ISG Provider Lens™

Cybersecurity – Solutions and Services

An analysis of the cybersecurity market that compares the attractiveness of portfolios and the competitive strength of providers

Customized report courtesy of: Infosys®

QUADRANT REPORT | JULY 2024 | GERMANY

Table of Contents

Page 1 of 2

Page 2 of 2

Report Authors: Frank Heuer, Gowtham Sampath (SSE), and Dr. Maxime Martelli (XDR)

AI and the SME segment are driving the German cybersecurity market

Cyber threats are increasing for German companies as cyberattacks become more advanced, frequent, complex and versatile. The shortage of qualified cybersecurity experts is exacerbating the situation and driving demand for external services. New technologies favor cyber threats and also offer new business opportunities for service providers. Service providers also benefit if they understand the requirements of different target groups.

Those responsible in German companies are currently facing various challenges. Increased cyber threats due to political tensions, such as the war in Ukraine, the trend toward remote work and the ongoing trend of digitalization, have expanded attack surfaces for cyberattacks in Germany, necessitating appropriate countermeasures. On the other hand, the weak economy is leading to financial challenges.

Business processes are increasingly being shifted to IT as part of digitalization. The company's Intellectual property is also increasingly being represented digitally. Consequently, with the increasing need to protect IT and communication systems, IT security has become corporate security. The increased use of home offices in Germany - and the resulting external connections of employees - has made IT systems more vulnerable to attack.

In addition to digitalization and increased remote working, the increasing provision of resources from the cloud has made IT systems more vulnerable and has led to the growing relevance of the zero-trust approach and the loss of importance of perimeter security. The principle of *never trust, always verify* entails mutual authentication and continuous network monitoring, among other measures.

Cybercriminals are implementing new, more advanced and more complex methods to overcome the cyber defense systems of

The **shortage of skilled workers is** driving demand for external security services.

companies and authorities at ever shorter intervals. There have been a number of spectacular cyberattacks in the recent past, but less prominent attacks, such as ransomware, are also causing increasing problems for companies. Accordingly, cybersecurity measures must be completely up to date. Companies and authorities are increasingly overwhelmed due to the shortage of IT specialists, especially in the cybersecurity market. As a result, IT managers are increasingly turning to external services, such as security operations centers. These providers, including many IT security product providers, are increasingly relying on proactive rather than reactive methods based on AI in order to keep up with the threats themselves.

Companies' own protection and legal regulations, such as the General Data Protection Regulation (GDPR) in the EU, are forcing companies to implement stronger security measures to prevent cyberattacks. This is still a major challenge, especially for midsize companies.

On the other hand, SMEs are also an interesting market segment for cybersecurity providers in Germany. Overall, SMEs have less mature IT security systems than large companies but are forced to upgrade them due to the factors described above. As a result, they have a lot of catching up to do and are, therefore, experiencing above-average growth in demand for cybersecurity solutions. A balanced customer structure of large and midsize companies is even more advantageous for security providers in order to benefit from the extensive budgets of large accounts. The current weak economy in Germany is not leaving the demand for cybersecurity solutions unaffected, meaning that SMEs, with their above-average growth in demand, are becoming an increasingly attractive market segment that also needs to be adequately addressed. It is not enough to simply offer midsize customers a service for large customers. Rather, the entire go-to-market approach - products, prices and communication - must be adapted to these customers. Communication and cultural aspects are particularly important in order to be accepted by SMEs as providers who take this segment seriously.

Despite the great importance of cybersecurity, IT managers are again increasingly struggling with the task of legitimizing investments in cybersecurity vis-à-vis company stakeholders, especially the CFO. Unlike other IT projects, it is not always possible to prove the profitability of cybersecurity investments; it is also not easy to quantify threat risks. On the other hand, more managers are recognizing that cyberattacks can lead to massive - and possibly existential - financial and reputational damage. As a result, IT security is becoming increasingly important in German companies and senior management is becoming more involved in cyber risk management.

The cause of cybersecurity incidents is still often not (solely) on the technical side. Rather, many cyberattacks are facilitated by careless user behavior, such as phishing and Trojan attacks. In addition to up to date IT security equipment, user training and advice, therefore, continue to play an important role.

Advice is also increasingly in demand with regard to technical threats. Consequently, they have substantial catching up to do and are experiencing above-average growth in demand for cybersecurity solutions. These represent a new quality in attacks on the encryption of confidential data. Although quantum-based threats do not play a role in practice, the first service providers have already started to provide advice on this due to the potentially serious consequences. These consulting services are primarily used by banks and insurance companies, as their assets consist of virtual assets and they want to be prepared for the new threats at an early stage.

Identity and Access Management (IAM)

IAM is a particularly important cybersecurity topic and will remain so in the future. One of the main reasons for the growing demand for IAM solutions is the increasing digitalization of all areas, which means that users, their identities and networked machines (Industry 4.0) need to be protected.

In addition, the number of users, devices and services is constantly increasing, along with the number of digital identities that need to be managed. The increased use of remote work contributes significantly to this trend. Many employees access company resources remotely, making it even more important to regulate and control access to data and systems.

Data Leakage/Loss Prevention and Data Security (Products)

In Germany, interest in DLP solutions has continued to grow significantly in recent years. Various factors affecting the security of data in the company are contributing to this. Data and Intellectual Property have become increasingly important and, in some cases, existentially significant corporate assets.

In addition, the increasing business use of private end devices poses a particular challenge in terms of protection against unwanted data outflows, as they are often beyond the configuration and control of the company administration.

Strategic Security Services (SSS)

In the face of increasingly frequent, intensive and advanced cyberattacks, German companies are being called upon to protect their IT systems from damage. Well-known large companies, public authorities and small and midsize companies are affected. At the same time, the shortage of IT specialists continues to make this situation more difficult.

Midsize companies are suffering from a particularly severe shortage of cybersecurity specialists. Therefore, they constitute a market segment that is growing above-average and thus becoming increasingly attractive.

Technical Security Services (TSS)

Companies and authorities in Germany are increasingly reliant on external cybersecurity services to keep their IT security systems up to date due to ever more sophisticated cyberattacks and the pressing shortage of skilled workers.

Service providers who can offer a broad range of TSS from a single source have a particular advantage in this market, as IT security projects are often complex and multifaceted.

Managed Security Services - SOC

The increasingly sophisticated cyberattacks are also driving demand for managed security services (MSS) from security operations centers (SOCs). The shortage of qualified experts and the need for specialist knowledge that is always up to date make these services even more interesting for German companies.

Large and especially midsize customers appreciate SOCs with a German or EU location due to the increased importance of data protection. For both target groups, integrated solutions consisting of IT and associated security solutions, end-to-end security services and a high level of innovation are also important to stay ahead in the race against cyber criminals.

Managed security service providers (MSSPs) are increasingly turning to automation and AI to combat cyber threats. The ideal solution combines machine efficiency with comprehensive human expertise.

> AI and quantum technology pose new threats for users, yet they also present new opportunities for cybersecurity service providers. Service providers who address both large companies with their large budgets and SMEs with their dynamically growing demand have an advantage here.

As enterprises increasingly rely on cloud applications, remote workforces and interconnected systems, the complexity and sophistication of cyberthreats have escalated. This dynamic environment requires advanced security measures that go beyond traditional perimeter defenses. As cyberthreats continue to grow in sophistication, the adoption of such cutting-edge security measures will be essential for maintaining a strong cybersecurity posture.

The necessity for advanced cybersecurity solutions such as extended detection and response (XDR) and security service edge (SSE) is driven by the evolving threat landscape, increased cloud adoption and the need for comprehensive security frameworks. These innovative platforms address critical challenges faced by enterprises, ensuring resilient and efficient protection of digital assets and business operations.

Some of the existing challenges are listed below:

Complexity in security architectures: Managing disparate security tools and solutions can lead to inefficiencies and gaps in protection, making integrated platforms such as XDR and SSE critical for streamlined operations.

Reactive threat detection and response: Traditional security measures often fail to provide real-time visibility and response capabilities. XDR leverages advanced analytics and automation to detect, investigate and respond to threats across various endpoints.

Lax data privacy and governance: Ensuring data privacy and governance in a decentralized IT environment is challenging. SSE offers centralized security policies and governance frameworks to manage data protection effectively.

Lack of scalability and performance: As organizations grow, their security solutions must scale accordingly without compromising IT or business operational performance. XDR and SSE are designed to provide scalable, high-performance security across expansive and evolving IT landscapes.

Poor user experience: Balancing robust security with a seamless user experience is essential. Enterprises require innovative solutions designed to be minimally intrusive while maximizing protection and security posture.

Extended detection and response (XDR) trends

The XDR market is witnessing various innovative trends to improve threat detection, response and the overall security posture. XDR solutions are gaining traction due to their ability to collect and correlate data across multiple security layers, including emails, endpoints, servers, cloud workloads and networks, providing a multifaceted view of the organization's security posture.

The key trends in the XDR space are listed below:

Integration of AI and ML: One of the latest trends in XDR is the integration of AI and ML algorithms to enhance threat detection and response capabilities. These advanced technologies enable XDR platforms to identify complex threats, predict potential attacks and automate response actions, thereby reducing the burden on security teams.

Convergence with other security solutions: Another emerging trend is the convergence of XDR with other security solutions such as security information and event management (SIEM) and security orchestration, automation and response (SOAR). This convergence creates a unified security architecture, improving threat visibility, detection and response times while streamlining security operations.

Threat intelligence integration: XDR platforms increasingly integrate with threat intelligence feeds to enhance threat detection and response. Combining internal security data with external threat intelligence allows XDR solutions to provide contextual insights into potential threats. This helps security teams to make informed decisions and prioritize their response efforts.

XDR for cloud and SaaS environments: As organizations continue to adopt cloud and SaaS applications, XDR solutions are expanding their coverage to include these environments. Cloud-native XDR platforms can monitor and secure cloud workloads, containers and serverless applications while providing visibility on SaaS application usage and potential risks.

Threat and compromise detection capabilities: XDR solutions incorporate user and entity behavior analytics (UEBA) capabilities to detect insider threats and account compromises. UEBA uses ML algorithms to analyze user behavior patterns and identify anomalies that could indicate malicious activity, helping organizations detect and respond to threats that might otherwise go unnoticed.

XDR enhancing security for ICS and OT environments: As the threat landscape for industrial control systems (ICS) and OT environments continues to evolve, security experts are tailoring XDR solutions to address these systems' unique security challenges. XDR for ICS and OT can monitor and analyze data from specialized industrial control systems, detecting threats early and enabling rapid response to minimize potential damage.

Compliance and regulatory support: With the increasing focus on data privacy and security regulations, organizations are enhancing XDR solutions to meet compliance requirements.

Enterprises are navigating a dynamic landscape characterized by increased adoption of cloud environments and evolving cyberthreats, necessitating security solutions that are scalable, flexible and robust. SSE solutions address these challenges by providing centralized visibility, advanced threat detection powered by AI and ML and seamless policy enforcement across all endpoints. By adopting SSE, organizations can ensure secure access to applications and data from any location, maintain compliance with regulatory standards and safeguard against data breaches and insider threats, thereby supporting business continuity and resilience in the face of a constantly changing threat landscape.

Challenges addressed by SSE Solutions are listed below:

Security of cloud applications: The proliferation of cloud services creates security complexities. SSE centralizes security policies and enforces consistent access control across all cloud applications.

Remote workforce security: With more employees working remotely, traditional perimeter-based security models become less effective. SSE provides secure access to cloud applications from any location, regardless of the device.

Data loss prevention (DLP): Data breaches and leaks are major concerns. SSE helps prevent sensitive data from being exfiltrated by enforcing DLP policies and data encryption across cloud services.

Shadow IT: Employees often use unsanctioned cloud applications. SSE provides visibility into shadow IT usage and allows for secure access control even for unapproved applications.

Complexity of security management: Managing multiple security point solutions can be complex and time consuming. SSE offers a unified platform for managing security policies across all cloud applications.

The SSE market is experiencing significant growth due to the increasing adoption of cloud applications, remote workforces and the need for a consolidated security approach.

Key trends shaping the market are listed below:

Cloud-native architectures: As businesses migrate to cloud environments, they adopt cloud-native security solutions that scale with workloads and support dynamic, distributed setups.

Convergence of security and networking: There is a growing trend to integrate networking and security functions into a single platform, streamlining operations and reducing the complexity of managing security and network performance.

Integration of SWGs and CASBs: Secure web gateways (SWGs) and cloud access security brokers (CASBs) are converging into comprehensive SSE solutions, providing unified threat protection, DLP and access control for cloud services.

Emphasis on zero trust security: SSE solutions are increasingly incorporating zero trust principles, granting access based on *least privilege* and continuous verification, enhancing security by minimizing the attack surface and lateral movement within the network.

SASE adoption: SSE is a foundational element of secure access service edge (SASE) architectures, which integrate network security and cloud access security into a unified cloud-delivered service.

AI and ML integration: SSE solutions leverage AI and ML to automate threat detection, improve anomaly identification and personalize security policies based on user behavior.

Focus on user experience: Balancing security with UX is crucial. SSE solutions are designed to be transparent to users, ensuring minimal disruption to their workflow while maintaining robust security.

Unified management consoles: There is a trend toward developing unified management interfaces that consolidate various security functions into a single dashboard, simplifying administration and providing a holistic view of the security landscape.

User and entity behavior analytics (UEBA): UEBA tools analyze the behavior of users and entities to identify potential security threats. By establishing baselines and detecting deviations, UEBA helps identify anomalous activities.

Identity-centric security: Emphasis on identity and access management (IAM) is becoming central to security strategies, ensuring that only authenticated and authorized users can access resources.

As businesses prioritize robust cybersecurity and navigate the complexities of the digital environment, the demand for innovative solutions such as XDR and SSE will be at the forefront of safeguarding their digital assets. As cyberthreats become more sophisticated and businesses rely increasingly on cloud services, XDR and SSE will be crucial in safeguarding enterprise security.

Provider Positioning

Page 1 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Absolute Software	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Acronis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Alice&Bob.Company	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
All for One Group	Not In	Not In	Not In	Not In	Contender	Contender	Not In	Not In
Axians	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
BAYOOSOFT	Product Challenger	Not In	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	Leader
Beta Systems	Product Challenger	Not In	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	Not In

Provider Positioning

Page 2 of 11

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

Provider Positioning

Page 3 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Cloudflare	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
Computacenter	Not In	Not In	Not In	Not In	Leader	Leader	Product Challenger	Contender
Controlware	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader	Leader
CoSoSys (Netwrix)	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
CyberArk	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
DATAGROUP	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger	Leader
Deloitte	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In

Provider Positioning

Page 4 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Deutsche Telekom	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
DIGITALL	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
DriveLock	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Not In	Leader	Product Challenger	Contender	Not In
Ericom Software	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
ESET	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Eviden	Leader	Not In	Not In	Not In	Leader	Leader	Leader	Not In
EY	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Leader	Not In	Not In	Not In	Not In

Provider Positioning

Page 5 of 11

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

Provider Positioning

Page 6 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
iC Consult	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
IN Groupe	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
indevis	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	Market Challenger
InfoGuard	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
Infosys	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In
itWatch	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Kaspersky	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Kyndryl	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Not In

Provider Positioning

Page 7 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Logicalis	Not In	Not In	Not In	Not In	Contender	Contender	Product Challenger	Product Challenger
Lookout	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
ManageEngine	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Materna Radar	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Rising Star ★	Product Challenger
Matrix42	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In	Not In
Nevis	Product Challenger	Not In	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	Product Challenger

Provider Positioning

Page 8 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Omada	Contender	Not In	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	Not In
Open Systems	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
OpenText	Contender	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Oracle	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Not In	Market Challenger	Product Challenger	Leader	Not In
Palo Alto Networks	Not In	Not In	Leader	Leader	Not In	Not In	Not In	Not In
pco	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Perimeter 81	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In

Provider Positioning

Page 9 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Market Challenger	Not In	Contender	Not In	Not In	Not In	Not In
Rapid7	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	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	Not In
Secureworks	Not In	Not In	Product Challenger	Not In	Not In	Contender	Not In	Not In
SenseOn	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 10 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Skyhigh Security	Not In	Product Challenger	Not In	Rising Star ★	Not In	Not In	Not In	Not In
SolarWinds	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger
suresecure	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Rising Star ★
Syntax	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Product Challenger
TCS	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger
TEHTRIS	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Thales	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

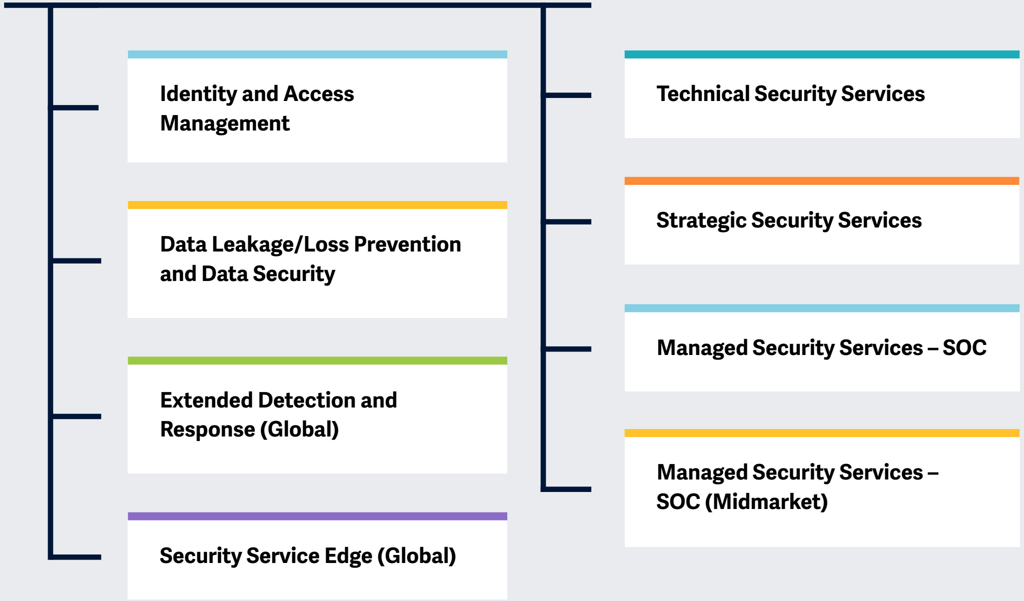
Provider Positioning

Page 11 of 11

	Identity and Access Management	Data Leakage/ Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Managed Security Services – SOC	Managed Security Services – SOC (Midmarket)
Trellix	Not In	Leader	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Unisys	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger	Not In
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Verizon Business	Not In	Not In	Not In	Not In	Not In	Contender	Product Challenger	Not In
Versa Networks	Not In	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Not In	Rising Star ★	Not In	Not In
Wipro	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In
Zscaler	Not In	Rising Star ★	Not In	Leader	Not In	Not In	Not In	Not In

Key focus areas for the Cybersecurity – Solutions and Services

Simplified Illustration Source: ISG 2024


Identity and Access Management
Data Leakage/Loss Prevention and Data Security
Extended Detection and Response (Global)
Security Service Edge (Global)
Technical Security Services
Strategic Security Services
Managed Security Services – SOC
Managed Security Services – SOC (Midmarket)

Definition

Cybersecurity in the age of artificial intelligence

The current cybersecurity landscape is dynamic, with changes occurring rapidly due to emerging threats, technological advancements and evolving regulatory environments.

The year 2023 could be termed as tumultuous from a cybersecurity perspective; the year saw increased sophistication and severity in the attacks. Enterprises responded by increasing their investments in cybersecurity and prioritizing relevant initiatives to prevent attacks and improve their security posture. Learnings from prior attacks in 2022 led to executives and businesses of all sizes and across industries investing in measures countering cyber threats. AI brings both challenges and opportunities to cybersecurity, offering automation for analysis and detection while posing risks of bias and misuse.

From an enterprise perspective, even small businesses realized their vulnerability to cyber threats, fueling demand for (managed) security and cyber resiliency services that would enable recovery and operation restoration post-cyber incidents. Therefore, service providers and vendors are offering services and solutions that help enterprises ensure recovery and business continuity.

Security services providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats, understanding the transformative impact of technologies such as AI and ML, and staying attuned to evolving regulatory frameworks on data protection, such as NIS-2, in the European Union.

Cybercriminals exploited large-scale vulnerabilities, persistently using ransomware to disrupt business activities, specifically healthcare, supply chain and public sector services.

Consequently, businesses started to invest in solutions such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR), and cloud and endpoint security. The market is shifting toward integrated solutions such as security service edge (SSE) and extended detection and response (XDR), which leverage the best tools and human expertise augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.

Scope of the Report

This ISG Provider Lens™ quadrant report covers the following eight quadrants for services/solutions:

Identity and Access Management, Data Leakage/Loss Prevention and Data Security, Technical Security Services, Strategic Security Services, Managed Security Services - SOC, Managed Security Services - SOC (Midmarket), vendors offering Security Service Edge and Extended Detection and Response solutions are analyzed and positioned from a global perspective rather than individual regions.

This ISG Provider Lens™ study offers IT decision makers:

- Transparency regarding the strengths and weaknesses of the relevant service providers and software manufacturers
- Differentiated positioning of providers according to segments (quadrants)
- Focus on the regional market

The study thus provides an essential decision-making basis for positioning, relationship and go-to-market considerations. ISG Advisors and enterprise clients also use information from these reports to evaluate their current and potential new vendor relationships.

Provider Classifications

The provider position reflects the suitability of providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the service requirements from enterprise customers differ and the spectrum of providers operating in the local market is sufficiently wide, a further differentiation of the providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptionsare possible).

Provider Classifications: Quadrant Key

Product Challengers offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/ services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not in means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.

Identity and Access Management

Who Should Read This Section

The report assessing IAM solution providers is relevant to enterprises in Germany seeking to enhance their cybersecurity posture and streamline access management processes. This ISG report targets organizations grappling with the complexities of managing user identities, access rights, and privileged access to critical assets.

In Germany, enterprises are adopting IAM solutions to enhance security, streamline user access and ensure compliance with regulations such as GDPR. They seek solutions offering robust user authentication, authorization and centralized access control.

Enterprises aim to adopt IAM solutions providing features such as single sign-on (SSO), multifactor authentication (MFA) and privileged access management (PAM) to safeguard critical assets.

Providers offer IAM solutions encompassing user provisioning, role-based access control (RBAC) and identity governance to meet diverse enterprise needs. They provide consulting services for IAM strategy development, implementation and continuous support.

German enterprises should read this report as it evaluates IAM solution providers, which is crucial for securing digital assets. As enterprises increasingly rely on digital infrastructure, IAM becomes vital for managing user identities and access rights.

IT security professionals must read this report to gain insights into the capabilities of different IAM solution providers and safeguard enterprise data and infrastructure.

Compliance officers must read this report to evaluate IAM solutions’ ability to meet regulatory compliance requirements.

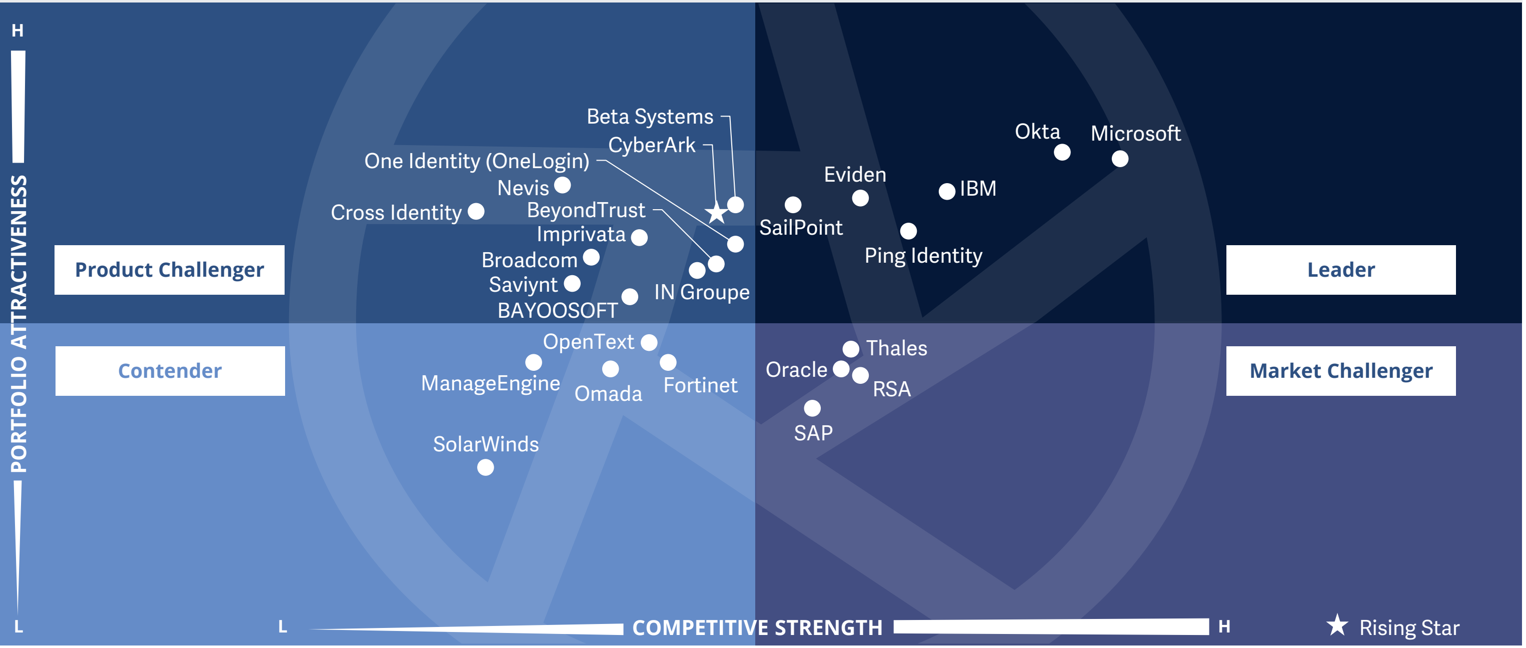
Enterprise decision-makers should read this report to select and implement IAM solutions and make informed decisions.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Identity and Access Management

Germany 2024



The quadrant evaluates the **most relevant** IAM providers in Germany that offer or operate their own software. Important topics are **SSO** and **MFA**. **Passwordless** authentication and **AI support** are becoming increasingly important.

Frank Heuer

Definition

IAM solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services for managing enterprise user identities and devices. This quadrant also includes SaaS offerings based on proprietary software. It excludes pure service providers that do not offer an IAM product (on-premises and/or cloud) based on proprietary software. Depending on organizational requirements, these offerings could be deployed in several ways, such as on-premises, customer-managed clouds or as-a-service models or a combination thereof.

IAM solutions aim to manage (collect, record and administer) user identities and related access rights and include specialized access to critical assets through privileged access management (PAM), where access is granted based on defined policies. To handle existing and new application requirements, IAM solution suites are increasingly embedded with secure mechanisms, frameworks and automation (for example, risk analysis) to provide real-time user and attack profiling functionalities. Solution providers are also expected to offer additional functionalities for social media and mobile use to address specific security needs beyond traditional web and contextual rights management. This quadrant also includes machine identity management.

Eligibility Criteria

1. Offer solutions that can be **deployed** as an **on-premises, cloud, identity-as-a-service** (IDaaS) or a managed third-party model
2. Offer solutions that can **support authentication** as a combination of **single-sign-on (SSO), multifactor authentication (MFA)**, and risk-based and context-based models
3. Offer solutions that can **support role-based access** and PAM
4. Provide **access management** for one or more enterprise needs such as **cloud, endpoint, mobile devices, APIs and web applications**
5. Offer solutions that can **support one or more legacy and new IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM
6. Offer a portfolio with one or more of the following – **directory solutions, dashboard or self-service management** and lifecycle management (migration, sync and replication) solutions – to support secure access.

Observations

IAM continues to be a particularly relevant cybersecurity topic. The increasing digitalization of all areas is a key reason for the growing demand for IAM solutions. This development means that users, their identities and networked production machines such as those in Industry 4.0. must be protected.

The number of natural digital identities to be managed is also constantly increasing. An important factor here continues to be the relocation of many employees to the home office. Increased remote and mobile access to company resources makes regulation and access control increasingly important. This also results in even higher security and convenience requirements. This is why topics such as multi-factor authentication (MFA), single sign-on (SSO), intuitive interfaces, passwordless authentication, biometrics and AI are becoming increasingly important.

As in the software market, IAM solutions can also observe a shift from on-premise operation to the cloud. Most providers have adapted to this and offer both on-premise and cloud operations. Pure cloud providers are also becoming increasingly common, with Okta leading the way.

On the provider side, Ping Identity has acquired and integrated its competitor, ForgeRock, which is no longer listed separately in our analysis. The new rising star is CyberArk. ManageEngine is a new addition to the quadrant.

From the 85 providers assessed for this study, 26 qualified for this quadrant, with six being Leaders and one Rising Star.

EVIDEN
an atos business

Eviden (an Atos Business) is profiling itself as a European provider in the German IAM market with a versatile portfolio and is further expanding its offering.

IBM.

With its large market presence, **IBM** scores and offers a powerful portfolio of IAM solutions that integrate particularly well into the IBM technology landscape.

Microsoft

Microsoft is increasingly gaining ground in the German IAM market due to its adept marketing and technological improvements.

Okta

Okta continues to be successful in Germany with purely cloud-based IAM solutions - especially among users who value quick and easy implementation.

Ping
Identity

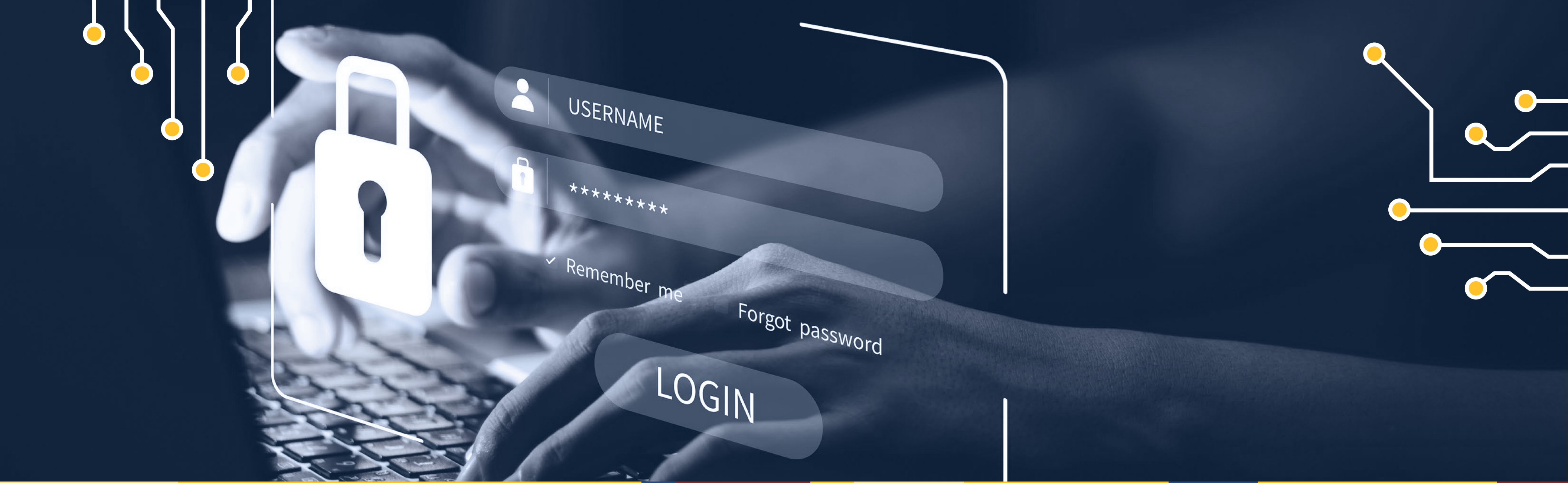
With an optimized balance of security, end-user convenience and versatile usability, **Ping Identity** is also increasingly successful in the German market.

SailPoint

SailPoint scores with risk minimization through artificial intelligence and simplified IAM management of multicloud environments.

CyberArk

CyberArk is the Rising star among providers of IAM solutions in Germany. CyberArk's comprehensive and advanced PAM solutions contribute to this.



Data Leakage/Loss Prevention and Data Security

Who Should Read This Section

This report is relevant to German enterprises across industries for evaluating DLP and data security service providers. This ISG report assesses service providers that help enterprises identify and monitor sensitive data, granting access only to authorized users and preventing data loss or leakage.

In Germany, enterprises are observing notable shifts in DLP strategies, reflecting the dynamic cybersecurity landscape. German enterprises are prioritizing DLP tools to secure sensitive data and comply with stringent data protection regulations such as GDPR. They seek scalable and efficient DLP solutions to mitigate risks associated with data breaches and insider threats.

Cloud-native DLP solutions are gaining traction, aligning with organizations' widespread adoption of cloud technologies.

Integrated DLP with collaboration tools is emerging as a priority, facilitating secure data sharing and collaboration within remote work environments. This integration ensures sensitive information remains protected regardless of the location or device used for access.

The surge in remote employees underscores the urgency for DLP solutions to effectively mitigate insider threats, safeguarding sensitive data accessed from diverse locations.

DLP providers respond to these trends by introducing innovative features such as extensive file tracking capabilities, ML-infused DLP for prioritizing data monitoring and API-driven solutions for seamless integration with existing systems. These advancements align with the evolving needs of German enterprises seeking scalable, flexible and compliance-centric DLP solutions to navigate the complexities of modern cybersecurity landscapes.

IT security professionals should read this report to get insights into emerging trends, innovative features and best practices in the field.

Chief information security officers must read this report to gain insights into the evolving landscape of DLP strategies and solutions, enabling informed decision-making investments in cybersecurity technologies.

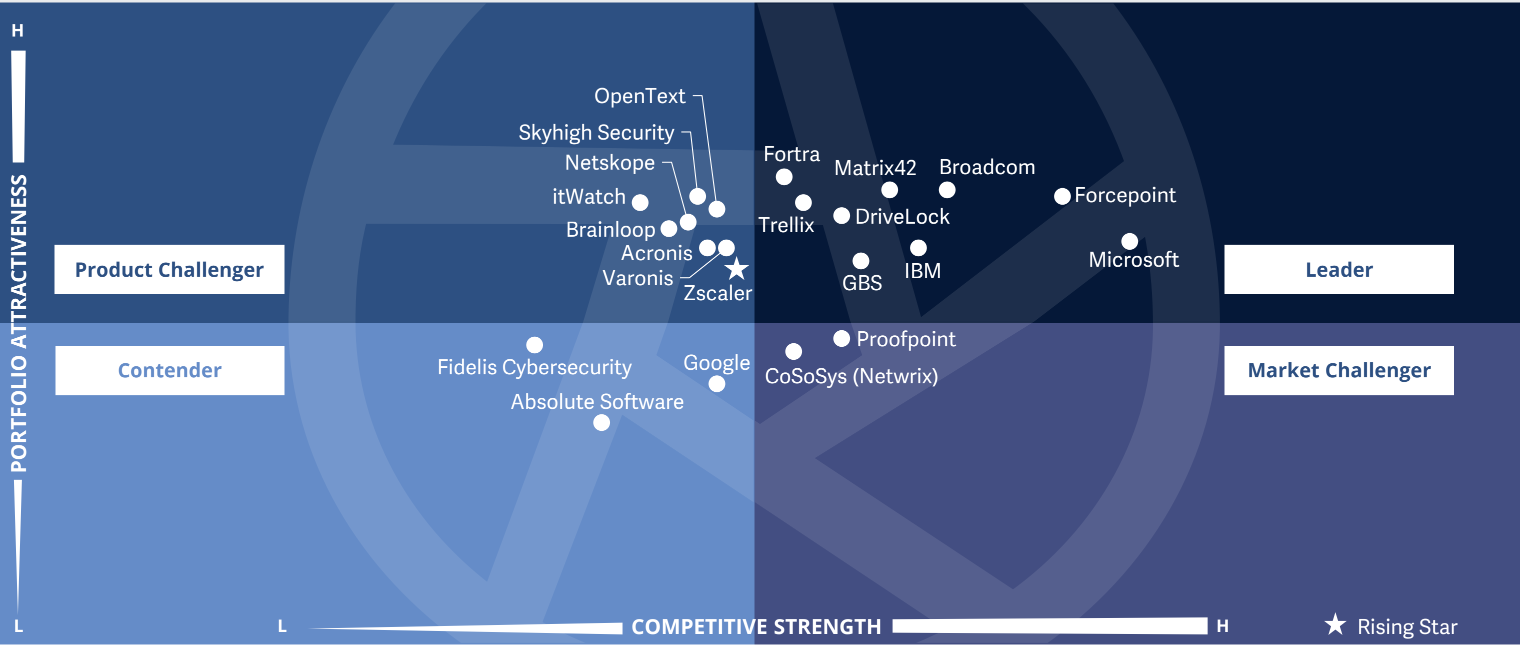
Compliance officers responsible for ensuring adherence to data protection regulations should read this report to learn how DLP solutions can help their organizations achieve and maintain compliance.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Data Leakage/Loss Prevention and Data Security

Germany 2024



This quadrant evaluates the **most relevant** DLP providers in Germany that offer or operate proprietary software. Pressing **data protection concerns** and the protection of intellectual property contribute to the importance of the market.

Frank Heuer

Definition

The DLP solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services, including SaaS solutions. This quadrant **excludes pure service providers that do not offer a DLP product (on-premises or cloud-based) based on proprietary software.** DLP solutions can identify and monitor sensitive data, provide access for only authorized users and prevent data loss/leakage. Vendor solutions in this space include a mix of products providing visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

These solutions are gaining considerable importance due to companies' escalating challenges in controlling data movements and transfers, with over a third of data violations originating internally. The number of devices, including mobile devices, used for data storage amplifies these concerns. Internet connectivity allows these devices to exchange data without passing through a central gateway. Data security solutions protect data from unauthorized access, disclosure or theft by prioritizing, classifying and monitoring data (when at rest and in transit) while allowing organizations to report on and improve data security.

Eligibility Criteria

1. Offer DLP solutions based on **proprietary software** and not third-party software
2. Demonstrate capability of supporting DLP **across any architecture, such as the cloud, network, storage or endpoint**
3. Showcase ability of **handling sensitive data** protection **across structured or unstructured,** text or binary data
4. Offer solution with **basic management support,** including, but not limited to, **reporting, policy controls,** installation and maintenance and advanced threat detection functionalities
5. Offer solution capable of **identifying sensitive data, enforcing policies,** monitoring traffic and improving data compliance

Observations

Data and Intellectual Property have gained increasing significance, sometimes reaching existential importance not solely for financial service providers. Industrial companies are also dependent on the reliable protection of company secrets in the face of international competition. This contributes to the increased interest in DLP solutions. The increasing business use of private end devices also poses a particular challenge, as they often elude company administration and in some cases cannot be comprehensively monitored for legal reasons. DLP solutions must take these restrictions into account when monitoring without allowing operational security gaps. With the General Data Protection Regulation, the importance of data protection in companies has also increased by law.

The enormous increase in company data requires powerful DLP solutions that can quickly detect and classify data and protect it from unauthorized actions according to its protection requirements. Cloud storage solutions and apps mean that data may leave the company network unintentionally during processing. Social media and communication platforms open up communication channels through which data can flow; last but not least, there are the risks associated with data transfers via email. However, it is not only unintentional data leaks that can occur through the fault of internal players; companies must also be able to protect themselves against unfaithful behavior on the part of internal participants.

AI is increasingly helping to overcome the challenges.

Zscaler is the new rising star. Trend Micro is no longer represented on the market.

From the 85 providers assessed for this study, 22 qualified for this quadrant, with nine being Leaders and one Rising star.

Broadcom

Broadcom combines performance with simple management and great flexibility - making it a leading provider of DLP solutions in Germany.

DriveLock

The German DLP provider **DriveLock** creates trust with the *Made in Germany* and *No Backdoor* currencies - and efficiently supports its customers in complying with guidelines.

Forcepoint

Forcepoint helps users and facilitates DLP with advanced solutions, rapid incident response and data protection compliance.

Fortra

Fortra offers a versatile DLP portfolio that simplifies data protection compliance for user organizations through proactive data classification and advanced analytics and reporting services.

GBS

The German DLP provider **GBS** uses sophisticated technology and the dual control principle to ensure secure communication and collaboration - while business processes remain unaffected.

IBM

With Guardium, **IBM** offers a comprehensive, flexibly applicable DLP solution that is competently and forward-lookingly supported with artificial intelligence.

MATRIX42

Matrix42 is increasingly making a name for itself in the security market and impresses with its comprehensive, efficient DLP functions and customer-oriented service. A high level of acceptance among end users is achieved with minimal disruption.

Microsoft

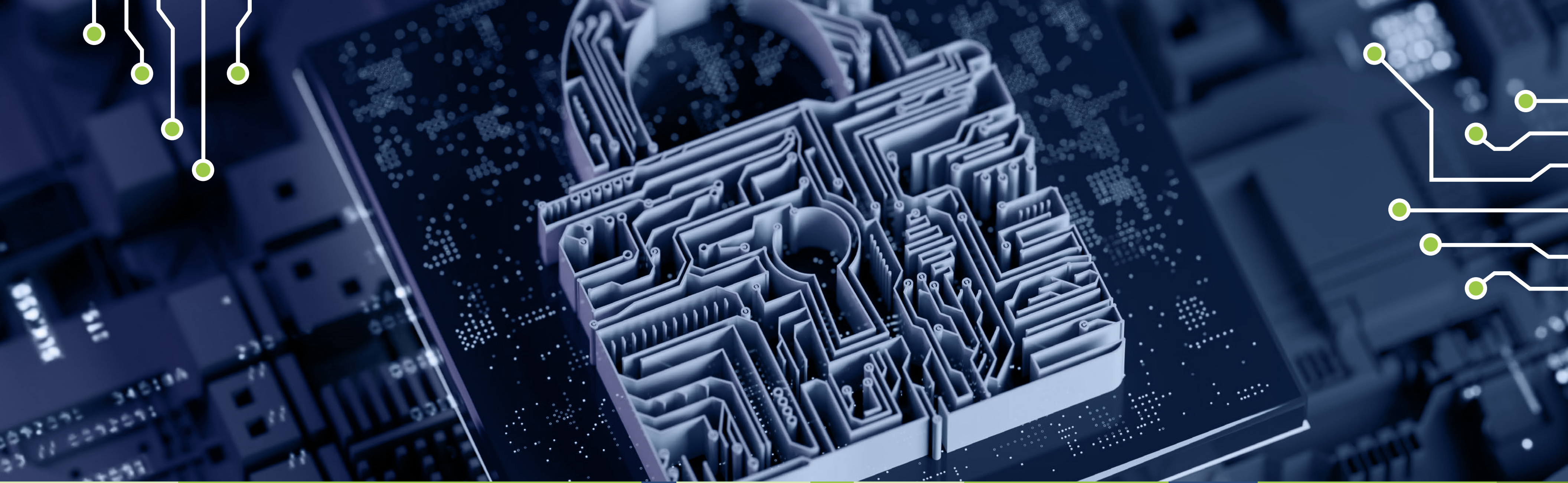
With clever marketing such as integration and bundling and improved solutions, **Microsoft** is expanding its leading position in the German DLP market.

Trellix

A comprehensive solution, cloud operation in Germany and a large local presence thanks to a comprehensive partner landscape make **Trellix** the leader in the German DLP market.

zscaler™

Zscaler is the new rising star for data loss/leakage prevention in Germany. This is due to a powerful solution and greater market presence.



Extended Detection and Response (Global)

Who Should Read This Section

This quadrant is relevant to enterprises globally for evaluating extended detection and response (XDR) solution providers. It assesses how each provider helps enterprises increase visibility across all telemetry sources and obtain a unified view of threat detection and response. ISG offers an analysis of the current positioning of global XDR players with a comprehensive overview of the market's competitive landscape.

Enterprises recognize the need for a proactive approach to threat detection and response, driven by data science techniques and dynamically updated threat intelligence. XDR empowers enterprises of all sizes and security maturity levels to achieve robust threat detection and response capabilities, regardless of limited security personnel, expertise or budget for a dedicated security operations center (SOC). A well-built XDR solution is an SOC enabler that presents a descriptive view of threats and automates initial triage tasks.

Using MITRE ATT&CK framework and open-source intelligence, XDR models detect anomalies and classify attacks based on specific tactics and techniques, providing actionable insights for SOC analysts. It enriches alerts with context, correlating events to determine true threat severity and attack chain participation. This reduces false positives and saves valuable investigative time. Advanced XDR solutions prioritize alerts based on risk scoring and business impact, guiding incident response planning. Additionally, XDR solutions should have a robust set of APIs that allow the extension of workflow functionalities to other external systems to streamline containment actions to events.

Cybersecurity professionals can gain valuable insights into XDR solutions that aid enterprises in enhancing visibility across endpoints to enable unified threat detection and response.

Strategy professionals should read this report to understand XDR providers' capabilities in helping enterprises manage security risks effectively and make informed security decisions.

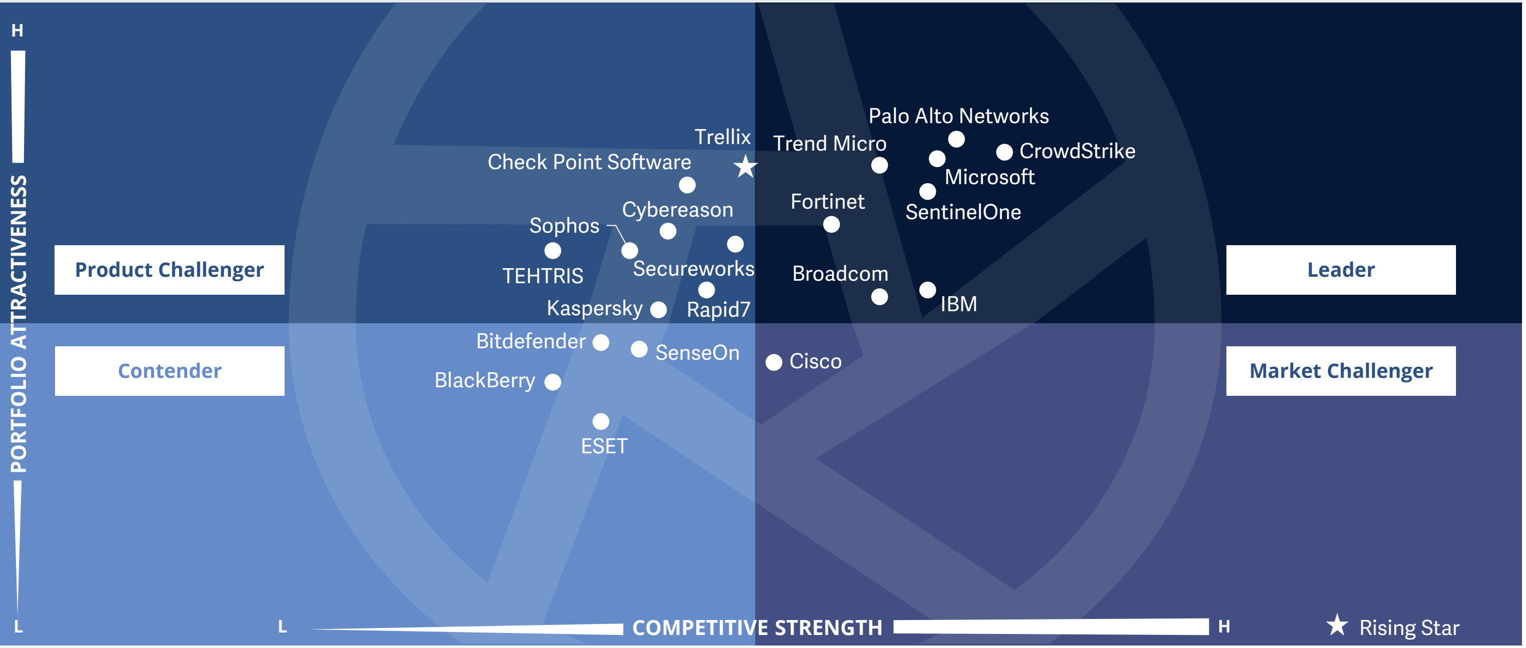
Technology professionals should read this report to understand XDR providers' integration capabilities and how they help with improved detection and faster response times to threats.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Extended Detection and Response

Global 2024



The Extended Detection and Response quadrant assesses security vendors' ability to provide **integrated threat detection, investigation and response capabilities across multiple endpoints,** networks and cloud environments.

Dr. Maxime Martelli

Definition

The XDR solution providers assessed for this quadrant are characterized by their ability to offer a platform that integrates, correlates and contextualizes data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple-point solutions. It uses advanced analytics to correlate alerts from multiple sources, including weak individual signals, to enable accurate detections. XDR solutions consolidate and integrate multiple products, providing comprehensive security for workspaces, networks and workloads. Typically, XDR solutions are aimed at vastly improving visibility and context understanding of identified threats across the enterprise. Characteristics of these solutions include telemetry and contextual data analysis for detection and response. XDR solutions comprise multiple products integrated into a single pane of glass for sophisticated viewing, detection and response capabilities. Their high automation maturity and contextual analysis offer tailored responses to affected systems, prioritizing alerts based on severity against known reference frameworks. This quadrant excludes **pure service providers that do not offer an XDR solution based on proprietary software.** XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expenses. They are particularly suitable for security operations teams struggling to manage diverse solution portfolios or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

Eligibility Criteria

1. Offer XDR solutions based on **proprietary software** and not on third-party software
2. Ensure an XDR solution has two primary components: **XDR front end and XDR back end**
3. Offer front end with **three or more solutions or sensors**, including, but not limited to, **endpoint detection and response, endpoint protection platforms**, network protection (firewalls, IDPS), network detection and response, identity management, email security, mobile threat detection, cloud workload protection and identification of deception
4. Provide solution with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solution capable of blocking sophisticated threats such as **advanced persistent threats, ransomware** and malware
6. Provide solution using **threat intelligence** and **real-time insights on threats** emanating across endpoints
7. Offer solution including **automated response features**

Observations

In 2024, the XDR market is evolving with several new trends and advancements. XDR solutions are integrating advanced AI and ML capabilities, thus enhancing behavioral analytics and automating response actions based on learned patterns.

Vendors have also increased their focus on cloud security and are providing comprehensive visibility and protection across hybrid and multicloud environments. XDR platforms are closely aligning with the MITRE ATT&CK framework, enabling more informed threat-hunting and response strategies.

XDR vendors are expanding their offerings to include robust managed detection and response (MDR) services, catering to organizations facing skill shortages. Moreover, XDR solutions are leveraging advanced UEBA for proactive threat detection and response. Automation and orchestration capabilities within XDR platforms are maturing, thus streamlining incident response processes and reducing manual tasks. XDR also aligns with zero trust principles, emphasizing continuous verification and strict access controls while incorporating features to support regulatory compliance requirements.

Such advancements underscore XDR's role in delivering sophisticated threat detection, response and compliance capabilities amid evolving cyber threats.

From the 35 companies assessed for this study, 21 qualified for this quadrant, with eight being Leaders and one Rising Star.

Broadcom

Broadcom's XDR includes comprehensive visibility, advanced analytics, automated response and a simplified management console, enabling organizations to effectively protect their digital assets against evolving threats.

CrowdStrike

CrowdStrike's Falcon® Insight XDR flexibility meets the increasing market demand for a simplified and single-pane-of-glass control panel with its Falcon tool. It aims to increase industry robustness by supporting standards and frameworks like CrowdXDR Alliance.

Fortinet

Fortinet's FortiXDR can be seamlessly integrated with Fortinet Security Fabric and Fortinet's other security products to streamline incident response with automated workflows and playbooks. This integration allows fast containment and threat remediation.

IBM

IBM's Security QRadar XDR undertakes a proactive and coordinated approach to threat detection and response, with multiple modules and integration across networks, clouds, endpoints and other workloads.

Microsoft

Microsoft's extensive customer base and strong brand recognition have helped the company establish a prominent position in the XDR market. Its XDR integrates its Defender Advanced Threat Protection (ATP) to provide threat detection and response.

Palo Alto Networks

Palo Alto Networks' strong market presence, commitment to innovation and focus on secure access service edge/security service edge (SASE/SSE) solutions for organizations make Cortex XDR a robust product and Palo Alto Networks a Leader in the XDR quadrant.

SentinelOne

SentinelOne maintains its momentum as one of the leading XDR vendors by using patented behavioral AI algorithms to detect and classify malicious activities. All security functions are bundled in a single agent, thus eliminating the need for multiple security products.

Trend Micro

Trend Micro expanded its endpoint detection and response (EDR) capabilities into a next-generation XDR product, which aligns with the MITRE ATT&CK framework and offers dynamic risk assessments. Its automation capabilities deliver advanced XDR.

Trellix

Trellix (Rising Star) XDR boasts an adaptable and interoperable framework that seamlessly connects with a vast array of external security solutions, fostering a unified cybersecurity strategy combined with a sophisticated threat detection mechanism.

Security Service Edge (Global)

Who Should Read This Section

This report is relevant to enterprises globally for evaluating security service edge (SSE) solution providers. It assesses SSE solutions' key features, such as zero-trust network access (ZTNA), cloud access security broker (CASB) and secure web gateways (SWGs). It evaluates how each provider helps enterprises ensure security across hybrid and multicloud ecosystems.

In this quadrant, ISG defines global SSE players' current positioning, offering a comprehensive overview of the competitive market landscape.

Due to the rapid shift to hybrid work models, enterprises seek solutions that accommodate employees, partners, suppliers, and customers accessing internal apps, the internet and SaaS applications. Enterprises want SSE solutions that simplify the adoption and deployment of security policies. A streamlined approach reduces complexity and accelerates implementation. Enterprises expect SSE platforms to monitor and track user activity across a network. Furthermore, SSE providers must protect all users from ransomware and other advanced malware threats.

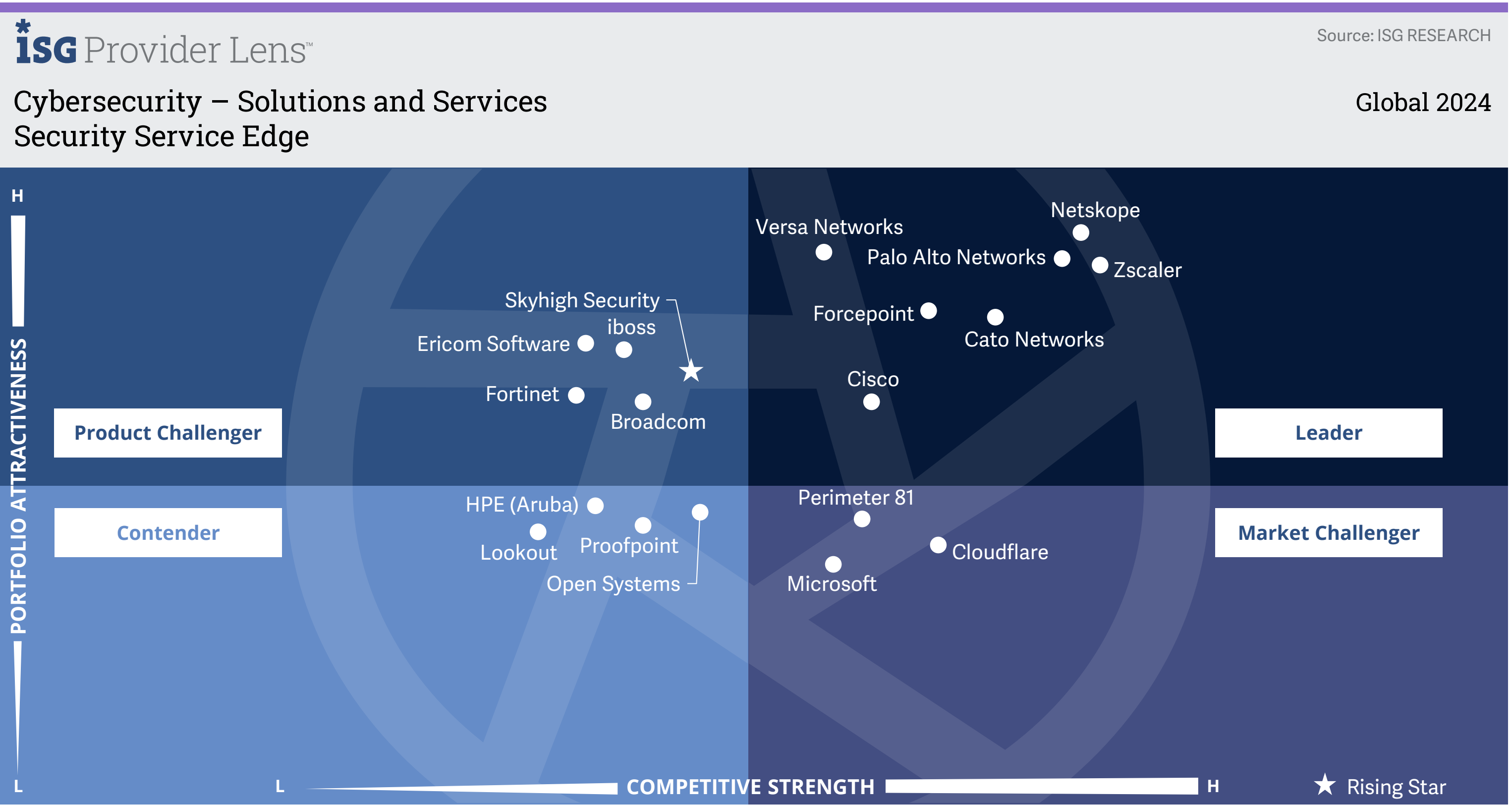
Enterprises adopt SSE to address modern security challenges, simplify access and enhance digital experiences. They seek providers that offer streamlined solutions, robust protection and agility in a rapidly evolving landscape.

The need for unified, secure access in a hybrid workforce drives SSE adoption. Enterprises expect SSE providers to offer simplified deployment, VPN bypass and robust malware protection. Providers should innovate, customize, prioritize UX and expand their global reach to succeed.

Data management professionals should read this report to understand how SSE providers help enterprises overcome challenges posed by data regulation mandates with better policy controls and reporting.

Technology professionals will be able to understand how SSE providers assist enterprises in adopting an enterprise-wide zero-trust framework to improve their security posture.

Strategy professionals can gain insights into SSE providers' critical capabilities and focus on user-centricity, delivering security to end users at the edge or devices through cloud.



This quadrant assesses SSE vendors that offer **cloud-centric solutions** that integrate individual solutions enabling **secure access to cloud services**, SaaS applications, web services and private applications with a **strong focus on UX**.

Gowtham Sampath

Definition

The SSE solution providers assessed for this quadrant offer cloud-centric solutions combining proprietary software or hardware and associated services, enabling secure access to the cloud, SaaS, web services and private applications. Vendors offer SSE solutions as an integrated security service through globally positioned points of presence (POP) with support for local data storage that combines individual solutions such as zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS). SSE can also include other security solutions such as data leakage/loss prevention (DLP), browser isolation and next-generation firewall (NGFW) to secure access to both cloud and on-premises applications.

Vendors showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients.

This quadrant excludes the network components of secure access service edge **(SASE), such as SD-WAN**, which are covered in the ISG Provider Lens™ Network – Software Defined Solutions and Services 2024 study.

SSE solutions strongly focus on user-centricity, delivering security to end users at the edge or devices through the cloud — rather than allowing users to access enterprise applications and databases — over dedicated networks centrally. ZTNA creates exclusive connectivity between users and applications, using context-based behavioral analysis to manage access. CASB offers visibility, enforces security policies and compliance, and controls shadow IT cloud usage, while FWaaS and SWG prevent malicious threats and access to infected websites and applications. Typically, an SSE solution has a unified console for visibility and governance, with advanced automation to assess UX.

Eligibility Criteria

1. Provide SSE as an **integrated solution** with **zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**
2. Offer solutions **predominantly based on proprietary** software, they may **partially rely on partner solutions** while avoiding **complete dependency on third-party** software
3. Maintain **globally located POPs** to deliver these solutions
4. **Deliver SSE to both cloud and on-premises** environments (including hybrid environments)
5. Exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/UEBA)** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **globally availability of the solution**

Observations

The Security Service Edge market is currently witnessing rapid growth driven by the increasing adoption of cloud applications, expanding remote workforce and evolving cyber threat landscape. ISG's analysis reveals several enterprise challenges necessitating SSE deployments:

- Organizations are increasingly using a mix of cloud platforms (public, private and hybrid), as traditional security solutions failed to ensure consistent security across these diverse environments.
- With the rise of remote work, securing access to cloud applications from various locations and devices becomes crucial.
- Managing a complex security ecosystem with multiple-point solutions can be challenging.
- Strict regulations like the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA) and GDPR require robust data security measures.

Vendor selection: Differentiation and characteristics in the SSE market

- Enterprises prioritize SSE vendors that cater to their industry-specific compliance and regulations and data security concerns.
- They seek vendors offering open standards and pre-built integrations with existing security tools and cloud platforms to avoid vendor lock-in and simplify deployment.
- SSE solutions need to scale effectively to accommodate growth in cloud application usage and user base, with low latency and reliable performance, which are essential for ensuring a positive UX for geographically dispersed workforces.
- Enterprises prefer vendors with robust threat intelligence capabilities and a proven track record of security expertise.
- Transparency in pricing and a clear understanding of the TCO, including integration costs, is critical for global companies when selecting an SSE vendor.

From the 35 companies assessed for this study, 19 qualified for this quadrant, with seven being Leaders and one Rising Star.

Cato Networks

Cato Networks focuses on improving the integration and performance of its SSE solutions by upgrading its ZTNA capabilities within the Secure Connect platform and expanding its partnerships with cloud providers.

Cisco

Cisco prioritizes integrating its SSE solution, Secure Access, with other Cisco security products to achieve a unified approach. The company also strengthens partnerships with cloud providers like Microsoft to enhance Secure Access' functionalities.

Forcepoint

Forcepoint focuses on expanding the reach of its Forcepoint Cloud Security Gateway, an SSE platform, by launching integrations with additional cloud platforms. This strategic move aligns with the growing adoption of multicloud environments.

Netskope

Netskope is expanding its global data center network, aiming to offer lower latency, improved performance and user reach. The company is also focusing on partnerships with SIEM vendors to enhance threat detection and investigation capabilities within its SSE platform.

Palo Alto Networks

Palo Alto Networks has introduced improvements to UX and streamlined policy management tools within its Prisma SASE platform. The company also strengthened partnerships with cloud providers such as AWS to offer preconfigured security policies.

Versa Networks

Versa Networks has introduced enhanced cloud workload protection functionalities within its Versa SASE platform and established partnerships with threat intelligence providers to improve threat detection capabilities, ensuring comprehensive protection for customers.

Zscaler has expanded its global data center network to improve performance for its Zscaler ZSSP platform. It also increased focus on partnerships with SASE framework providers for industry-standard secure access, fostering a unified and secure cloud security ecosystem.

Skyhigh Security

Skyhigh Security (Rising Star) has launched Cloud Workload Protection Platform (CWPP) integration to offer comprehensive cloud security alongside its core SSE platform. This offering surpasses basic SSE functionalities, extending additional protection for cloud workloads.

Technical Security Services

Who Should Read This Section

The report serves as a comprehensive resource for enterprises for evaluating TSS providers across industries in Germany. It goes beyond merely assessing these providers' proprietary offerings, emphasizing their capabilities in integrating various security products and solutions from different vendors. With a focus on the current market landscape, this ISG report evaluates the current market positioning of TSS providers and elucidates their strategies for addressing critical security challenges organizations face.

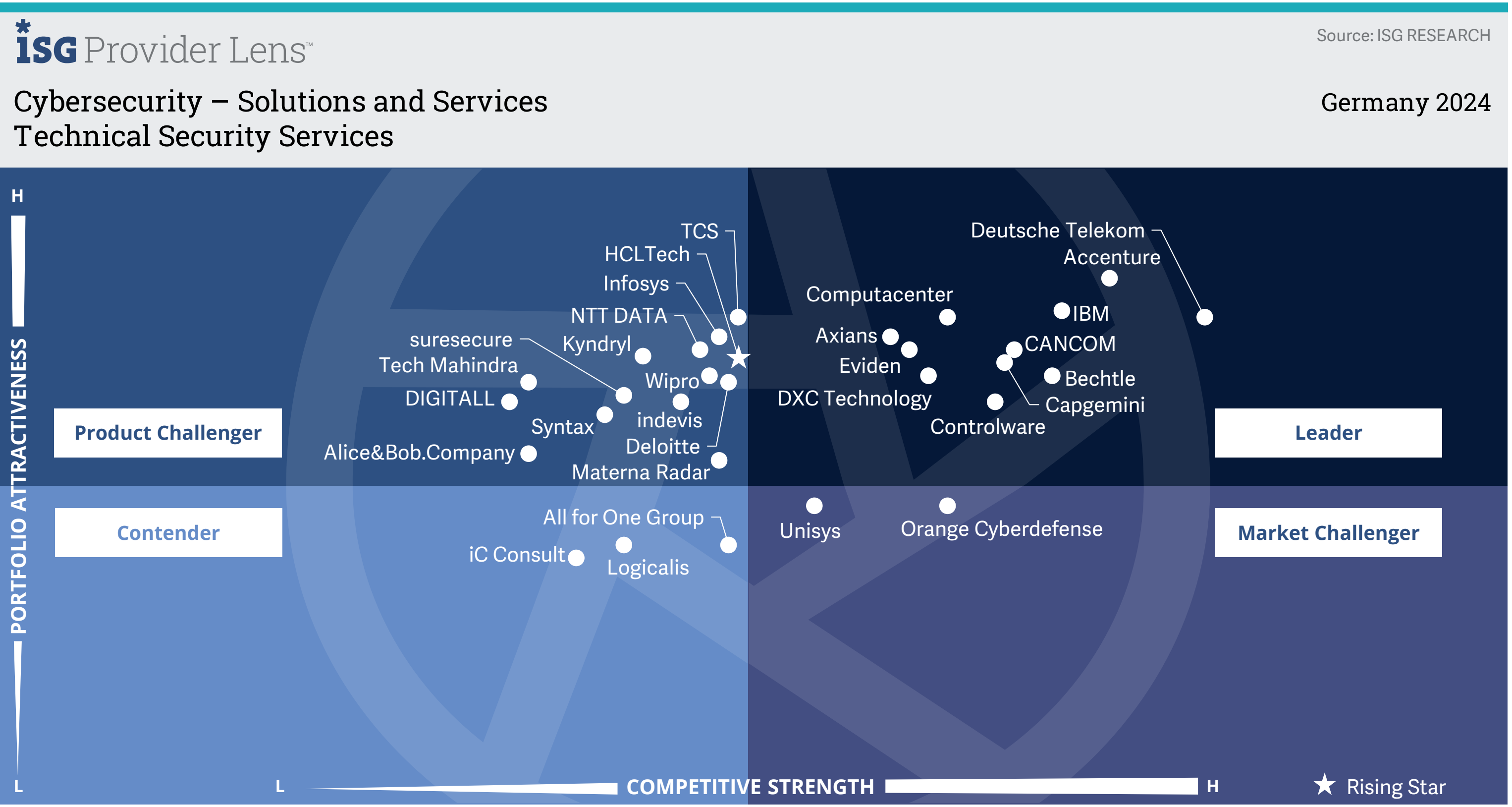
German enterprises can gain valuable insights from this report, particularly in navigating the ever-evolving cybersecurity landscape. As adopting zero trust principles become increasingly prevalent, understanding how TSS providers approach Zero Trust implementations is paramount for aligning security strategies with the evolving threat landscape. This report offers valuable insights into cloud-native security solutions, including secure access service edge (SASE) and security service edge (SSE), essential for transitioning from on-premises data centers to public cloud environments.

It explores the trend of consolidating security technologies to streamline security infrastructure and mitigate complexity. By comprehending the benefits of vendor consolidation and embracing integrated security platforms, German enterprises can optimize their security investments effectively. Staying abreast of industry trends and harnessing innovative security technologies can help organizations bolster their cybersecurity posture, effectively mitigating emerging threats and safeguarding their assets and data.

Strategy professionals should read this report to learn the current market landscape, enabling informed decision-making concerning security strategies, vendor selection and technology investments.

Consultants and advisors specializing in cybersecurity and IT strategy should read this report to assess the competitive landscape and identify suitable TSS providers for specific client needs.

Cybersecurity professionals should read this report to understand the capabilities and market positioning of TSS providers that contribute to the overall security posture of their organizations.



This quadrant focuses on the **most relevant** providers of technical security services in Germany, whose services do not only cover their own products. External providers are playing **an increasingly important role** due to the shortage of specialists.

Frank Heuer

Definition

The TSS providers assessed for this quadrant cover integration, maintenance and support for both IT and OT security products or solutions. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security and SASE and others.

TSS providers offer standardized playbooks and road maps that aid in transforming an existing security environment with best-of-breed tools and technologies, improving security posture and reducing threat impact. Their portfolios are designed to enable complete or individual transformations of existing security architectures across domains such as networks, cloud, workplace, OT, IAM, data privacy and protection, risk and compliance management and SASE, among others. The offerings also include product or solution identification, assessment, design and development, implementation, validation, penetration testing, integration and deployment.

TSS providers invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio scope. This quadrant also encompasses classic MSS provided without a security operations center (SOC).

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Have gained **authorization by security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies.

Observations

German companies continue to face a mounting challenge as cyberattacks grow in intensity, sophistication, complexity and frequency. This is made more difficult by the lack of cybersecurity experts. Companies, therefore, increasingly need the support of external service providers. Providers proficient in current technologies and addressing different target groups have an advantage here.

SMEs must catch up, as they often suffer from problems such as a shortage of IT specialists. Increasingly complex security threats and stricter legal regulations are increasingly prompting these companies to seek external support. SMEs often appreciate the local presence of service providers for short distances and uncomplicated, fast support.

To be successful in the demanding key account market, providers must be able to present extensive international experience and teams. Providers with a balanced customer structure consisting of key accounts and SMEs benefit from both the large budgets of key accounts and the above-average growth in demand from SMEs.

IT security projects are often demanding and multifaceted. Therefore, providers offering comprehensive TSS from a single source have an advantage. Service providers who cooperate with renowned technology providers and whose employees have numerous high-quality certifications can also benefit from this.

Service providers offering their customers end-to-end security services and associated IT solutions from a single source also have an advantage.

From the 85 providers assessed for this study, 30 qualified for this quadrant, with eleven being Leaders and one Rising Star.

accenture

Comprehensive services and cost-efficient solutions based on robotic process automation make **Accenture** a leading provider of TSS in Germany.

axians

With comprehensive technical cybersecurity services, partnerships with numerous renowned cybersecurity technology providers and a balanced customer structure, **Axians IT Security** is successful in the German market.

BECHTLE

Bechtle scores with a large local market presence and extensive resources, thus positioning itself as a leading provider of TSS in Germany, especially for the dynamically growing market segment of midsize companies.

CANCOM

CANCOM convinces its customers with customized solutions based on a comprehensive range of topics and services. CANCOM offers high-performance technical cybersecurity services for SMEs and demanding KRITIS sectors.

Capgemini

Capgemini distinguishes itself with thought leadership as an innovative provider of TSS and can boast a large international team.

Computacenter

Computacenter combines its strong partner network with comprehensive services and in-house expertise to position itself as a TSS leader in the German market.

controlware

With its targeted and modular technical cybersecurity services and German roots, **Controlware** knows how to succeed in the fast-growing SME segment.

Based on a large, highly qualified team and a seamless end-to-end service offering made in Germany, **Deutsche Telekom** is the **security** leader for TSS in Germany.

DXC TECHNOLOGY

DXC Technology's customers benefit from integrated IT/security solutions and the efficiency of an internationally active, extensive team.

EVIDEN
an atos business

Eviden (an Atos Business) has established itself as a leading provider of TSS in Germany, among other things, through a holistic cybersecurity approach that also emphasizes business relevance.

IBM

IBM impresses major clients with its extensive experience, comprehensive cybersecurity expertise and strong international delivery capabilities.

HCLTech

HCLTech (Rising Star) is increasingly successful and thus is the rising star for TSS in Germany. The provider impresses with international experience, a comprehensive range of services and high-quality technology partnerships.

Strategic Security Services

Who Should Read This Section

This report is relevant for German enterprises evaluating SSS providers and trying to understand the competitive market landscape. Leveraging this information, enterprises can select providers capable of assessing security maturity, defining tailored cybersecurity strategies and mitigating risks effectively.

German enterprises are adopting trends such as consolidating technology for streamlined security infrastructure and embracing zero trust security principles to enhance their cybersecurity posture. Integrating security technologies with firewalls, CASBs and threat intelligence platforms is also increasing to enhance real-time threat detection and response capabilities.

Service providers in the German market offer a range of solutions, including securing edge computing, implementing secure internet gateway systems and enhancing zero trust philosophies with context-aware access controls. They also provide cloud-based delivery models, AI- and ML-powered security controls, and consistent security across multicloud environments to meet evolving customer needs.

This ISG report offers valuable insights into the SSS provider landscape and industry trends. German enterprises can make informed decisions when selecting a service provider, while service providers can stay updated on market developments and tailor their offerings to effectively meet evolving security demands.

IT security professionals should read this report to gain insights into the current positioning of SSS providers and evaluate their capabilities in assessing security maturity and defining tailored cybersecurity strategies.

IT directors should read this report to understand the competitive market landscape and trends in security services, enabling informed decision-making when selecting service providers.

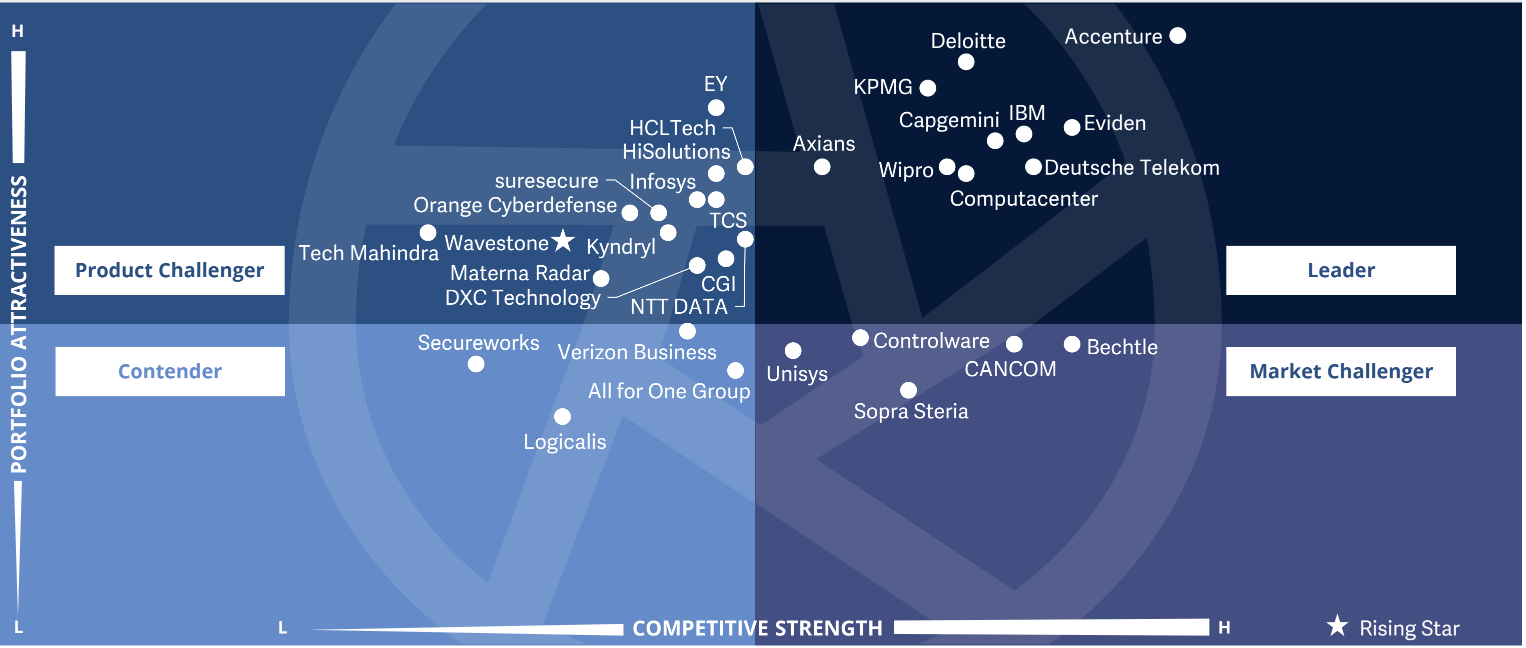
Compliance officers should read this report to ensure alignment with security standards and regulations, leveraging the information provided in the report to enhance security posture.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Strategic Security Services

Germany 2024



This quadrant focuses on the **most relevant** cybersecurity consultants in Germany who offer services for more than just their own products. Their services are **increasingly in demand in the** wake of growing cyber threats and new technologies.

Frank Heuer

Definition

The SSS providers assessed for this quadrant offer IT and OT security consulting. The services include security audits, compliance and risk advisory services, security assessments, security solution consulting, and awareness and training. These providers also help assess security maturity and risk posture and define cybersecurity strategies for enterprises based on their specific requirements.

These providers should employ security consultants with extensive experience in planning, developing and managing end-to-end security programs for enterprises. With the growing need for such services among SMBs and the lack of talent availability, SSS providers should also make these experts available on-demand through vCISO (virtual Chief Information Security Officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity road maps and prioritize business-critical applications for recovery. They should also conduct periodic tabletop exercises and cyber drills for board members, key business executives and employees to help them develop cyber literacy and establish best practices to better respond to actual threats and cyberattacks. They should also be adept with security technologies and products available in the market and offer advice on choosing the best product and vendor suited to an enterprise's specific requirements.

This quadrant examines service providers that are not exclusively focused on proprietary products or solutions. The services analyzed here cover all security technologies, including OT security and SASE.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. **Offer at least one of the above** strategic security services in the respective country
3. Provide **security consulting services using frameworks**
4. **No exclusive focus** on **proprietary products** or solutions

Observations

The cybersecurity threat situation continues to escalate. The war in Ukraine is just the most prominent example of the escalation of threats. Together with a lack of resources, this is leading to an increasing need for orientation with regard to cybersecurity. New, technically sophisticated threats are also on the horizon for the near future.

In the face of increasingly intense and sophisticated cyberattacks - also in the wake of geopolitical conflicts - companies are being called upon to protect their IT systems from damage. Well-known large companies, public authorities and small and midsize companies are no-longer affected. At the same time, the shortage of IT specialists continues to make this situation more difficult, with SMEs suffering in particular. These factors mean that companies increasingly need external support. This often starts with consulting.

Providers with a balanced customer structure consisting of major customers and SMEs benefit from the large budgets of major customers and the above-average growth in demand from SMEs.

Furthermore, service providers who can offer security consulting to their customers and also implement and operate so that the strategy can be seamlessly put into practice have an advantage. Providers who, in addition to security consulting, can also offer associated IT solutions—and possibly also associated redesigned business processes—from a single source have an advantage. The first consultants are gearing up to defend against quantum-based cyberattacks.

Secureworks and Zensar are no longer represented in the quadrant.

Of the 85 providers evaluated in this study, 33 qualified for this quadrant. Of these, ten achieved a position as Leader. One provider was identified as a Rising Star.

accenture

Experience, expertise and a comprehensive range of services that have been systematically developed further contribute to **Accenture's** great success in cybersecurity consulting in Germany.

axians

With its pragmatic, targeted approach to cybersecurity consulting, **Axians IT Security** meets the needs of the SME target group. The portfolio is also being developed dynamically.

Capgemini

Capgemini convinces its German clients in cybersecurity consulting with a broad range of consulting services, experience and up-to-date consulting approaches.

Computacenter

Computacenter supports its customers with cybersecurity consulting that is integrated into a holistic end-to-end approach, enabling it to position itself as a strategic partner with an understanding of its customers' infrastructure and business requirements.

Deloitte.

Deloitte has a strong global presence and understands the synthesis of business and technology consulting in cybersecurity consulting.

T

With extensive experience in demanding environments and end-to-end services from a single source, **Deutsche Telekom** is an impressive cybersecurity consultant in Germany.

Eviden (an Atos Business) has established itself as a leader in the German market for cybersecurity consulting. It is a new provider with a holistic approach and numerous certifications.

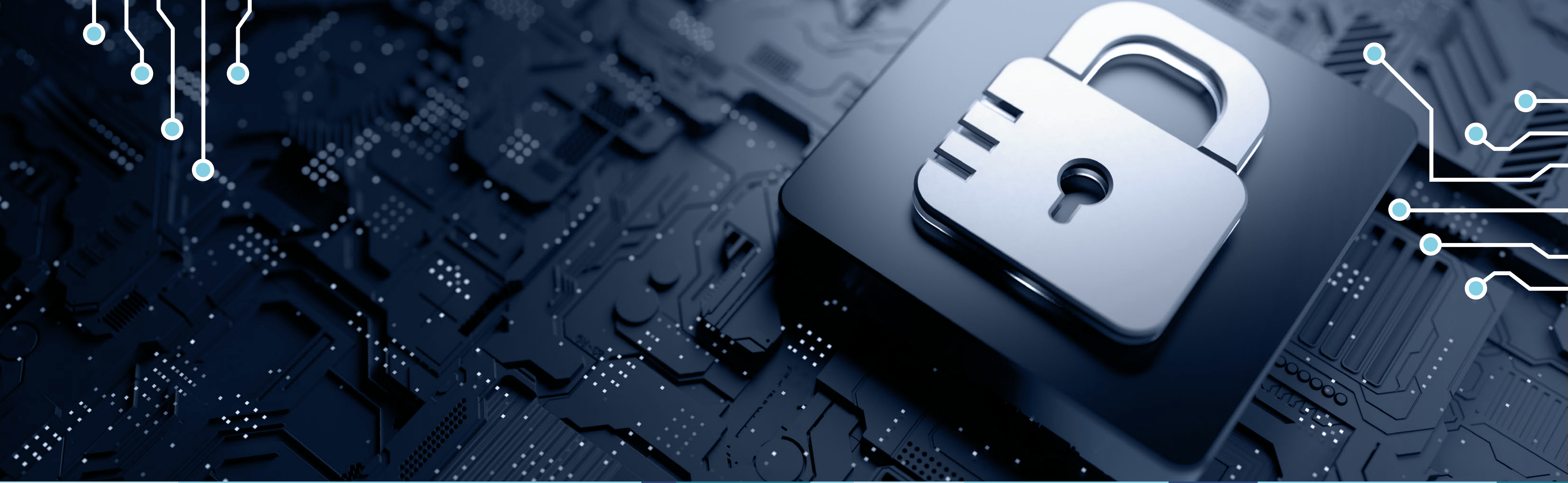
IBM's cybersecurity consulting clients benefit from the provider's comprehensive, integrated and innovative portfolio and deep technological expertise, making IBM a leading consulting firm in Germany.

KPMG distinguishes itself in cybersecurity consulting in Germany with a high level of strategic expertise and the skillful integration of technical and business aspects.

Wipro impresses its customers in Germany with its comprehensive technical expertise and extensive services and its customer-oriented pricing model for cybersecurity consulting.

Wavestone

With the sensational merger with Q_PERIOR, **Wavestone (Rising Star)** suddenly increased its presence in the German market and immediately positioned itself as the rising star for cybersecurity consulting.



Managed Security Services – SOC

Who Should Read This Section

This report is relevant to German enterprises to understand the MSS market landscape, enabling them to make informed decisions when selecting MSS providers that align with their unique security needs.

The ISG report offers insights into critical market challenges and how each provider addresses them, enabling enterprises to assess the capabilities of MSS providers in meeting their security requirements.

German enterprises seek robust security solutions to counter the increasing number of cyber threats, particularly in remote work and cloud-based services. They require continuous monitoring, advanced threat detection capabilities, incident response and remediation support to ensure business continuity and protect their valuable data and systems from ransomware attacks.

MSS providers in the German market offer services tailored to meet these needs, including managed detection and response (MDR) services, advanced analytics, AI, ML and deep learning techniques for behavior-based threat analysis, and threat intelligence as a service. MSS providers cater to the growing demand for zero trust and SASE frameworks, ensuring enterprises have access to the latest security technologies and expertise to protect their operations from evolving threats.

Chief information security officers should read this report to gain insights into the current market landscape of MSS providers, enabling them to make informed decisions.

Chief technology officers should read this report to evaluate the potential impact of MSS on their organization's technology infrastructure.

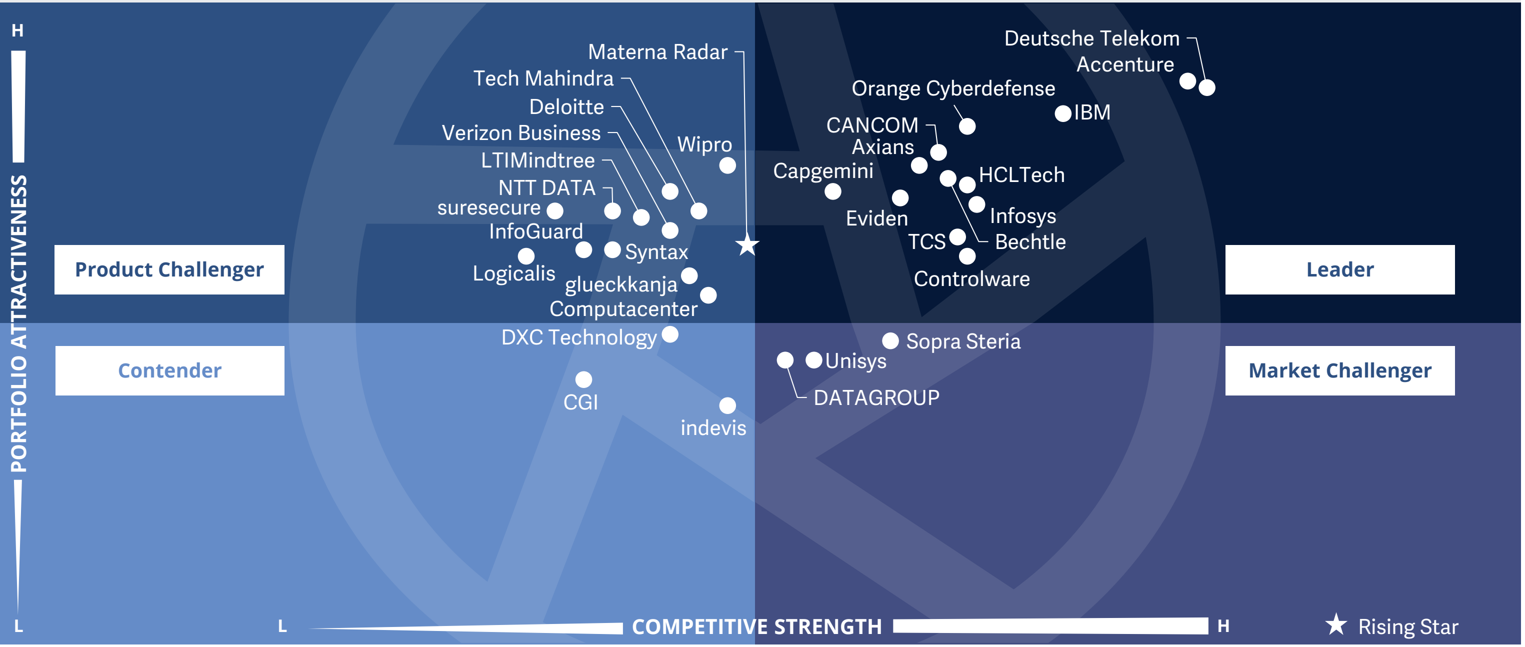
Risk and compliance officers should read this report for insights into current security trends and regulations, ensuring their organization's security posture aligns with industry standards and regulatory needs.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Managed Security Services - SOC

Germany 2024



This quadrant focuses on the **most relevant** providers of **managed security services from SOCs** on the German market, excluding service providers that only offer their services for their own products. The threat situation and skills shortage are **driving** the market.

Frank Heuer

Definition

The providers assessed in the MSS-SOC quadrant offer services related to the continuous monitoring of IT and OT security infrastructures and management of IT infrastructure for one or several customers by a security operations center (SOC). **This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools.** These service providers can handle the entire security incident lifecycle from identification to response.

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional MSS with innovation to fortify clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies and infrastructure. They must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, Security Information and Event Management (SIEM) services,** security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. **Manage own SOCs**
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models

Observations

The demand for MSS from SOCs is being driven by increasingly sophisticated, frequent, complex and versatile cyberattacks. The shortage of qualified experts and the need for specialist knowledge that is always up to date are also pushing these services into the focus of German companies.

Globally distributed SOCs play a special role for large companies due to their often international presence. However, large companies also value EU and German SOC locations due to the increased importance of data protection. In addition, this target group often expects individually tailored solutions for their specific requirements.

Midsize companies are also increasingly interested in SOC services in order to master the growing challenges of a severe shortage of skilled workers. SOCs in Germany and German-speaking contacts are plus points for this target group.

In general, providers are also expected to be highly innovative in order to stay ahead in the race against cyber criminals. This includes the expansion of SOCs in the direction of cyber defense centers, whereby the increasingly complex threats are also countered with AI and automation. In addition to reactive measures, proactive prevention services are also becoming increasingly important. For industrial customers, the inclusion of OT security to secure networked production facilities is becoming increasingly interesting.

From the 85 providers assessed for this study, 32 qualified for this quadrant, with thirteen being Leader and one Rising Star.

accenture

Comprehensive services, a broad spectrum of addressed technologies, a global presence and the development of new target groups are the basis for **Accenture's** great success in the German market for managed security/SOC services.

axians

Axians IT Security is increasingly successful in the German market for managed security/SOC services with its comprehensive, customer-oriented services.

BECHTLE

Bechtle impresses its customers with comprehensive, certified and modularly adaptable managed security/SOC services, thus positioning itself as a leader in Germany.

CANCOM

With a growing range of managed security products covering a broad spectrum of managed technologies and SOC services made in Germany, **CANCOM** is making a name for itself as a leader in the German market.

Capgemini

Capgemini's success in the German market for managed security/SOC services is based on comprehensive services, strong resources and international presence.

controlware

Modular, customizable services and SOC services made in Germany contribute to **Controlware's** success in the German market for managed security/SOC services.

T

With its comprehensive, advanced managed security/SOC services, large qualified team and its operations in Germany, **Deutsche Telekom** is a leading provider.

EVIDEN
an atos business

Eviden (an Atos Business) scores with a comprehensive offering, innovative approaches and the global availability of its managed security/SOC services.

HCLTech

HCLTech's strong commitment to the German market for managed security/SOC services is paying off. Among other things, several dedicated SOCs are operated in Germany.

IBM

IBM combines its own high-performance technology with comprehensive, globally available managed security/SOC services for the benefit of internationally active major customers.

Infosys

Infosys has extensive resources and is continuously developing its managed security/SOC services for the benefit of its key accounts, positioning itself as a leader in these services.

orange Cyberdefense

Orange Cyberdefense scores with its European origin, global and local presence and continuously optimized managed security/SOC services.

tcs TATA CONSULTANCY SERVICES

Cost-efficient solutions, global presence and comprehensive technology coverage, including OT security, make **TCS** a leader in the German market for managed security/SOC services.

MATERNA RADAR CYBER SECURITY

Materna Radar is the new Rising star for managed security/SOC services in Germany. The clever expansion of Materna's business and services based on European technology contributed to this.

Infosys

Leader

> "Infosys is continuously developing its managed security/SOC services to benefit its key accounts, positioning itself as a leader in these services."
>
> *Frank Heuer*

Overview

Headquartered in Bengaluru, India, Infosys has more than 322,600 employees across 274 offices in 56 countries. In the 2023 financial year, the company generated revenue of $18.2 billion, with Financial Services being its largest segment. In addition to strategic security services and technical security services, Infosys also offers managed security services. These include the Infosys *Cyber Next - Platform Powered Services*, which provide insight into security events, automated response capabilities and proactive vulnerability management.

Strengths

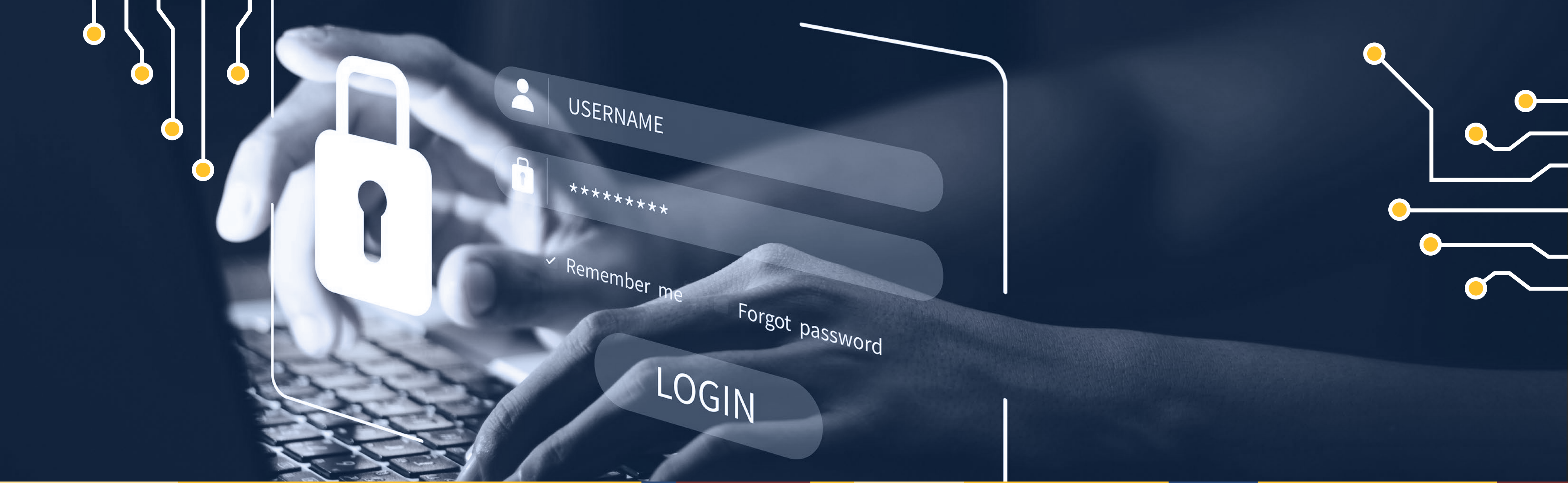
Continuous improvement of the security level: Infosys helps its clients stay current and supports them in continuously improving their cybersecurity maturity. For this, Infosys leverages its global network of Cyber Defense Centers spread across the US, Europe and India.

Delivery and services from Germany: Infosys has a strong presence in Germany and is well-staffed regarding its MSS in this country. In addition, Infosys now has two dedicated SOCs in Germany. Infosys' business in Germany is growing very strongly.

Wide range of services: Infosys offers comprehensive MSS that leaves nothing to be desired. In addition, the services cover a broad spectrum of security technologies. This is particularly interesting for large companies with a diverse security landscape. Infosys is also expanding its MSS with a comprehensive roadmap ahead. Together with the Infosys Center for Emerging Technology Solutions, Infosys Cybersecurity is constantly developing innovations, validating them and bringing new solutions to the market.

Caution

Infosys is almost entirely geared toward the needs of large companies, with hardly any focus on midsize companies, which need to catch up in terms of MSS. With its SOC operations in Germany, Infosys is well-placed to tap into this target group.



Managed Security Services – SOC (Midmarket)

Who Should Read This Section

This report is relevant to midmarket enterprises in Germany to understand the MSS market landscape, enabling them to make informed decisions when selecting MSS providers that align with their unique security needs. This ISG report offers insights into critical market challenges and how each provider addresses them, enabling enterprises to assess MSS providers' capabilities in meeting their security requirements.

Midmarket enterprises in Germany seek robust security solutions to counter the increasing number of cyber threats, particularly in remote work and cloud-based services. They require continuous monitoring, advanced threat detection capabilities, incident response and remediation support to ensure business continuity and protect their valuable data and systems from ransomware attacks.

These businesses prioritize IT investment to stay technologically advanced, leveraging technologies such as cloud computing, big data and IoT to enhance operational efficiency and drive revenue growth.

MSS providers in the German market offer services tailored to meet these needs, including managed detection and response (MDR) services, advanced analytics, AI, ML and deep learning techniques for behavior-based threat analysis, and threat intelligence as a service. Furthermore, MSS providers address the growing demand for zero trust and SASE frameworks, ensuring enterprises have access to the latest security technologies and expertise to protect their operations from evolving threats.

IT security managers should read this report to gain insights into the current market landscape of MSS providers and the latest trends in security technologies and services.

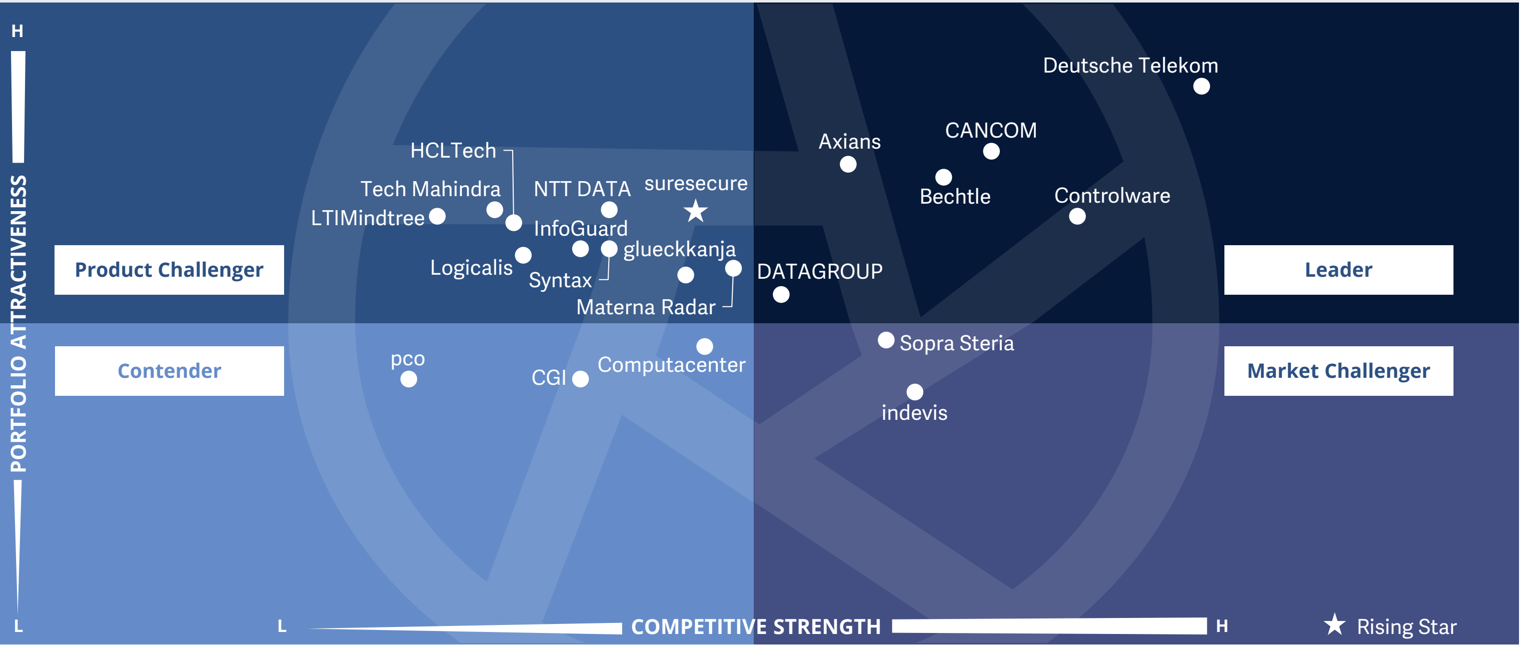
Chief information officers should read this report to learn how MSS providers address critical market challenges and evaluate the potential impact on their organization's IT strategy and operations.

Chief technology officers should read this report to understand the latest trends and technologies in the MSS market and make informed decisions.

Cybersecurity – Solutions and Services
Managed Security Services - SOC (Midmarket)

Germany 2024

Source: ISG RESEARCH



This quadrant focuses on the **most relevant** providers of **managed security services from SOCs** for German SMEs, excluding providers that only support their own products. The **shortage of skilled workers** is leading to increasing demand.

Frank Heuer

Definition

The providers assessed in the MSS-SOC quadrant offer services related to the continuous monitoring of IT and OT security infrastructures and management of IT infrastructure for one or several customers by a security operations center (SOC). **This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools**. These service providers can handle the entire security incident lifecycle from identification to response.

There is an increasing demand for providers to assist enterprises in enhancing their overall security posture and maximizing the long-term effectiveness of their security programs through continuous improvement. MSS-SOC providers must combine traditional MSS with innovation to fortify clients with an integrated cyber defense mechanism. They should be capable of delivering managed detection and response (MDR) services and be equipped with the latest technologies and infrastructure. They must also have expertise in threat hunting and incident management to support enterprises in actively detecting and responding through threat mitigation and containment. To meet the growing customer expectations for proactive threat hunting, providers are enhancing their SOC environments with security threat and vulnerability intelligence, with significant investments in technologies such as automation, big data, analytics, AI and ML. These sophisticated SOCs support expert-driven security intelligence response, offering clients a holistic and unified approach to advanced-level security.

Eligibility Criteria

1. Typical services include **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, Security Information and Event Management (SIEM) services**, security advisors and auditing support, remotely or at a client's site
3. Possess **accreditations** from security tools vendors
4. Manage own SOCs
5. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
6. Offer various pricing models

Observations

Midsize companies in Germany are even more affected by the shortage of cybersecurity specialists than large companies. At the same time, they are confronted with new and more complex security challenges and are increasingly targeted by cybercriminals who believe this target group to be easy victims. As a result, even medium-sized companies increasingly rely on external services such as security operations centers. SOCs have the necessary up-to-date specialist knowledge and equipment to continuously monitor customer systems.

For the SME segment, SOCs in Germany are a plus point for trust and data protection. In addition, decision-makers in SMEs appreciate the geographical proximity to service providers. German-speaking contacts also play an important role in this customer group. Many SMEs offer their customers pragmatic, fast solutions and therefore often expect their service providers to provide uncomplicated, fast implementation, including rapid onboarding for SOC services.

SMEs also expect SOC service providers to be highly innovative in order to stay ahead of cybercriminals. This includes using AI and automation to master even more complex threats. In addition to reactive measures, proactive prevention services are becoming increasingly important. For industrial customers, including OT security to secure networked production facilities is becoming increasingly interesting.

From the 85 providers assessed for this study, 21 qualified for this quadrant, with six being Leaders and one Rising star

axians

Axians IT Security can convince its midsize customers with comprehensive and needs-oriented SOC services. This makes the provider one of the leading SOC service providers in Germany.

BECHTLE

With its comprehensive and adaptable services and delivery from Germany, **Bechtle** is a leader in SOC services for German SMEs.

CANCOM

CANCOM is expanding its SOC services and can thus strengthen its position as a leading service provider for German SMEs.

controlware

With its flexible, customer-oriented services, **Controlware** is a leader in the market for SOC services for German SMEs.

DATAGROUP

DATAGROUP succeeds in becoming one of the leading providers of managed security/SOC services for the German Mittelstand with high-quality, integrated services.

T

Deutsche Telekom Security is the leading provider of managed security/SOC services for German SMEs, with a large team and a comprehensive range of products and services.

sure[secure]

With its focus on the dynamically growing target group and an innovative technology platform, **suresecure** is the rising star for managed security/SOC services for German SMEs.

Star of Excellence

A program, designed by ISG, to collect client feedback about providers' success in demonstrating the highest standards of client service excellence and customer centricity.

Customer Experience (CX) Insights

Source: ISG Star of Excellence™ research program, Insights till June2024

In the ISG Star of Excellence™ research on enterprise customer experience (CX), clients have given feedback about their experience with service providers for their **Cybersecurity Solutions and Services**.

Based on the direct feedback of enterprise clients, below are the key highlights:

Client Business Role

▲ **Most satisfied**
Information Technology

▼ **Least satisfied**
Human Resources

Region

▲ **Most satisfied**
Africa

▼ **Least satisfied**
Eastern Europe

Industry

▲ **Most satisfied**
Chemicals

▼ **Least satisfied**
Public sector

Industry Average CX Score

81.9

▲ Highest CX: 91.0
▼ Lowest CX: 64.8

CX Score: 100 most satisfied, 0 least satisfied
Total responses (N) = 419

Most Important CX Pillar

Execution and Delivery

Service Delivery Models	Avg % of Work Done
Onsite	53.6%
Nearshore	21.6%
Offshore	24.8%

service
digital transformation
work
understand
provide
requirement
team
business
real time
cloud computing
high quality
needs
challenge
cutting edge
high level
solution
organization
company
result
commitment
performance
success
difficult
supply chain
flexible
order
cyber security
data management
service provider
cloud service
data security
improve
ability
lack
missing
expectations
complaint
helped
product
innovative solutions
right time
beginning
everything
focus
innovation
time
long term
supporting
cloud based
managed service
lacking
carried
make
help
address
cloud infrastructure
impact
tool
working
happy
excellence
specialized skills
customer experience
timely manner
resolved
automation solutions
transformation service
new services
management services
quality control
cloud security
application development
customer oriented
consultant
project management
highest level
knowledge
compared
new solutions
manage
deploy
transition
quick response
security solution
emerging technologies
strategic partnership
digital workplace
technical solution

Appendix

The ISG Provider Lens 2024 – Cybersecurity – Solutions and Services research study analyzes the relevant software vendors/service providers in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Authors:
Frank Heuer, Gowtham Sampath (Global – SSE), and Dr. Maxime Martelli (Global – XDR)

Editors:
Maria Müller-de Haen and Indrani Saha

Research Analyst:
Monica K

Data Analysts:
Rajesh Chillappagari and Laxmi Sahebrao

Consultant Advisor:
Roger Albrecht

Project Manager:
Shreemadhu Rai B

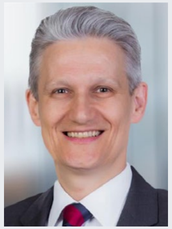
Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of May 2024, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars ($US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Solutions and Services market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
   * Strategy & vision
   * Tech Innovation
   * Brand awareness and presence in the market
   * Sales and partner landscape
   * Breadth and depth of portfolio of services offered
   * CX and Recommendation



Author

Frank Heuer

Principal Analyst

Frank Heuer is a Principal Analyst at ISG Germany. His focus is on cybersecurity, digital workspace, communication, social business & collaboration and cloud computing.

His main areas of responsibility include advising ICT providers on strategic and operational marketing and sales. Mr. Heuer is a speaker at conferences and webcasts on his main topics and a member of the IDG expert network. Mr. Heuer has been active as an analyst and consultant in the IT market since 1999.

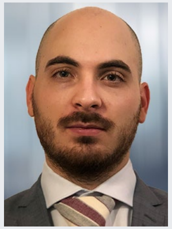
Author - SSE (Global)

Gowtham Sampath

Senior Manager, ISG Provider Lens™

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries. He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Author - XDR (Global)



Dr. Maxime Martelli

Consulting Manager

Maxime Martelli is a Consulting Manager at ISG France. He takes part in ISG's "Digital & Strategy" solution for multinational firms and the public sector services, as well as applying his expertise around Information Security and Cloud Security projects. Author, teacher and lecturer in the field of IT, Maxime is passionate about technology and applies his knowledge of processes, digital strategy, and IT organization to satisfy his clients' requirements. As a Security Analyst, he conducts transformation and strategy projects for all kind of Security tools and solutions, with a strong focus on SOC/SIEM and SASE next-generation security transformations.

Enterprise Context and Global Overview

Monica K

Assistant Manager, Lead Research Specialist

Monica K is an Assistant Manager and Lead Research Specialist and a digital expert at ISG. She has created content for the Provider Lens™ studies, as well as content from an enterprise perspective, and she is the author of the global summary report for Cybersecurity, ESG and sustainability market. Monica K brings over a decade year of experience and expertise in technology, business and market research for ISG clients.

Her previous role was at a research firm where she specialized in emerging technologies such as IoT and product engineering, vendor profiling, and talent intelligence. Her portfolio included the management of comprehensive research projects and collaboration with internal stakeholders on diverse consulting initiatives.

Study Sponsor

Heiko Henkes

Director and Principal Analyst

Heiko Henkes serves as Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens™ (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as a strategic program manager and thought leader for IPL lead analysts.

Henkes heads Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice. His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation, IT competencies, sustainable business strategies and change management in a cloud-AI-driven business landscape. Henkes is known for his contributions as a keynote speaker on digital innovation, sharing insights on using technology for business growth and transformation.

IPL Product Owner

Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens™ research, please visit this webpage.

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including AI and automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.

ISG Provider Lens™

JULY, 2024

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES