Anbieter offerieren verhaltens- und kontextbezogene Analysemodule sowie eine offene Integration mit anderen Endpoint- und Network-Detection- & Response-Produkten.

Security Service Edge (Produkte)

Security Service Edge (SSE) befindet sich noch in einem frühen Stadium der Reife und Akzeptanz bei Unternehmen. SSE umfasst Lösungen, die Unternehmen einen sicheren Zugang zur Cloud ermöglichen, die Remote-Arbeit erleichtern, Edge-Computing-Lösungen absichern und die digitale Transformation unterstützen. Die wachsende Zahl von Remote- und Hybrid-Mitarbeitern und der Übergang zur Cloud haben das Umfeld für SSE-Lösungen geschaffen.

Strategic Security Services

Neben den akuten Krisen (Ukraine-Krieg und Auswirkungen der COVID-Pandemie) sind Unternehmen in Deutschland 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.

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 hinsichtlich IT-Security haben gerade die mittelgroßen Unternehmen zu leiden. Der Mittelstand ist damit ein überdurchschnittlich wachsendes – und entsprechend zunehmend attraktives – Marktsegment.

Technical Security Services

Weiterhin sind Unternehmen und Behörden in Deutschland 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.

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.

Managed Security Services - SOC

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken – sowie die zusätzlichen Herausforderungen durch die aktuellen Krisen – 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 deutscher Unternehmen.

> Ohne künstliche Intelligenz und Automatisierung können Managed Security Services Provider Cyberattacken kaum mehr bewältigen – es sollte aber nicht auf die menschliche Expertise verzichtet werden.

Große wie auch mittelständische Kunden wissen Security Operations Centers (SOCs) mit deutschem 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 zugehörigen Security-Lösungen sowie eine hohe Innovationskraft wichtig, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben.

Managed Security Services Provider setzen vermehrt künstliche Intelligenz und Automatisierung ein, um der Cyberbedrohungen Herr zu werden. Ideal ist eine Kombination der maschinellen Effizienz mit umfassender menschlicher Expertise.

> Cybersecurity-Anbieter, die in Deutschland überdurchschnittlich wachsen wollen, sollten sich verstärkt auf die Bedürfnisse des Mittelstandes konzentrieren – und auf die entsprechende Kommunikation mit diesem Segment.

Anbieterpositionierung

Seite 1 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Absolute Software	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Not In	Leader	Leader	Leader
Acronis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Alice&Bob.Company	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
All for One Group	Not In	Not In	Not In	Not In	Market Challenger	Contender	Not In
Axians	Not In	Not In	Not In	Not In	Leader	Leader	Leader
BAYOONET	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Bechtle	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader
Beta Systems	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 2 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Bitdefender	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
BlackBerry	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Brainloop	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Broadcom	Product Challenger	Leader	Leader	Product Challenger	Not In	Not In	Not In
CANCOM	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader
Capgemini	Not In	Not In	Not In	Not In	Leader	Leader	Leader
Cato Networks	Not In	Not In	Not In	Leader	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Not In	Product Challenger	Contender
Check Point	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Cisco	Not In	Not In	Contender	Leader	Not In	Not In	Not In

Anbieterpositionierung

Seite 3 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Cloudflare	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In
Computacenter	Not In	Not In	Not In	Not In	Leader	Leader	Product Challenger
Controlware	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader
CoSoSys	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger
Deutsche Telekom	Not In	Not In	Not In	Not In	Leader	Leader	Leader

Anbieterpositionierung

Seite 4 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
DIGITALL	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
DriveLock	Not In	Leader	Market Challenger	Not In	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger
Ericom Software	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
ESET	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Eviden (Atos)	Leader	Not In	Not In	Not In	Leader	Leader	Leader
EY	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In
Fidelis Cybersecurity	Not In	Contender	Product Challenger	Not In	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Leader	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 5 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Fortinet	Contender	Not In	Leader	Product Challenger	Not In	Not In	Not In
Fortra	Not In	Leader	Not In	Not In	Not In	Not In	Not In
GBS	Not In	Leader	Not In	Not In	Not In	Not In	Not In
glueckkanja-gab	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★
Google	Not In	Contender	Not In	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
HiSolutions	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In
HPE (Aruba)	Not In	Not In	Not In	Rising Star ★	Not In	Not In	Not In
IBM	Leader	Leader	Leader	Not In	Leader	Leader	Leader
iboss	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In

Anbieterpositionierung

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
iC Consult	Not In	Not In	Not In	Not In	Contender	Not In	Not In
Imprivata	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
IN Groupe	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
indevis	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender
Infinite Networks	Not In	Not In	Not In	Contender	Not In	Not In	Not In
InfoGuard	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Infosys	Not In	Not In	Not In	Not In	Rising Star ★	Product Challenger	Leader
itWatch	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Kaspersky	Not In	Not In	Contender	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Not In	Leader	Not In

Anbieterpositionierung

Seite 7 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Kyndryl	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In
Logicalis	Not In	Not In	Not In	Not In	Contender	Contender	Product Challenger
Lookout	Not In	Not In	Not In	Contender	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Materna	Not In	Not In	Not In	Not In	Product Challenger	Contender	Product Challenger
Matrix42	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Not In	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In
Nevis	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger

Anbieterpositionierung

Seite 8 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Omada	Contender	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Open Systems	Not In	Not In	Not In	Contender	Not In	Not In	Not In
OpenText	Contender	Product Challenger	Not In	Not In	Not In	Not In	Not In
Oracle	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Not In	Market Challenger	Product Challenger	Leader
Palo Alto Networks	Not In	Not In	Leader	Leader	Not In	Not In	Not In
Perimeter 81	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 9 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Proofpoint	Not In	Market Challenger	Not In	Contender	Not In	Not In	Not In
Rapid7	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Product Challenger	Not In	Not In	Product Challenger	Not In
SentinelOne	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In
Solarwinds	Contender	Not In	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Seite 10 von 11

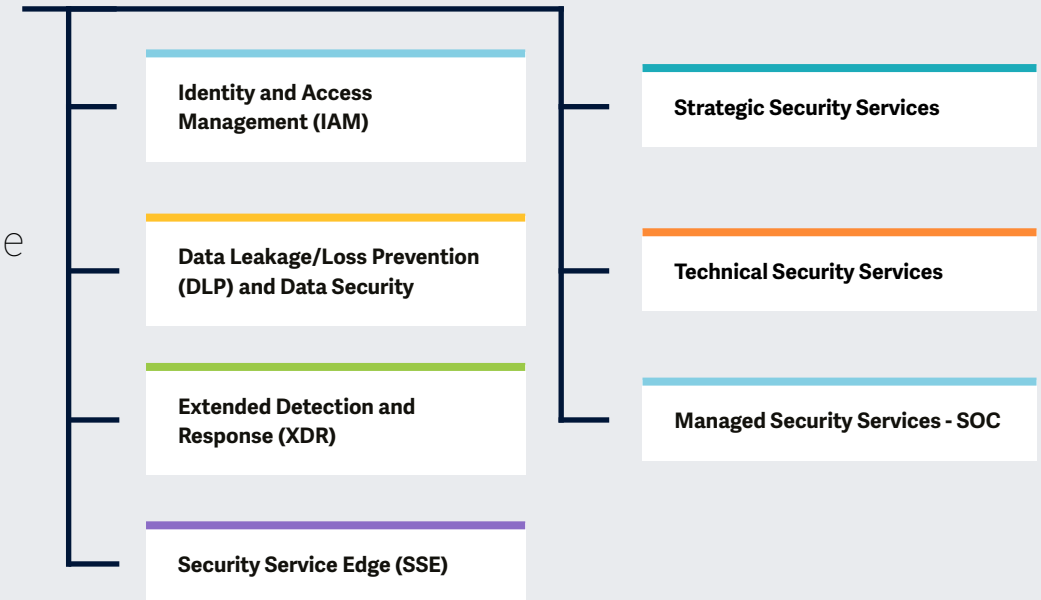
	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Sophos	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger
suresecure	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★	Not In
Syntax	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
TCS	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Tech Mahindra	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Thales	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Rising Star ★	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Leader	Not In	Not In	Not In	Not In
Unisys	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger

Anbieterpositionierung

Seite 11 von 11

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Verizon Business	Not In	Not In	Not In	Not In	Not In	Contender	Product Challenger
Versa Networks	Not In	Not In	Not In	Leader	Not In	Not In	Not In
VMware	Not In	Not In	Market Challenger	Contender	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger
Zensar	Not In	Not In	Not In	Not In	Contender	Contender	Not In
Zscaler	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In

Schwerpunktbereiche der Studie „Cybersecurity – Solutions and Services 2023“



Vereinfachte Illustration; Quelle: ISG 2023

Definition

Aus Cybersicherheitssicht könnte man das Jahr 2022 als turbulent bezeichnen; trotz sinkender Datenschutzverletzungen waren die Angriffe in diesem Jahr deutlich raffinierter und schwerer. Im Jahr 2022 haben die Unternehmen ihre Investitionen in die Cybersicherheit erhöht und entsprechenden Initiativen zur Verhinderung von Angriffen und zur Verbesserung ihres Sicherheitsstatus eine hohe Priorität eingeräumt. Sie hatten aus den Angriffen von 2021 ihre Lektion gelernt; Führungskräfte und Unternehmen aller Größen und Branchen investierten entsprechend in Maßnahmen, um auf Bedrohungen der Cybersicherheit und auf Cyberangriffe reagieren und diese überstehen zu können.

Auch kleine Unternehmen wissen inzwischen, welche Gefahren von Cyber-Bedrohungen ausgehen, und haben erkannt, dass sie aktiv ins Visier genommen werden und sehr anfällig für Cyberangriffe sind. Dadurch stieg der Bedarf an (verwalteten) Sicherheitsdiensten und Cyber Resiliency Services, die es Unternehmen ermöglichen, nach einem Cybervorfall schnell den Betrieb wieder

aufzunehmen. Dienstleister und Anbieter offerieren daher Services und Lösungen zur Unterstützung der Wiederherstellung und der Geschäftskontinuität.

Cyberkriminelle nutzten große Schwachstellen wie Log4shell aus und störten die Geschäftsaktivitäten auch weiterhin mit Ransomware; insbesondere das Gesundheitswesen, die Lieferkette und der öffentliche Sektor gerieten ins Visier.

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

Betrachtungsumfang der Studie

In diesem ISG Provider Lens™ Quadrantenbericht deckt ISG die folgenden sieben Quadranten für Dienstleistungen/ Lösungen ab: Identity & Access Management (IAM), Data Leakage/Loss Prevention (DLP) & Data Security, Extended Detection & Response (XDR), Security Service Edge (SSE) – Global, Strategic Security Services, Technical Security Services, Managed Security Services - (SOC). Die Anbieter von Security Service Edge (SSE)-Lösungen werden in dieser Studie in diesem Jahr zunächst aus einer globalen Perspektive analysiert und positioniert, nicht aus der Perspektive einzelner Länder und Regionen, da sich der Markt derzeit noch im Anfangsstadium und Reifungsprozess befindet.

Die ISG Provider Lens™ Studie „Cybersecurity – Solutions and Services" bietet Geschäfts- und IT-Entscheidern folgende Vorteile:

- Transparente Darstellung der Stärken und Schwächen relevanter Anbieter
- Eine differenzierte Positionierung der Anbieter nach Segmenten, basierend auf Wettbewerbsstärken und Portfolio- Attraktivität
- Fokus auf regionale Märkte

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

Klassifizierung der Anbieter

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

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

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

Anbieterklassifizierungen: Bewertungskategorien

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

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

Identity and Access Management (IAM)

Wer diesen Bericht lesen sollte

Dieser Quadrant ist für Unternehmen in Deutschland relevant, um Anbieter von Identitäts- und Zugriffsmanagementlösungen (IAM) zu evaluieren. Darüber hinaus wird bewertet, wie die einzelnen Anbieter Unternehmen bei der Bewältigung komplexer Sicherheitsherausforderungen im Zusammenhang mit der Sicherung des Benutzerzugangs und von digitalen Identitäten unterstützen.

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

In Deutschland verfolgen Unternehmen einen Zero-Trust-Ansatz, um IAM und die damit verbundenen Tools zu konsolidieren. Sie modernisieren ihre IAM-Systeme, um ihre IAM-Infrastruktur zu vereinfachen, die Komplexität zu verringern und die allgemeine Sicherheitslage durch die Zentralisierung von Identitäts- und Zugriffsmanagementrichtlinien und -kontrollen zu verbessern. Durch die Einführung eines Zero-Trust-Ansatzes für IAM kann die Sicherheit weiter erhöht werden, und zwar durch das Implementieren einer kontinuierlichen Überwachung, risikobasierter Zugriffskontrollen und adaptiver Authentifizierungsmechanismen. Cloudbasierte IAM-Plattformen unterstützen dynamische Zugriffskontrollen und Risikobewertungen in Echtzeit. Die Integration von IAM-Tools mit KI/ML-Technologien gewinnt zunehmend an Bedeutung, da sie für den Schutz der sensiblen Daten und Systeme eines Unternehmens vor Cyberbedrohungen entscheidend ist. Echtzeit-Analysen der Aktivitäten von privilegierten Konten, des Benutzerverhaltens und der Zugriffsanfragen verhelfen zu tieferen Einblicken in potenzielle Sicherheitsbedrohungen und ermöglichen schnelle Reaktionen, um Risiken zu mindern. Dieser Ansatz hilft Unternehmen bei der Einhaltung von Branchenvorschriften und dem Schutz sensibler Informationen vor Cyberbedrohungen. Es wird erwartet, dass die passwortlose Authentifizierung weiter zunehmen wird, da sie das Benutzererlebnis verbessert und eine reibungslose Anmeldung ermöglicht, was für digitale Unternehmen unerlässlich ist; aus diesem Grund sind sie auf der Suche nach Authentifizierungsmethoden mit höherer Sicherheit.

Cybersicherheits-Experten sollten diesen Bericht lesen, um zu verstehen, wie die Provider durch den Einsatz von Technologien Compliance- und Sicherheitsbedenken adressieren und gleichzeitig eine nahtlose Erfahrung für Unternehmenskunden bieten.

Compliance- und Governance-Experten wird in diesem Bericht vermittelt, wie der Benutzerzugriff auf Systeme und Daten verwaltet werden kann, um die Einhaltung von Vorschriften zu gewährleisten und Audits zu optimieren.

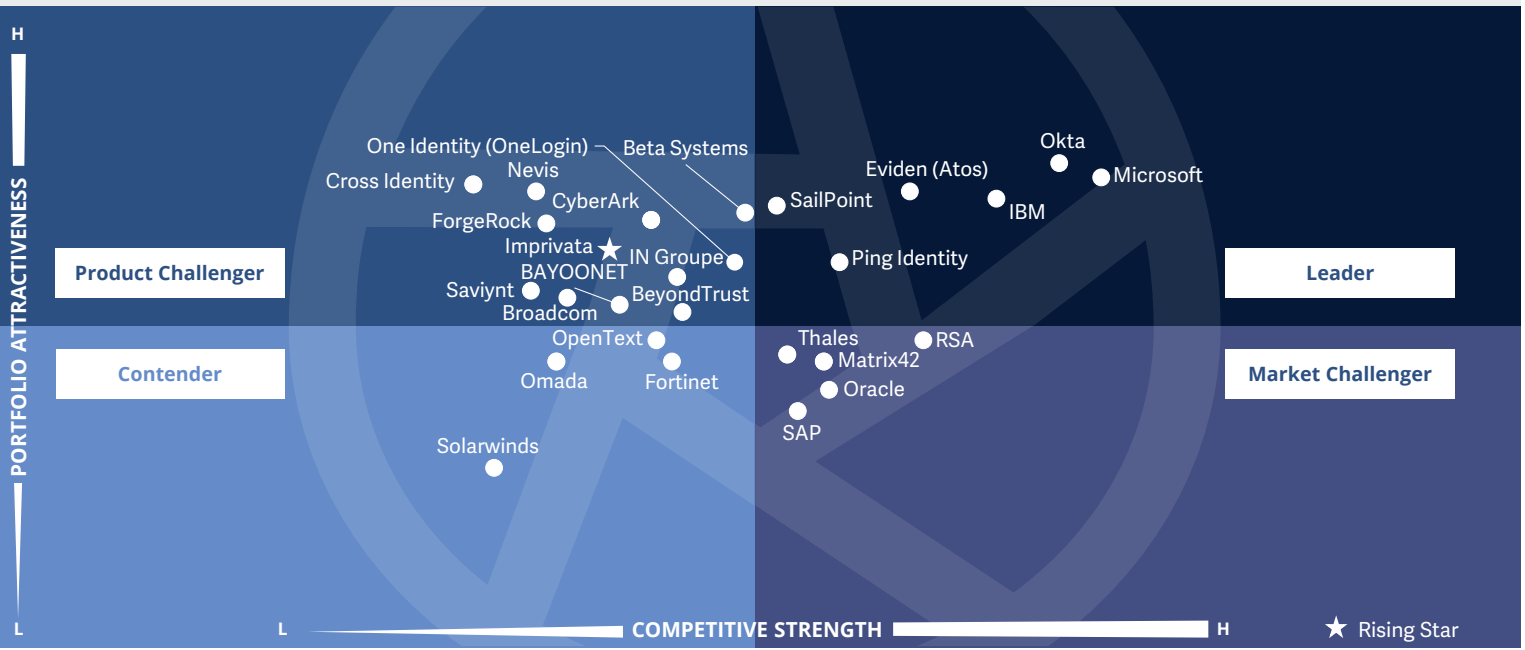
Strategie-Experten gewinnen aus diesem Bericht ein besseres Verständnis dahingehend, wie IAM-Tools die Benutzererfahrung verbessern und gleichzeitig die Sicherheit und Effizienz ihrer Systeme und Daten verbessern können.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Identity and Access Management (IAM)

Deutschland 2023



Dieser Quadrant bewertet die **relevantesten** IAM-Anbieter in Deutschland, ohne Anbieter, die keine eigene Software anbieten beziehungsweise betreiben. Zu den wichtigsten Themen gehören **SSO** und **MFA. Passwortlose Authentifizierung** wird immer bedeutender.

Frank Heuer

Definition

Die im Rahmen dieses Quadranten bewerteten IAM-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die Verwaltung von Benutzeridentitäten und -geräten in Unternehmen Dieser Quadrant umfasst auch SaaS-Angebote auf Basis von proprietärer Software. **Reine Dienstleister, die keine IAM-Produkte (On-Premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert**. Entsprechend den individuellen Unternehmensanforderungen können diese Angebote 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 dem Management (Erfassung, Aufzeichnung und Verwaltung) von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets auf Basis von Privileged Access Management (PAM), d.h. des Zugriffs anhand von definierten Policies.

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

Auswahlkriterien

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

Beobachtungen

Derzeit und zukünftig ist IAM ein besonders wichtiges Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch Maschinen und bestimmte Unternehmensbereiche (Industrie 4.0). Zudem nimmt die Anzahl zu verwaltender digitaler Identitäten stetig zu. Ein weiterer Faktor ist der Umzug vieler Mitarbeiter in das Home Office. Durch vermehrte Remote- und mobile Zugriffe auf die Unternehmensressourcen wird die Regulierung und Kontrolle des Zugriffs zunehmend wichtig. Dies resultiert auch in nochmals höheren 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 bieten 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. Anbieterseitig ist zudem zu erwähnen, dass Imprivata den letztjährigen Rising Star OGiTiX übernommen hat. Atos hat unter anderem sein Cybersecurity-Geschäft unter dem Namen „Eviden" (in der Studie als Eviden (Atos) aufgeführt) ausgelagert.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 27 für diesen Quadranten qualifizieren. Dabei erreichten sechs eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

EVIDEN an atos business

Eviden (Atos) ist ein innovativer Anbieter mit einem vielseitigen IAM-Portfolio und ist darüber hinaus in der Lage, seinen Kunden große Flexibilität bei der Wahl der Betriebsform ihrer Lösungen zu bieten.

IBM

IBM kann im Markt für Identity & Access-Management von seinem breiten Leistungsspektrum und seiner großen Marktpräsenz profitieren und punktet darüber hinaus mit starker Performance und einer hohen Integrationsfähigkeit.

Microsoft

Microsoft baut seine Position im Markt für Identity- & Access-Management-Lösungen geschickt mit Hilfe von bewährten Marketingrezepten, aber auch mit technologischen Verbesserungen des Produktes aus.

Okta

Der rein cloudbasierte Ansatz von **Okta** ermöglicht Kunden einen leichten Einstieg in IAM-Lösungen. Auch aufgrund dieses Vorteils baut Okta seine Position im deutschen Markt für Identity & Access Management immer weiter aus.

Ping Identity

Ping Identity bietet eine innovative IAM-Lösung an, die vielseitig einsetzbar ist. Auch aufgrund dieser Merkmale ist Ping Identity auch in Deutschland zunehmend erfolgreich.

SailPoint

SailPoint gelingt der Sprung unter die führenden Anbieter von Identity & Access Management in Deutschland. Gründe sind zum Beispiel die Unterstützung durch künstliche Intelligenz und die erleichterte IAM-Verwaltung von Multi-Cloud-Umgebungen.

Imprivata

Imprivata ist der „Rising Star" unter den Anbietern von Identity- & Access-Management-Lösungen in Deutschland. Hierzu trägt bei, dass Imprivata mit dem Gesundheitswesen auf eine Wachstumsbranche spezialisiert ist und eine flexible Möglichkeit der Nutzung offeriert.

Data Leakage/Loss Prevention (DLP) and Data Security

Wer diesen Bericht lesen sollte

Dieser Quadrant ist für Unternehmen in Deutschland relevant, um Anbieter von Data Leakage/Loss Prevention (DLP) und Datensicherheitslösungen zu evaluieren. Darüber hinaus wird bewertet, wie die einzelnen Anbieter Unternehmen bei der Bewältigung komplexer Sicherheitsherausforderungen im Zusammenhang mit dem Datenschutz und Datenverlusten unterstützen.

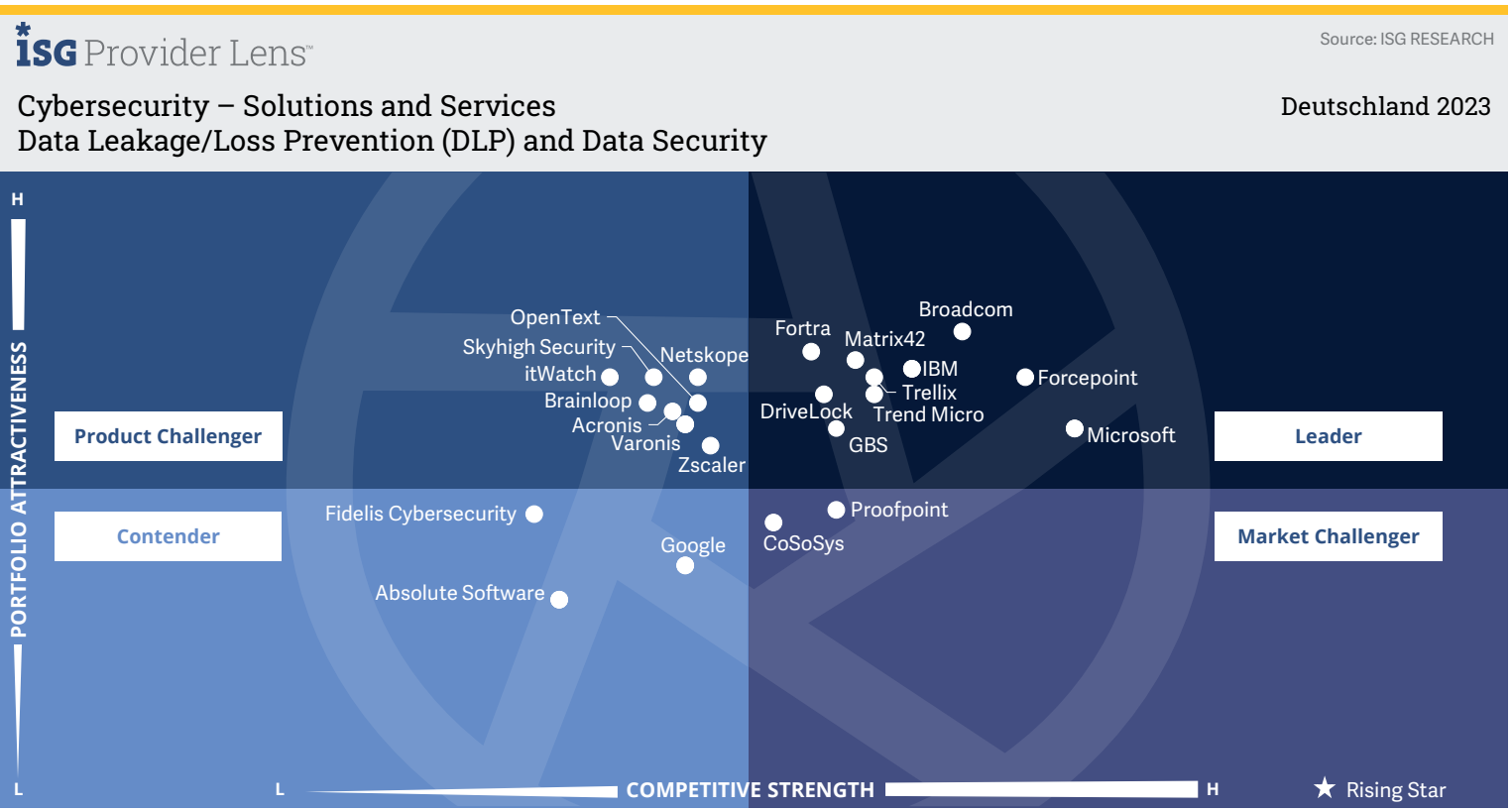
ISG gibt einen umfassenden Überblick über das Wettbewerbsumfeld in diesem Markt und stellt die aktuelle Positionierung dieser Anbieter dar.

In Deutschland ist die Nachfrage nach DLP-Lösungen in den letzten Jahren aufgrund verschiedener Faktoren, die sich auf die Datensicherheit in Unternehmen auswirken, deutlich gestiegen. Da immer mehr Unternehmen ihre Daten in die Cloud verlagern, hat Cloud-DLP auf dem Markt an Bedeutung gewonnen. DLP-Lösungen werden in Cloud Access Security Broker (CASB)-Lösungen integriert, um einen umfassenden Datenschutz in On-Premises- und Cloud-Umgebungen zu gewährleisten. Dank dieser Integration können Unternehmen den Datenfluss zwischen Cloud-Diensten überwachen und kontrollieren und so Einblicke in die Schatten-IT und nicht genehmigte Cloud-Anwendungen erhalten. Ein DLP-Lösungsangebot, das eine Analyse des Benutzerverhaltens (User Behavior Analytics, UBA) bietet, ist ein wesentliches Feature, das Unternehmen ein besseres Verständnis dafür vermittelt, wie Benutzer mit sensiblen Daten interagieren, und ungewöhnliche Aktivitäten erkennt, die auf eine eventuelle Datenverletzung hindeuten. Durch die Kombination von UBA und DLP erhalten Unternehmen einen umfassenderen Überblick über ihre Datensicherheitslage und können potenzielle Datendiebstähle und Verstöße proaktiv erkennen. API-gesteuertes DLP ist eine weitere wichtige Komponente von DLP-Lösungen. Durch die Automatisierung von Datenschutzprozessen in lokalen und cloudbasierten Anwendungen stellt API-gesteuertes DLP sicher, dass sensible Daten geschützt werden. Unternehmen integrieren auch Datenschutz- und Compliance-Maßnahmen in ihre DLP-Lösungen, um sicherzustellen, dass sie Vorschriften wie die DSGVO erfüllen.

Cybersicherheits-Experten sollten diesen Bericht lesen, um zu verstehen, wie Anbieter von DLP-Lösungen die Compliance- und Sicherheitsherausforderungen bewältigen und gleichzeitig weiterhin eine nahtlose Erfahrung für Unternehmen bieten.

Datenmanagement-Experten erfahren aus diesem Bericht, wie die Anbieter Informationen schützen, sich um den Datenschutz kümmern sowie die Themen Information Governance, Datenqualität und Datenlebenszyklusmanagement adressieren.

Strategie-Experten können sich mit diesem Bericht über die vielen potenziellen Alleinstellungsmerkmale von Lösungsanbietern informieren, die sie erreichen können, indem sie neue Kundenanforderungen besser adressieren.



Dieser Quadrant bewertet die **relevantesten** DLP-Anbieter in Deutschland, ohne Anbieter, die keine eigene Software anbieten beziehungsweise betreiben. **Die Relevanz des Schutzes von Daten** und geistigem Eigentum trägt zur Bedeutung des Marktes bei.

Frank Heuer

Definition

Die im Rahmen dieses Quadranten bewerteten DLP-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch SaaS-Lösungen auf Basis von proprietärer Software. **Reine Dienstleister, die keine DLP-Produkte (On-Premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert**. DLP-Lösungen können sensible Daten identifizieren und überwachen, 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 diversen Geräten gewährleisten.

Sie gewinnen erheblich an Bedeutung, da es für Unternehmen immer schwieriger wird, Datenbewegungen und -übertragungen zu kontrollieren (über ein Drittel aller Datenverletzungen sind auf eine interne Quelle zurückzuführen). Die Zahl der Geräte, einschließlich der Mobilgeräte, die zur Datenspeicherung genutzt werden, nimmt in Unternehmen zu. Sie sind mit einer Internetverbindung ausgestattet und können Daten senden und empfangen, ohne diese über ein zentrales Internet-Gateway zu leiten. Datensicherheitslösungen schützen Daten vor unbefugtem Zugriff, Offenlegung oder Diebstahl durch die Priorisierung, Klassifizierung und Überwachung von Daten (im Ruhezustand und bei der Übertragung); sie ermöglichen ein Security Reporting und helfen, die Sicherheit der gefährdeten Daten zu verbessern.

Auswahlkriterien

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

Beobachtungen

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

Die enorme Zunahme an Unternehmensdaten erfordert leistungsfähige DLP-Lösungen, die die Daten schnell aufspüren, klassifizieren und entsprechend ihrem Schutzbedarf vor unerlaubten Aktionen 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.

Anbieterseitig ist im DLP-Markt erwähnenswert, dass HelpSystems inzwischen unter dem Namen Fortra auftritt.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 23 für diesen Quadranten qualifizieren. Dabei erreichten zehn eine Position als Leader.

Broadcom

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

DriveLock

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

Forcepoint

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

Fortra

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

GBS

Neben den verstärkten Aktivitäten von **GBS** für eine erhöhte Präsenz im deutschen Markt tragen auch die ausgefeilte Technik und das Vier-Augen-Prinzip zum Erfolg bei.

IBM

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

Matrix42

Matrix42 bietet eine effiziente DLP-Lösung an, die über ein sehr breites Funktionsspektrum verfügt. Matrix42 bewirkt mit anwenderfreundlich geringen Beeinträchtigungen eine hohe Akzeptanz bei den Endusern – und fördert damit auch den erfolgreichen Einsatz der Lösung.

Microsoft

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

Trellix

Dank des übernommenen Unternehmens McAfee ist das Vertriebsnetz von **Trellix** in Deutschland sehr dicht. Darüber hinaus ist Trellix im Hinblick auf die Delivery durch seine starke lokale und internationale Präsenz sehr vielseitig aufgestellt.

Trend Micro

Seinen Erfolg im deutschen Markt für Data-Loss- & Data-Leakage-Prevention-Produkte hat **Trend Micro** insbesondere der Integrierbarkeit sowie der einfachen Einführung und Anwendung seiner DLP-Lösung zu verdanken.

Extended Detection and Response (XDR)

Wer diesen Bericht lesen sollte

Dieser Quadrant ist für Unternehmen in Deutschland relevant, um Anbieter von Extended Detection & Response (XDR) Lösungen zu evaluieren. Darüber hinaus wird bewertet, wie die einzelnen Anbieter Unternehmen dabei helfen, die Transparenz über alle Telemetriequellen hinweg zu erhöhen und eine einheitliche Sicht auf die Erkennung von und Reaktion auf Bedrohungen zu erhalten.

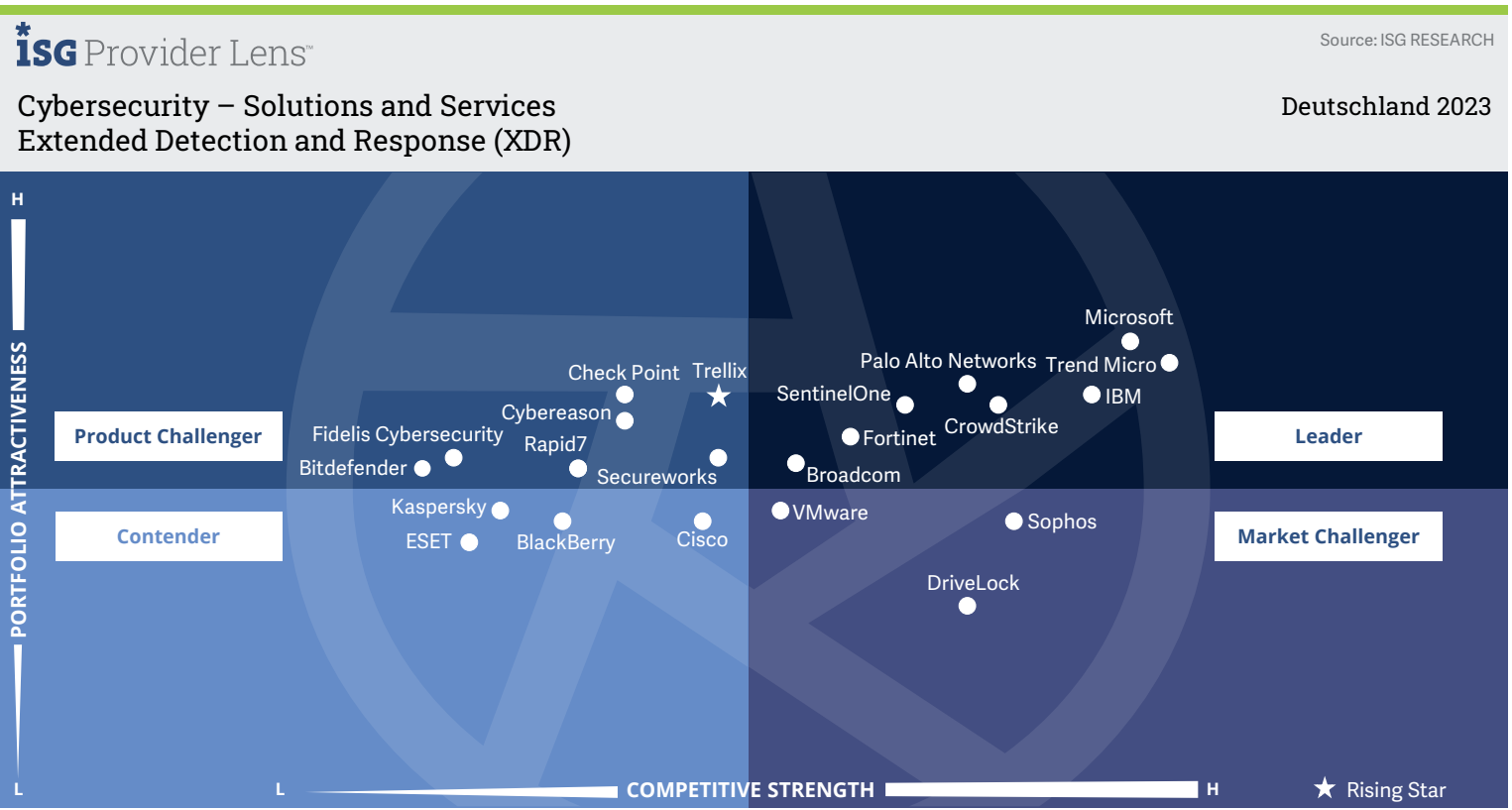
ISG gibt einen umfassenden Überblick über das Wettbewerbsumfeld in diesem Markt und stellt die aktuelle Positionierung dieser Anbieter dar.

XDR ist eine fortschrittliche Cybersicherheitslösung, die mehrere Sicherheitstechnologien integriert, u.a. Endpoint Detection & Response (EDR), Network Detection & Response (NDR) und Security Information & Event Management (SIEM), um umfassendere Funktionen zur Erkennung von und Reaktion auf Bedrohungen zu bieten. Für Unternehmen mit hochentwickelten Sicherheitsfunktionen kann XDR die Einhaltung mehrerer Sicherheitskonzepte gewährleisten, u.a. Secure Access Service Edge (SASE) und Zero Trust; dazu werden Daten aus verschiedenen Sicherheitsquellen, einschließlich Endpunkten, Netzwerken und Cloud-Umgebungen, erfasst und analysiert. XDR nutzt fortschrittliche Analysen und maschinelles Lernen zum Erkennen und Priorisieren von Bedrohungen und bietet automatisierte Reaktionsmaßnahmen, um diese Bedrohungen zu entschärfen. Durch die Integration von XDR mit SSE erhalten Unternehmen eine durchgängige Transparenz und Kontrolle über ihre gesamte Sicherheitsumgebung, einschließlich Remote-Mitarbeiter, Zweigstellen und Cloud-Anwendungen. Dies ermöglicht einen umfassenden Ansatz zur Erkennung von und Reaktion auf Bedrohungen und macht Compliance und Reporting einfacher. XDR-Lösungen sind komplex, deshalb erfordert ihre Bereitstellung, Konfiguration und Wartung umfassendes Fachwissen. XDR muss modernste KI- und ML-Innovationen einbeziehen, um Bedrohungen aufzuspüren und Angriffe zu antizipieren; das hilft Unternehmen, auf komplexe Bedrohungen in der sich schnell entwickelnden Bedrohungslandschaft zu reagieren.

Cybersecurity-Experten bietet dieser Bericht wertvolle Einblicke in XDR-Lösungen, die Unternehmen bei der Verbesserung der Sichtbarkeit über Endpunkte hinweg helfen, um eine einheitliche Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

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

Strategie-Experten sollten diesen Bericht lesen, um die Fähigkeiten von XDR-Anbietern zu verstehen, die Unternehmen dabei helfen, Sicherheitsrisiken effektiv zu verwalten und fundierte Entscheidungen über ihre Sicherheitsstrategie zu treffen.



Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich dadurch aus, dass sie eine Plattform anbieten, die Daten und Warnungen aus **verschiedenen Quellen** zur **Bedrohungsabwehr**, –erkennung und -reaktion **integriert und korreliert**.

Frank Heuer

Definition

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich dadurch eine Plattform aus, die Daten und Warnungen aus verschiedenen Komponenten zur Bedrohungsabwehr, -erkennung und -reaktion integriert, korreliert und kontextualisiert. XDR ist eine aus der Cloud bereitgestellte Technologie, die Multipoint-Lösungen umfasst und anhand von fortschrittlichen Analysen Warnmeldungen aus mehreren Quellen, unter anderem auch von schwachen Einzelsignalen, mit Vorfällen korreliert, um so die Erkennung zu präzisieren. XDR-Lösungen konsolidieren und integrieren mehrere Produkte und sind auf umfassende Arbeitsplatz-, Netzwerk- oder Workload-Sicherheit ausgelegt. Sie zielen normalerweise darauf ab, die Transparenz und den kontextuellen Rahmen der identifizierten Bedrohung und deren Kontext unternehmensweit zu verbessern. Daher verfügen diese Lösungen über spezifische Merkmale, u.a. Telemetrie und kontextbezogene Datenanalyse, Erkennung und Reaktion. XDR-Lösungen umfassen mehrere Produkte und Lösungen, die in einer einzigen Konsole integriert sind, so dass man dank ausgefeilter Funktionen Bedrohungen sehen, erkennen und darauf entsprechend darauf reagieren kann. Der hohe Automatisierungsgrad und die kontextbezogene Analyse bieten spezifische Reaktionsmöglichkeiten, die auf das betroffene System zugeschnitten sind und Warnmeldungen nach Schweregrad im Vergleich zu bekannten Referenz-Frameworks priorisieren. **Reine Dienstleister, die keine XDR-Lösungen auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert**. XDR-Lösungen zielen darauf ab, die Produktvielfalt, die Alarmmüdigkeit, die Integrationsprobleme und die Betriebskosten zu reduzieren, und eignen sich besonders für Sicherheitsteams, die Schwierigkeiten damit haben, ein Best-of-Breed-Lösungsportfolio zu verwalten oder einen Mehrwert aus einer Security Information & Event Management (SIEM) oder Security, Orchestration, Automation & Response (SOAR)-Lösung zu generieren.

Auswahlkriterien

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

Beobachtungen

Lösungen für XDR haben in den letzten zwei Jahren an Bedeutung gewonnen und sich durchgesetzt. Unternehmen wollen die Informationen, die sie aus der breiten Palette der in ihrer IT-Infrastruktur eingesetzten Sicherheitstools gewinnen, besser verstehen und im Zusammenhang betrachten (korrelieren). Der Markt setzt sich aus offenen und nativen XDR-Tools zusammen. ISG hat in diesem Quadranten native XDR-Anbieter berücksichtigt. Sie werden von Unternehmen bevorzugt, weil sie in der Lage sind, ohne weiteres eine integrierte Produktsuite anzubieten.

Die Anbieter haben ihre XDR-Kompetenzen auf der Grundlage ihrer bestehenden Präsenz auf dem Markt für Endpoint Detection & Response (EDR) aufgebaut, wobei einige von ihnen von ihrem ebenfalls bestehenden Netzwerk- und Cloud-Portfolio profitieren. Natives XDR bietet eine sofortige, vorteilhafte Integrationsmöglichkeit in bestehende native oder proprietäre Produkte.

Unternehmen bevorzugen inzwischen aus Rationalisierungsgründen solche Plattformen eines einzigen Anbieters. XDR-Lösungen sind hochgradig automatisiert und korrelieren Protokolle, Warnungen und Benachrichtigungen aus internen und externen Quellen, was zu einer verbesserten Bedrohungsanalyse führt.

Führende Produkte enthalten auch verhaltens- und kontextbezogene Analysemodule, um Angriffsvektoren und die Angriffskette besser zu verstehen, und haben im letzten Jahr an Bedeutung gewonnen. Die meisten führenden Anbieter offerieren auch eine offene Integration mit anderen EDR- und NDR-Produkten, um die Integration zu erleichtern. Starke XDR-Produkte zeichnen sich durch übersichtliche Dashboards und eine einheitliche Konsole aus.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 22 für diesen Quadranten qualifizieren. Dabei erreichten acht eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Broadcom

Broadcom bietet Echtzeit-Transparenz und -Verwaltung von Bedrohungen in lokalen, cloudbasierten oder hybriden Infrastrukturen auf Basis einer einheitlichen Konsole.

CrowdStrike

Die cloud-native, KI-gestützte Plattform von **CrowdStrike** erkennt Verhaltensmuster, um Sicherheitsbedrohungen analysieren und sie in Echtzeit bekämpfen zu können.

Fortinet

Fortinet bietet eine robuste Grundlage für XDR, mit einer gemeinsamen Datenstruktur und einheitlicher Sichtbarkeit. Die Lösung ermöglicht automatisierte Analysen, die Untersuchung von Vorfällen und vordefinierte Bedrohungsreaktionen.

IBM

Die Übernahme von ReaQta durch **IBM** hat das XDR-Portfolio und die Marktpräsenz des Unternehmens gestärkt. IBM profitiert von seinen umfassenden Sicherheitslösungen und zudem von der QRadar-Suite und kann so eine starke Lösung anbieten.

Microsoft

Microsoft hat aufgrund der Benutzerfreundlichkeit und der fortschrittlichen Funktionen seiner Endpoint-Lösung auf dem Markt erheblich an Boden gewonnen.

Palo Alto Networks

Palo Alto Networks hat auf Basis seines Portfolios und künstlicher Intelligenz eine leistungsfähige XDR-Lösung geformt. Die Lösung ist umfassend mit breiter Abdeckung und ermöglicht schnellere Prioritätensetzung und Untersuchungen.

SentinelOne

SentinelOne hat Attivo Networks übernommen und kann so die Fähigkeiten der Singularity XDR-Plattform nutzen, um Bedrohungen über Endpunkte, Cloud Workloads, IoT-Geräte, Mobilgeräte und Daten hinweg zu entschärfen.

Trend Micro

Trend Micro ermöglicht es Anwendern, Sicherheits- und Untersuchungsfunktionen hinzuzufügen, und bietet Bedrohungserkennung, Reaktion und Analyse in einem einzigen Agenten.

Trellix

Trellix (Rising Star) überwacht Bedrohungen und Verhaltensweisen, um Angriffe zu bekämpfen. Dazu werden ein breites Spektrum an Funktionen sowie Bedrohungsdaten in Echtzeit genutzt. Trellix nutzt KI-gesteuerte Analysen, um Bedrohungen schnell priorisieren und bekämpfen zu können.

Security Service Edge (SSE)

Wer diesen Bericht lesen sollte

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

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

Mit der zunehmenden Cloud-Nutzung benötigen Unternehmen eine robuste Sicherheitslösung, um digitale Ressourcen zu schützen und ihren Mitarbeitern einen sicheren Zugang zu ermöglichen. Diese Lösungen sind nutzerorientiert und bieten den Endanwendern Sicherheit über die Cloud, anstatt ihnen den zentralen Zugriff auf Unternehmensanwendungen und Datenbanken über dedizierte Netzwerke zu gewähren.

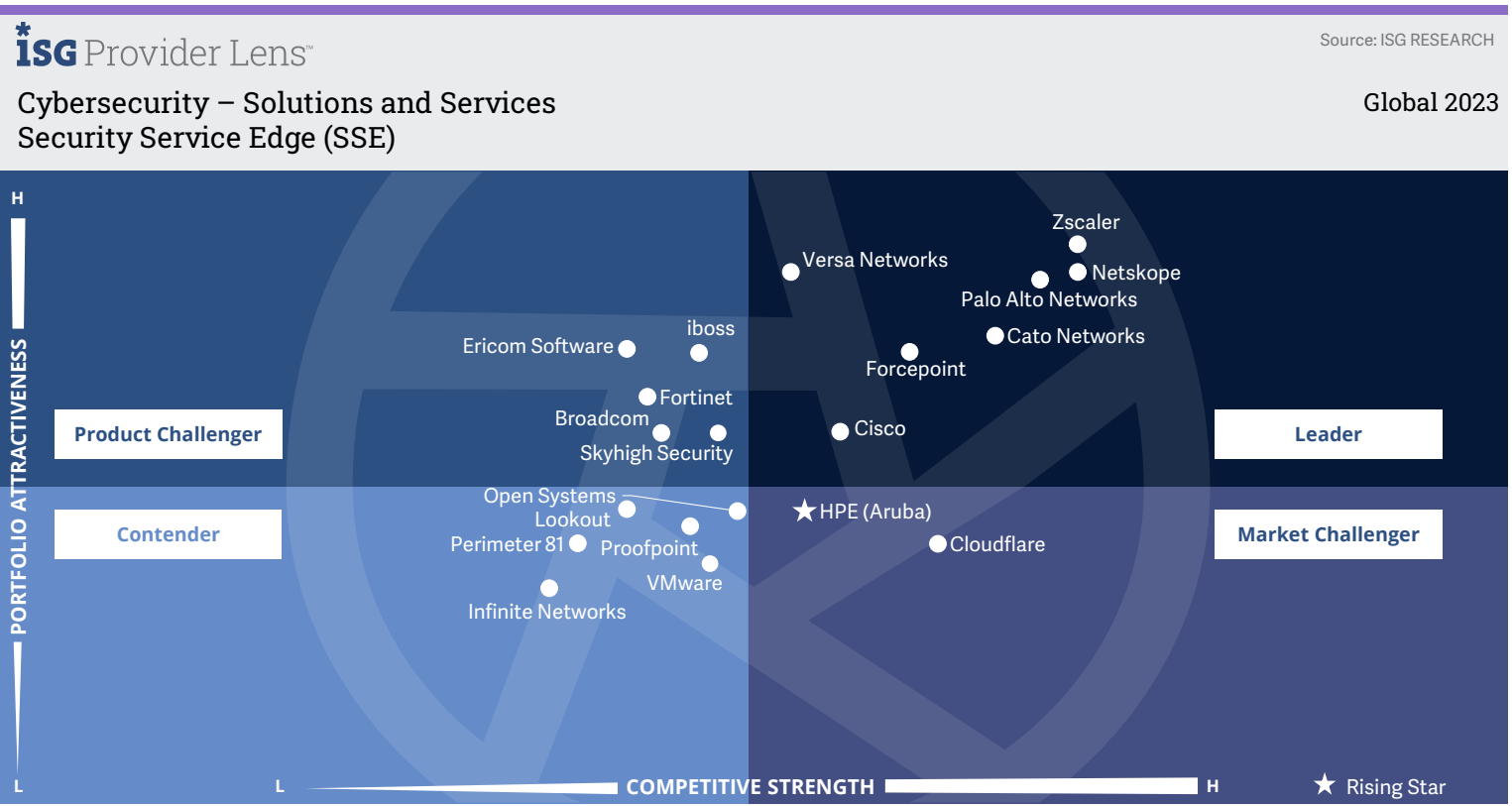
Da Unternehmen Security und Remote Access Services in einem einzigen Framework konsolidieren, ist mit SSE-Angeboten eine einheitliche Verwaltungskonsole für die Echtzeit-Transparenz von Sicherheitsereignissen in der gesamten Sicherheitsinfrastruktur möglich. Diese Vereinheitlichung hilft Unternehmen bei der Einhaltung diverser Sicherheitsvorschriften und -standards, denn so wird ein einzigen Kontrollpunkt für Sicherheitsrichtlinien und -konfigurationen bereitgestellt.

SSE-Lösungen verbessern die Effizienz der Sicherheitsabläufe in Unternehmen und erfreuen sich zunehmender Beliebtheit als Testlauf vor der Implementierung von Secure Access Service Edge (SASE)-Lösungen. SSE-Anbieter müssen angemessene technische Unterstützung und eine solide Integration mehrerer Sicherheitskomponenten bieten. Unternehmen setzen zunehmend auf spezifische Sicherheitsfunktionen für Webanwendungen und APIs sowie auf automatisierte erweiterte Analysefunktionen wie User Entity Behavior Analytics (UEBA).

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

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

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



Die in diesem Quadranten bewerteten SSE-Lösungsanbieter zeichnen sich dadurch aus, dass sie Lösungen für einen **sicheren Zugang** zu Cloud-Diensten, SaaS-Anwendungen, Webdiensten und privaten Anwendungen ermöglichen.

Gowtham Kumar Sampath

Definition

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

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

Die Netzwerkkomponenten von Secure Access Secure Edge (SASE), wie SD-WAN oder Mikrosegmentierung, werden in diesem Quadranten nicht berücksichtigt, werden aber in der Studie „Network – Software-Defined Solutions & Services" behandelt.

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

In dieser Studie werden die SSE-Anbieter auf der globalen Ebene analysiert.

Auswahlkriterien

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

Beobachtungen

Security Service Edge (SSE) ist ein neuer Quadrant, der auf globaler Ebene analysiert wird, da sich dieses Thema in einem frühen Stadium der Reife und Akzeptanz bei Unternehmen befindet. SSE umfasst Lösungen, die Unternehmen einen sicheren Zugang zur Cloud ermöglichen, die Remote-Arbeit erleichtern, Edge-Computing-Lösungen absichern und die digitale Transformation unterstützen.

Die wachsende Zahl von Remote- und Hybrid-Mitarbeitern und der Übergang zur Cloud haben das Umfeld für SSE-Lösungen geschaffen. Die Verwendung von VPNs erhöht die Wahrscheinlichkeit von Sicherheitsverletzungen aufgrund fehlender Patches. Unter anderem aus diesem Grund entwickelt sich SSE zu einer praktikablen Option für den sicheren Zugriff auf Unternehmensdaten. Unternehmen sehen sich mit Budgetbeschränkungen konfrontiert und sind im Hinblick auf die Rentabilität bei der Nutzung von Premium-Lösungen wie AWS Direct Connect oder Microsoft ExpressRoute zurückhaltend.

Die SSE-Anbieter ermöglichen eine einheitliche Sicht auf das System; sie kombinieren Betriebs- und Gerätedaten, um eine verbesserte Sichtbarkeit im gesamten Unternehmen mit automatisierten Warnmeldungen, Fernüberwachung und -verwaltung sowie Sicherheitsüberwachung gewährleisten zu können. Im Markt sind zum einen offene und zum anderen native SSE-Produkte verfügbar; Unternehmen bevorzugen native oder konvergierte SSE-Lösungen, um von den Vorteilen einer integrierten Produktsuite und einer verbesserten Interoperabilität mit bestehenden Sicherheitstools zu profitieren. Die Anbieter investieren kontinuierlich in Innovationen, um der sich anbahnenden Bedrohungen Herr zu werden. Neben einem sicheren Zugriff auf die Cloud nutzen Unternehmen SSE, um einen umfassenden Einblick in die Schatten-IT zu erhalten; dazu zählen unter anderem vom Unternehmen nicht genehmigte Anwendungen, Geräte und Internetnutzung.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 20 für diesen Quadranten qualifizieren. Dabei erreichten sieben eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Cato Networks

Cato Networks bietet eine native, konvergente Lösung, deren Stärke in den SASE-Funktionen liegt. Angesichts des Interesses an der schrittweisen Einführung von SSE, um SASE zu realisieren, hat das Unternehmen sein „SSE 360" als Kernstück seines Portfolios positioniert.

Cisco

Cisco „Umbrella" ist eine konvergente Lösung, die auf einer hauseigenen KI-Engine und Playbooks mit Elementen von DLP, XDR und Threat Hunting basiert und die Transparenz und Effizienz, die Untersuchung von Bedrohungen sowie die Beseitigung von Störungen umfassend verbessert.

Forcepoint

Forcepoint hat seine SSE-Architektur und -Roadmap durch strategische Übernahmen wie die von BitGlass und Cyberinc ausgebaut und damit seine datenbasierte SSE-Plattform konsolidiert.

Netskope

Netskope wuchs im vergangenen Jahr mit SSE beträchtlich, und zwar auf Basis seiner SASE-Kompetenzen und der Erweiterung des Angebots um Echtzeit-Kontrollen sowie eines stärkeren Fokus auf die Verbesserung der Benutzerfreundlichkeit und der kontinuierlichen Leistungssteigerung.

Palo Alto Networks

Palo Alto Networks wuchs im vergangenen Jahr mit SSE signifikant und verfolgt die Strategie, ZTNA 2.0 zu adressieren. Dies zielt auf die Anforderungen für die Absicherung von hybriden Unternehmen und Remote-Arbeitskräften mit sofort einsatzbereiten Konfigurationen ab.

Versa Networks

Versa Networks bietet mehrere Produkte an, die auf die Herausforderungen von Zero Trust und Remote-Arbeit ausgerichtet sind. Die Lösung nutzt KI, um die Sicherheitslage von Benutzern und Geräten zu überwachen und so die Genauigkeit der Bedrohungserkennung zu verbessern.

Zscaler ist mit Zero Trust Exchange weiterhin Marktführer im Bereich SASE; die Lösung zielt darauf ab, Geschäftsrisiken zu adressieren und Unternehmen bei der digitalen Transformation zu unterstützen.

HPE (Aruba) (Rising Star) hat mit der Übernahme von Axis Security den Einstieg in den SSE-Markt vollzogen und an Dynamik gewonnen. In Kombination mit der Partnerschaft mit Lookout helfen die SSE-Funktionen Kunden, die Überwachung der Schatten-IT zu verbessern.

Technical Security Services

Wer diesen Bericht lesen sollte

Mit diesem Quadranten will ISG Unternehmen in Deutschland branchenübergreifend bei der Bewertung von Anbietern von technischen Sicherheitsdiensten unterstützen, die auf die Implementierung und Integration von Sicherheitsprodukten oder -lösungen spezialisiert sind. Der Bericht fokussiert sich auf Provider, die nicht nur Dienste für ihre eigenen Produkte anbieten, sondern auch Lösungen anderer Anbieter integrieren können.

ISG definiert die aktuelle Marktpositionierung dieser Anbieter und zeigt auf, wie die einzelnen Anbieter kritische Sicherheitsherausforderungen angehen.

Die zunehmende Komplexität der Sicherheitsbedrohungen und der Bedarf an spezialisiertem Fachwissen zur Bekämpfung dieser „Advanced Threats" tragen zur Nachfrage nach technischem Know-how bei. OT-Sicherheit hat an Bedeutung gewonnen, und so wird die Zusammenarbeit zwischen IT- und OT-Teams immer wichtiger, um sicherzustellen, dass Sicherheitsmaßnahmen in alle Systeme und Geräte integriert werden.

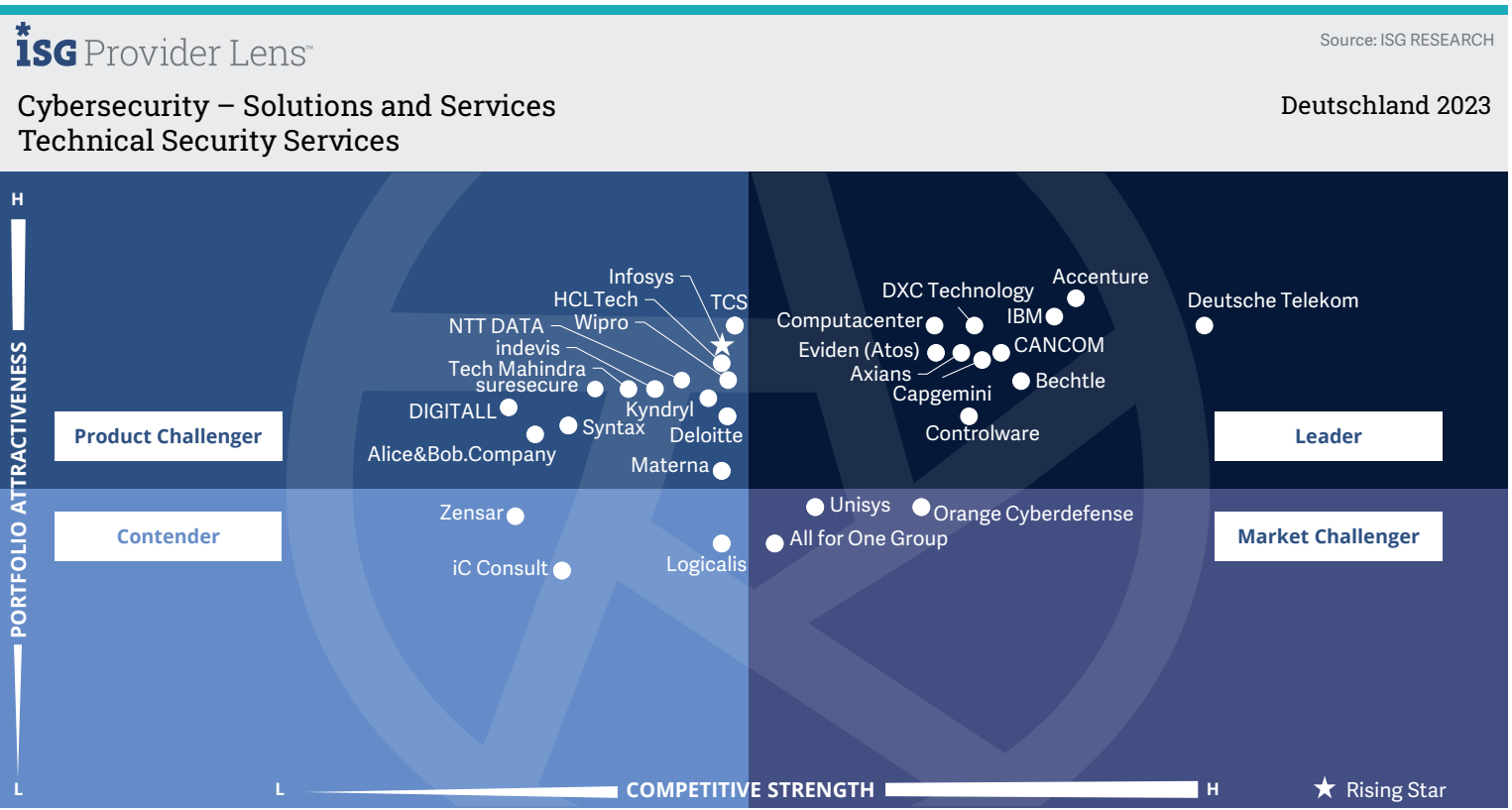
Regelmäßige Schwachstellenbewertungen und Penetrationstests können dabei helfen, potenzielle Sicherheitsrisiken zu erkennen und zu beseitigen; der Einsatz von cloudbasierten Sicherheitslösungen wiederum kann dazu beitragen, Cyberangriffe auf vernetzte OT-Geräte zu neutralisieren. Unternehmen suchen Hilfe bei der Implementierung von Frameworks für die Sicherheitsarchitektur, die standardisierte Playbooks und Roadmaps anbieten, um Kunden bei der Transformation ihrer bestehenden Sicherheitsumgebung mit Hilfe von Best-of-Breed-Tools und Methoden für das Security Design zu unterstützen. Das hilft, das Security Management zu vereinfachen, die Kosten zu senken und die Wirksamkeit der Sicherheitsmaßnahmen zu verbessern.

Die technologische Konsolidierung erhöht auch die Nachfrage nach technischem Know-how und Implementation Engineering, da die Unternehmen die Sicherheitsverwaltung vereinfachen, die Kosten senken und die Wirksamkeit der Sicherheitsmaßnahmen verbessern müssen. Es werden zudem immer mehr Lösungen für die Verwaltung von Identitäten und Zugriffsrechten implementiert.

Technologie-Experten sollten diesen Bericht lesen, um die Integrationsmöglichkeiten der Anbieter zu verstehen, die anhand fortschrittlicher Technologien zur Transformation von Altsystemen die Auswirkungen von Bedrohungen verringern.

Sicherheits- und Datenexperten gewinnen durch diesen Bericht Einblicke in die Einhaltung der Sicherheits- und Datenschutzgesetze durch die Anbieter und können sich über Markttrends auf dem Laufenden halten.

Experten aus den Fachabteilungen hilft dieser Bericht, Datensicherheit, Kundenerfahrung und Datenschutz inmitten der derzeit so wichtigen digitalen Transformation in Balance zu bringen.



Dieser Quadrant bewertet die **relevantesten** Dienstleister für technische Security Services, ohne Anbieter, die ihre Leistungen nur auf eigene Produkte beziehen. Externe Dienstleister werden **immer wichtiger**, um IT-Security-Systeme auf dem Laufenden zu halten.

Frank Heuer

Definition

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

TSS Provider bieten standardisierte Playbooks und Roadmaps an, die dabei helfen, eine bestehende Sicherheitsumgebung mit den besten Tools und Technologien umzugestalten, den Sicherheitsstatus zu verbessern und die Auswirkungen von Bedrohungen zu reduzieren. Ihre Portfolios sollen u.a. die vollständige oder individuelle Transformation einer bestehenden Sicherheitsarchitektur mit relevanten Produkten in Bereichen wie Netzwerken, Cloud, Arbeitsplatz, OT, IAM, Datenschutz und -sicherheit, Risiko- und Compliance-Management und SASE ermöglichen. Die Angebote beinhalten zudem die Identifizierung von Produkten oder Lösungen, Bewertung, Design und Entwicklung, Implementierung, Validierung, Penetrationstests, Integration und Bereitstellung. Die Anbieter setzen auch hochentwickelte Lösungen ein, die anhand von umfassenden Schwachstellen-Scans über Anwendungen, Netzwerke, Endgeräte und einzelne Benutzer hinweg Schwachstellen aufdecken und externe und interne Bedrohungen entschärfen.

TSS Provider investieren in den Aufbau von Partnerschaften in den Bereichen Sicherheitstechnologie, Cloud, Daten und Netzwerke; so erhalten sie spezialisierte Akkreditierungen und erweitern ihren Tätigkeitsbereich und ihr Portfolio. Dieser Quadrant umfasst auch klassische Managed Security Services, also Services, die ohne ein Security Operations Center (SOC) erbracht werden.

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.

Auswahlkriterien

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

Beobachtungen

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

Mittelständler zeigen nach wie vor besonderen Nachholbedarf, da sie besonders häufig unter dem IT-Fachkräftemangel, Überforderung oder mangelndem Kapital leiden. Die zunehmenden, komplexeren Sicherheitsbedrohungen und die verschärften gesetzlichen Regelungen bewegen diese Firmen jedoch immer häufiger zum Handeln, wofür in vielen Fällen externe Unterstützung erforderlich ist. Mittelständler wissen dabei häufig die lokale Präsenz der Dienstleister für kurze Wege und unkomplizierte, schnelle Unterstützung zu schätzen.

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

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

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.

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

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten 11 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

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

axians

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

BECHTLE

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

CANCOM

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

Capgemini

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

Computacenter

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

Controlware

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

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

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

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

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

Ein umfangreiches, innovatives Portfolio und starkes Wachstum machen **Infosys** zum „Rising Star" für Technical Security Services in Deutschland. Zur Innovation trägt auch das Cyber Security Center of Excellence bei.

Strategic Security Services

Wer diesen Bericht lesen sollte

Dieser Quadrant soll Unternehmen in Deutschland branchenübergreifend bei der Evaluierung von Dienstleistern helfen, die sich auf strategische Sicherheitsservices (SSS) spezialisiert haben und in der Lage sind, den Sicherheitsreifegrad und die Risikolage zu bewerten und maßgeschneiderte Cybersicherheitsstrategien für Unternehmen zu definieren.

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

Unternehmen sind bestrebt, ihr Cyberrisiko durch eine rasche Transformation ihrer Sicherheitssysteme zu verringern. Sie müssen ihre digitalen Werte und geschäftskritischen Daten schützen, ihre Gefährdung reduzieren und auf zukünftige Bedrohungen in der sich ständig verändernden Bedrohungslandschaft vorbereitet sein. Sicherheitsberater helfen ihnen bei einer umfassenden Risikobewertung mit komplexen Sicherheitstests wie Red & Purple Teaming, um Sicherheitslücken aufzudecken. Die Anbieter unterstützen Unternehmen nicht nur bei der Entwicklung robuster Sicherheitsstrategien und -Roadmaps, sondern helfen ihnen auch bei der Entwicklung einer Sicherheitskultur. Sie bieten Services und Schulungen für mehr Sicherheitsbewusstsein für Vorstandsmitglieder, wichtige Führungskräfte und Mitarbeiter, um sie besser mit Cybersecurity-Themen vertraut zu machen und Best Practices einzuführen, damit sie besser auf tatsächliche Bedrohungen und Cyber-Angriffe reagieren können. Durch die Zusammenarbeit mit Sicherheitsberatern können Unternehmen ihre Sicherheitsfunktion verbessern und die Rolle des CISO im Unternehmen stärken. Unternehmen müssen auch gesetzliche Vorschriften und Compliance-Vorschriften in ihre Sicherheitsprogramme integrieren und benötigen Governance-Modelle, um ihre Cyberrisiko-Situation zu verbessern und entsprechend beizubehalten. Sie nutzen kontinuierlich die Erkenntnisse aus der Überwachung und Berichterstattung über kritische Kennzahlen wie die Anzahl der aufgedeckten und behobenen Sicherheitsvorfälle; so können sie die richtigen Kontrollen, Richtlinien, Technologien und Verfahren priorisieren und die Compliance-Risiken ermitteln.

Cybersecurity-Experten erhalten durch diesen Bericht einen umfassenderen Überblick über Sicherheitstrends. Er zeigt auf, mit welchen Leistungen die Anbieter Unternehmen bei der Ausarbeitung robuster Sicherheitsstrategien unterstützen.

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

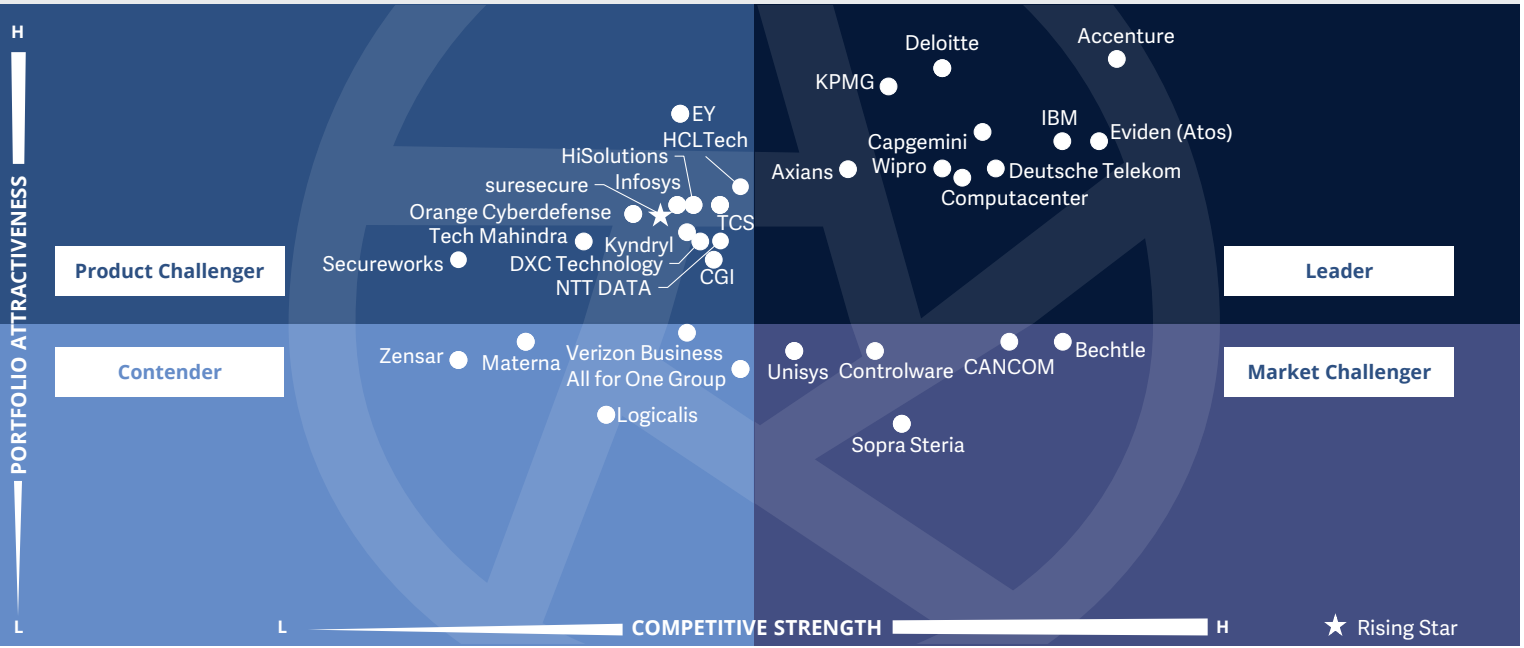
Technologie-Experten gewinnen durch diesen Bericht Einblicke in die neuen Trends in der Sicherheitslandschaft und die Fähigkeiten der Anbieter, maßgeschneiderte Sicherheitsplattformen zu entwickeln.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Strategic Security Services

Deutschland 2023



Dieser Quadrant bewertet die **relevantesten** Cybersecurity-Berater in Deutschland, die ihre Leistungen nicht nur auf ihre eigenen Produkte beziehen. Aufgrund zunehmender Cyberbedrohungen suchen Unternehmen **vermehrt nach externer Unterstützung** und Orientierung.

Frank Heuer

Definition

Die in diesem Quadranten bewerteten Provider von Strategic Security Services (SSS) bieten Beratung für IT- und OT-Sicherheit an. Die abgedeckten Services umfassen Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zur Architektur von Sicherheitslösungen sowie Aufklärung und Schulungen. Diese Services dienen der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition einer auf die individuellen Anforderungen zugeschnittenen Cybersecurity-Strategie für Unternehmen.

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

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

Auswahlkriterien

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

Beobachtungen

Die Cybersecurity-Gefährdungssituation nimmt weiter zu – aktuell auch durch den Ukraine-Krieg angefacht. Dies bewirkt zusammen mit mangelnden Ressourcen ein zunehmendes Bedürfnis nach Orientierung hinsichtlich Cybersicherheit. Perspektivisch zeichnen sich zudem neue, technisch ausgefeilte Bedrohungen ab.

Angesichts der immer intensiveren und raffinierteren Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Hiervon sind schon lange nicht mehr nur die bekannten großen Unternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelgroße Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin; darunter leiden besonders die mittelgroßen Unternehmen.

Diese Faktoren bewirken, dass Unternehmen zunehmend externe Unterstützung benötigen. Am Anfang steht hierbei häufig die Beratung.

Großunternehmen zählen weiterhin zu den wichtigsten Nachfragern von Strategic Security Services. Aus den oben beschriebenen Gründen nehmen auch mittelständische Firmen diese Leistungen zunehmend in Anspruch. Anbieter mit einer ausgewogenen Kundenstruktur aus Großkunden und mittelständischen Unternehmen profitieren sowohl von den umfangreichen Budgets der Großkunden als auch vom überdurchschnittlichen Nachfragewachstum der Mittelständler.

Des Weiteren sind Dienstleister, die ihren Kunden neben Sicherheitsberatung auch -Umsetzung und -Betrieb anbieten können, damit die Strategie bruchlos in die Tat umgesetzt werden kann, im Vorteil, ebenso wie Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen aus einem Guss anbieten können.

Erste Berater stellen sich auf die Abwehr von quantum-basierenden Cyberattacken ein.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 33 für diesen Quadranten qualifizieren. Dabei erreichten 10 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

Wir sind uns der Präsenz von PwC auf dem Markt bewusst, haben aber beschlossen, das Unternehmen aufgrund unzureichender Informationen in diesem Jahr nicht in der Studie zu positionieren.

accenture

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

axians

Axians kann im deutschen Markt für Cybersecurity Consulting mit pragmatischen, zielgerichteten Lösungen speziell bei mittelständischen Unternehmen punkten. Axians entwickelt sein Portfolio darüber hinaus dynamisch weiter.

Capgemini

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

Computacenter

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

Deloitte.

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

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

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

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

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

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

suresecure profiliert sich mit seiner überaus dynamischen Entwicklung als „Rising Star" für Strategic Security Services in Deutschland. Das Spektrum der Beratungsleistungen ist gerade für einen jungen Dienstleister umfangreich.

Rising Star

„suresecure profiliert sich mit seiner überaus dynamischen Entwicklung als ‚Rising Star' für Strategic Security Services in Deutschland."

Frank Heuer

suresecure

Übersicht

Die 2017 gegründete suresecure GmbH ist ein reiner Cybersicherheits-Dienstleister aus Düsseldorf. 2022 stellte suresecure den einhundertsten Mitarbeiter ein. Der Fokusmarkt ist Deutschland. Strategic Security Services sind im Portfolio suresecures Teil der kompletten Wertschöpfungskette aus Strategie – Beratung – Implementierung – Betrieb. Bedeutende Elemente des Beratungsangebotes von suresecure sind [secure]check und [secure]assessment. Ergänzend zu den klassischen Leistungen der Wertschöpfungskette hat suresecure mit securance eine Maklerfirma gegründet, die Versicherungen im Cyberbereich vermittelt, und zwar mit dem Know-how eines IT-Beratungshauses.

Stärken

Breites Portfolio: Das Spektrum der Strategic Security Services von suresecure ist gerade für einen jungen Dienstleister umfangreich und lässt keine Wünsche offen. Unter anderem mit zielgerichteten Workshops weckt suresecure das Verständnis, dass IT-Security ein wichtiger Bestandteil der Unternehmensstrategie sein muss.

Kundenorientiertes Preismodell: suresecure ist bereit, kundenorientiert ein Risiko einzugehen. Im Gegensatz zu vielen anderen Anbietern offeriert suresecure auch ein ergebnisbasiertes Preismodell. Dies schafft Vertrauen bei (potenziellen) Kunden, da suresecure hiermit deutlich das Vertrauen in die hohe Qualität der eigenen Leistungen demonstriert.

Nutzung von Erfahrungen: Die Erfahrungen aus Sicherheitsvorfällen und allen Sicherheitsereignissen, die in das SOC einfließen, helfen suresecure, auf dem neuesten Stand zu sein.

Sehr dynamische Entwicklung: Die Entwicklungsgeschichte von suresecure ist besonders bemerkenswert. Das Unternehmen ist erst sechs Jahre alt, hat aber mit außerordentlich hohen Wachstumsraten bereits eine dreistellige Beschäftigtenzahl erreicht. Das Management von suresecure ist zudem ambitioniert. suresecure hat sich das Ziel gesetzt, ein Qualitätsführer im Markt für Cybersecurity Services zu werden. Dafür investiert suresecure stark in Fachkräfte und Expertise.

Herausforderungen

Der Wettbewerb ist stark. Die große globalen Anbieter drängen mit ihren umfangreichen Ressourcen zunehmend in den Mittelstandsmarkt, die Hauptzielgruppe von suresecure. Der Anbieter wird also seine Vorteile weiterhin deutlich darstellen müssen.

Managed Security Services - SOC

Wer diesen Bericht lesen sollte

Dieser Quadrant ist für Unternehmen in Deutschland branchenübergreifend hilfreich bei der Bewertung von Dienstleistern, die sich auf Managed Security Services (MSS) spezialisiert haben und sie bei der Bekämpfung von Sicherheitsbedrohungen unterstützen. Er gibt auch Einblicke in die Art und Weise, wie die einzelnen Anbieter die kritischen Herausforderungen des Marktes angehen.

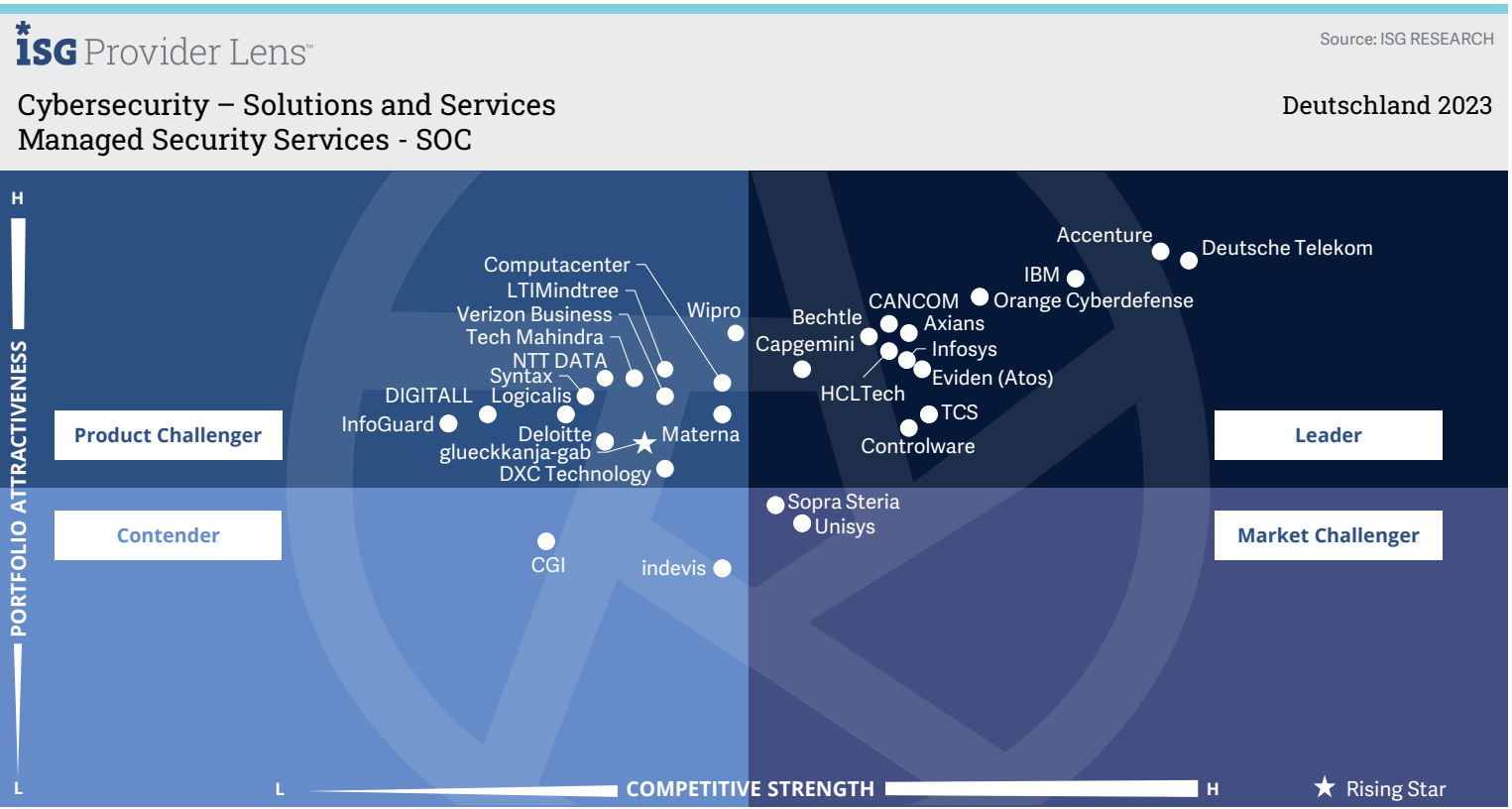
ISG gibt einen umfassenden Überblick über das Wettbewerbsumfeld in diesem Markt und stellt die aktuelle Positionierung dieser Anbieter dar.

Mit der Verlagerung hin zum Remote Working und der zunehmenden Nutzung von cloudbasierten Anwendungen und Diensten sind Unternehmen anfälliger für Cyberangriffe geworden. Gemanagte Detection & Response Services (MDR) bieten eine wichtige Schutzebene gegen diese Bedrohungen und gewährleisten die Sicherheit von Remote-Mitarbeitern und cloudbasierten Ressourcen. Unternehmen benötigen eine kontinuierliche Überwachung, Funktionen zur Erkennung von komplexen Bedrohungen sowie Unterstützung bei der Reaktion auf Vorfälle und der Behebung von Problemen, um Datenschutzverletzungen zu verhindern und die Geschäftskontinuität zu gewährleisten. Die Nachfrage nach MDR-Diensten wird auch durch die Bedeutung von Compliance-Vorschriften und Datenschutzgesetzen angetrieben. Die Erkennung von Ransomware und die so genannte „Ransomware Readiness", also Ransomware-Bereitschaft, stehen nach wie vor ganz oben auf der Agenda, denn Unternehmen müssen ihre wertvollen Daten und Systeme davor schützen, von böswilligen Akteuren kompromittiert zu werden. Damit kann man sich proaktiv auf die Ransomware-Bedrohung vorbereiten. Fortgeschrittene Analytik, KI, ML und Deep-Learning-Techniken für die verhaltensbasierte Bedrohungsanalyse gewinnen zunehmend an Interesse. Feeds mit Bedrohungsdaten (Threat Intelligence) ermöglichen eine proaktive Risikoidentifizierung, Überwachung und genaue Erkennung; Threat Intelligence as a Service gewinnt an Zugkraft. Angesichts der zunehmenden Einführung von Zero Trust und SASE und dem Mangel an qualifiziertem Personal und Know-how steigt der Bedarf an Managed Services.

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

Experten aus den Fachabteilungen erhalten durch diesen Bericht wertvolle Einblicke dahingehend, wie Sicherheitsabläufe vereinfacht werden können. Außerdem werden praktische Lösungen zur Verringerung der Komplexität und zur Steigerung der Effizienz vorgestellt.

Technologie-Experten sollten diesen Bericht lesen, um mit der sich verändernden Sicherheitslandschaft Schritt halten zu können, denn er bietet Einblicke in neue Trends, maßgeschneiderte Sicherheitsplattformen und strategische Ziele.



Dieser Quadrant bewertet die **relevantesten** Dienstleister für Managed Security Services in Deutschland, ohne Anbieter, die ihre Leistungen nur auf eigene Produkte beziehen. Externer Betrieb durch **Security Operations Centers** ist zunehmend gefragt.

Frank Heuer

Definition

Die im Rahmen der Managed Security Services (SOC) (MSS (SOC)) bewerteten Anbieter offerieren Dienstleistungen im Zusammenhang mit dem Betrieb und der Verwaltung von IT- und OT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). 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.

Es besteht eine steigende Nachfrage nach Anbietern, die Unternehmen dabei unterstützen, ihre IT-Sicherheit insgesamt zu verbessern und die Wirksamkeit ihrer Sicherheitsprogramme durch kontinuierliche Verbesserungen langfristig zu maximieren. Zu diesem Zweck müssen MSS (SOC)-Anbieter traditionelle Managed Security Services mit Innovationen zusammenführen, um die Sicherheit ihrer Kunden mit einem integrierten Cyber-Abwehrmechanismus stärken zu können. Sie sollten in der Lage sein, Managed Detection & Response Services (MDR) zu erbringen, mit den neuesten Technologien, Infrastrukturen ausgestattet sein und Threat Hunting und Incident Management Experten beschäftigen, so dass Unternehmen aktiv Bedrohungen erkennen und sie in Reaktion darauf abwehren und eindämmen können. Aufgrund der steigenden Kundenerwartungen in Bezug auf die proaktive Bedrohungsjagd sind die Anbieter dabei, ihre SOC-Umgebungen mit Sicherheitsintelligenz auszubauen und erhebliche Investitionen in Technologien wie Automatisierung, Big Data, Analytik, KI und maschinelles Lernen zu tätigen. Diese hochmodernen SOCs sollten eine von Experten gesteuerte Reaktion auf Sicherheitsinformationen unterstützen und gleichzeitig den Kunden einen ganzheitlichen und einheitlichen Ansatz für Sicherheit auf hohem Niveau bieten.

Auswahlkriterien

1. Zu den typischen Dienstleistungen gehören **Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests, Firewall-Betrieb, Anti-Virus-Betrieb, Identity & Access Management (IAM)-Betriebsservice, Data Leakage/Loss Prevention (DLP)-Betrieb** und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Insbesondere ist auch Secure Access Service Edge (SASE) mit berücksichtigt
2. Angebot von Sicherheitsdiensten wie **Erkennung und Vorbeugung, Security Information & Event Management (SIEM)** sowie Sicherheitsberatung und Audits, entweder remote oder vor Ort beim Kunden
3. **Akkreditierungen** von Anbietern von Security Tools
4. **SOCs idealerweise im Besitz und unter der Leitung des Anbieters** und nicht überwiegend von Partnern
5. **Zertifizierte Mitarbeiter**, z.B. Zertifizierungen wie Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)

Beobachtungen

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken fördern die Nachfrage nach Managed Security Services. Knappe qualifizierte Ressourcen und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich in den Fokus deutscher Unternehmen.

Bei den Großunternehmen spielen aufgrund der häufig internationalen Präsenz dieser Kunden global verteilte Security Operations Centers (SOCs) eine besondere Rolle. Aber auch SOCs mit deutschem Standort wissen Großunternehmen aufgrund des wichtiger gewordenen Datenschutzaspektes – im Zuge unternehmensinterner Compliance oder gesetzlicher Regelungen – zu schätzen.

Aber gerade auch Mittelständler – die noch stärker als Großunternehmen vom Cybersecurity-Fachkräftemangel betroffen sind – sind immer mehr auf die Unterstützung externer Dienstleister angewiesen, um diese wachsenden Herausforderungen zu meistern. Auch sie interessieren sich inzwischen zunehmend für Managed Security Services.

Für diese Zielgruppe sind SOCs in Deutschland ein Pluspunkt. Auch deutschsprachige Ansprechpartner spielen für diese Kundengruppe eine wichtige Rolle.

Darüber hinaus wird von den Anbietern eine hohe Innovationskraft erwartet, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Erweiterung der SOCs in Richtung Cyber Defense Centers, wobei den immer komplexeren Bedrohungen auch mit künstlicher Intelligenz und Automatisierung begegnet wird. Da auch Cyberkriminelle sich zunehmend künstlicher Intelligenz bedienen, sind Cyber Fusion Centers als Ergänzung zu bestehenden SOCs entstanden, um das Cyber Security Management zielgerichtet und zukunftsgerecht auszubauen.

Von den 261 Anbietern, die in dieser Studie bewertet wurden, konnten sich 31 für diesen Quadranten qualifizieren. Dabei erreichten 13 eine Position als Leader. Ein Anbieter wurde als Rising Star identifiziert.

accenture

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

axians

Axians offeriert im Rahmen seiner Managed Security Services ein breites Spektrum an Services und gemanagten Security-Themen. Für besonders gefährdete Daten und Systeme bietet das globale Cyber Defence Center von Axians ein erhöhtes Maß an Sicherheit und flexible Lösungen.

BECHTLE

Bechtles Managed Security Services decken ein breites Spektrum an Leistungen und gemanagten Technologien ab. Zudem sind sie auch modular anpassungsfähig. Neben verschiedenen anderen Ländern betreibt Bechtle auch ein dediziertes SOC in Deutschland mit deutschsprachigem Support.

CANCOM

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

Capgemini

Capgemini bietet im Rahmen seiner Managed Security Services vielfältige Dienstleistungen an, die ein breites Spektrum gemanagter Security-Themen adressieren. Speziell auch gemessen an der Anzahl der Bestandskunden stellt Capgemini in Deutschland ein großes Expertenteam bereit.

Controlware

Speziell auch gemessen an der Anzahl der Kunden unterhält **Controlware** in Deutschland ein großes Expertenteam und offeriert seinen Kunden modulare, individualisierbare Managed Security Services.

Die **Deutsche Telekom** betreibt Managed Security Services unter anderem in Deutschland und unterhält hierzulande zudem ein äußerst großes Team für Managed Security Services. Der Anbieter entwickelt sein bereits sehr umfassendes Angebot kontinuierlich weiter.

Deutschland zählt zu den SOC-Standorten von **Eviden (Atos)**, was auch für viele Großunternehmen interessant ist. Sowohl die abgedeckten Themen als auch die Leistungen der Managed Security Services adressieren ein breites Spektrum.

HCLTech

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

IBM ist im Markt mit einem der breitesten Portfolios für IT Security Services vertreten. Die Managed Security Services des Anbieters basieren auf der leistungsstarker, hauseigener Technologie. Das weltweite Netzwerk aus SOCs ermöglicht einen globalen Betrieb.

Die Leistungen von Infosys im Rahmen der Managed Security Services lassen keine Wünsche offen. Darüber hinaus ist **Infosys** auch personell hinsichtlich seiner Managed Security Services in Deutschland stark aufgestellt.

Orange Cyberdefense

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

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

glueckkanja-gab

glueckkanja-gab ist der „Rising Star" für Managed Security Services in Deutschland. Dazu trägt vor allem der proaktive, qualifizierte Kundenservice bei.

Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2023 – Cybersecurity – Solutions and Services" analysiert die entsprechenden Softwareanbieter/Dienstleister im deutschen Markt auf Basis eines mehrstufigen Marktforschungs- und Analyseprozesses und positioniert diese Anbieter auf Basis der ISG Research™-Methodik.

Federführender Autor:
Frank Heuer

Herausgeber:
Maria Müller-de Haen

Forschungsanalyst:
Bhuvaneshwari Mohan

Datenanalysten:
Rajesh Chillappagari und Shilpashree N

Beratender Consultant:
Roger Albrecht

Projektmanager:
Donston Sharwin

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

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

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

teilgenommen haben, als auch für Anbieter, die nicht teilgenommen haben, dem aktuellen Stand vom April 2023. Zwischenzeitliche Fusionen und Akquisitionen und die damit zusammenhängenden Veränderungen sind in diesem Bericht nicht berücksichtigt.

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

Dabei wurde die Studie in folgende Schritte gegliedert:

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

Autor

Frank Heuer
Leitender Analyst

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

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

Autor

Gowtham Kumar Sampath
Stellvertretender Direktor & Leitender Analyst

Gowtham Sampath ist Senior Manager bei ISG Research und verantwortlich für die Erstellung der ISG Provider LensTM Quadrantenberichte für die Bereiche Banking Technology/Platforms, Digital Banking Services, Cybersecurity sowie Analytics Solutions & Services. Gowtham verfügt über 15 Jahre Marktforschungserfahrung; seine Analysen sollen die Lücke zwischen Datenanalyseanbietern und Unternehmen schließen und gehen auf Marktchancen und Best Practices ein.

In dieser Funktion arbeitet er auch mit Beratern zusammen, um branchenübergreifend Ad-Hoc-Anfragen von Unternehmenskunden im Bereich der IT-Services zu adressieren. Darüber hinaus verfasst er Thought Leadership Researcharbeiten, Whitepapers und Artikel über neue Technologien im Bankwesen zu den Themen Automatisierung, Digital und User Experience (DX bzw. UX) sowie über die Auswirkungen der Datenanalyse in diversen Branchen.

Forschungsanalyst

Bhuvaneshwari Mohan

Senior Forschungsanalyst

Bhuvaneshwari ist Senior Forschungsanalyst bei ISG und verantwortlich für die Unterstützung sowie Mitverfasserin der Provider Lens™ Studien zu Digital Banking Services und Digital Business Enablement und ESG Services. Sie unterstützt die Lead Analysts im Researchprozess, entwickelt Inhalte aus Unternehmensperspektive und verfasst den Global Summary Report. Sie verfügt über 7 Jahre praktische Erfahrung und hat tiefgreifende Custom Reports für verschiedene Branchen erstellt.

Sie ist eine vielseitige Research Professional mit Erfahrung in Competitive Benchmarking, Social Media Analytics und Talent Intelligence. Bevor sie zu ISG kam, hatte sie Research-Rollen bei IT & Digital Services Providers und war vor allem Teil von Sales Enablement Teams. Ihre Kernkompetenzen liegen in den Bereichen AI/ML, Blockchain, IoT, Digital und Experience Engineering.

IPL-Produktverantwortlicher

Jan Erik Aase

Partner und globaler Leiter - ISG Provider Lens™

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

ISG Provider Lens™

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

ISG Research™

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

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

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

ISG

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

Weitere Informationen unter isg-one.com.

ISG Provider Lens™

JUNI, 2023

BERICHT: CYBERSECURITY – SOLUTIONS AND SERVICES