

# 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:



Executive Summary	04
Provider Positioning	07
Introduction	
Definition	18
Scope of Report	20
Provider Classifications	21
Appendix	
Methodology & Team	65
Author & Editor Biographies	66
About Our Company & Research	68

---

Identity and Access Management (IAM)	22 – 26
Who Should Read This Section	23
Quadrant	24
Definition & Eligibility Criteria	25
Observations	26

---

Data Leakage/Loss Prevention (DLP) and Data Security	27 – 32
Who Should Read This Section	28
Quadrant	29
Definition & Eligibility Criteria	30
Observations	31

---

Extended Detection and Response (XDR)	33 – 37
Who Should Read This Section	34
Quadrant	35
Definition & Eligibility Criteria	36
Observations	37

---

Security Service Edge (SSE)	38 – 43
Who Should Read This Section	39
Quadrant	40
Definition & Eligibility Criteria	41
Observations	42

---

## Technical Security Services

44 – 50

Who Should Read This Section	45
Quadrant	46
Definition & Eligibility Criteria	47
Observations	48
Provider Profile	50

---

## Managed Security Services - SOC

58 – 63

Who Should Read This Section	59
Quadrant	60
Definition & Eligibility Criteria	61
Observations	62

---

## Strategic Security Services

51 – 57

Who Should Read This Section	52
Quadrant	53
Definition & Eligibility Criteria	54
Observations	55
Provider Profile	57

Report Author: Frank Heuer

**Current crises and the SME segment are driving the German cybersecurity market**

Currently, companies are facing various challenges in terms of cybersecurity. Increased cyberthreats due to the Ukraine war, the upheavals caused by the COVID-19 pandemic, which have been overcome, and the long-term trend of digitization have created vulnerabilities for cyberattacks in Germany, requiring appropriate countermeasures. On the other hand, the weakened economy presents further financial challenges.

As businesses undergo digital transformation, more processes are being shifted to IT. Digital representation of intellectual corporate property is also increasing. Protecting IT and communication systems has become essential for corporate security. The COVID-19 crisis has further heightened the need for IT security, as remote work and external connectivity of employees have increased the susceptibility of

IT systems to attack. With remote work likely to continue even after the pandemic, this challenge will persist.

**The shortage of skilled workers is driving the demand for external cybersecurity service providers in Germany.**

The increased use of cloud resources, hybrid work and the vulnerability it brings to IT systems have emphasized the relevance of the zero-trust approach. The principle of *never trust, always verify* means, among other things, mutual authentication and continuous network monitoring.

Cybercriminals are developing new, sophisticated and complex methods to bypass companies' and authorities' cyber defense systems at shorter intervals than ever. In the past year, there have been notable cyberattacks, including ransomware attacks, causing significant trouble for businesses. Accordingly, cybersecurity measures must be seamlessly up to date. More companies and public authorities

Cybersecurity challenges are increasing for businesses in various ways.



are struggling with this, particularly due to the shortage of IT specialists, especially in the cybersecurity market. As a result, IT managers and executives are increasingly turning to external service providers, such as managed security service providers, that employ proactive rather than reactive methods based on AI to safeguard against such threats.

Cybersecurity providers seeking above-average growth in Germany should prioritize the needs of SMEs and effectively communicate with this segment.

In addition to the company's own protection, legal regulations such as the General Data Protection Regulation (GDPR) in the EU also require companies to implement stronger security measures to prevent cyberattacks. Compliance with these regulations remains a major challenge for midsize companies in particular.

On the other hand, SMEs present an interesting market segment for cybersecurity providers. As they upgrade their less mature IT security systems, as compared to large enterprises, driven by the factors described above, there is an above-average growth in the demand for cybersecurity solutions among SMEs. Having a balanced customer structure for both midsize and large companies is advantageous for providers to leverage the budgets of large accounts. Despite the economic slowdown, the demand for cybersecurity solutions remains unaffected among SMEs, making it an increasingly attractive market segment and the one that needs to be addressed adequately. The services meant for large customers cannot simply be offered to SMEs. Rather providers should tailor their entire go-to-market strategy, including products, prices and communication, to suit the needs of SMEs. Providers must understand that communication and cultural aspects are particularly important to be accepted by SMEs.

Despite the great importance of cybersecurity, IT managers are increasingly struggling with justifying IT security investments to

stakeholders, especially the CFOs. Unlike other IT projects, it is not always easy to prove the return on investment or quantify threat risks. However, executives are increasingly aware that cyberattacks can lead to significant financial and reputational damage. Consequently, cybersecurity is gaining importance within companies, and senior management is becoming more involved in cyber risk management.

Furthermore, technical factors alone do not contribute to the vulnerability of IT systems. Careless user behavior, such as falling victim to Trojan and phishing attacks, play a key role in facilitating cyberattacks. Therefore, in addition to updated security equipment, user training and consulting also play an important role.

Looking ahead, there are future technical threats to consider, such as quantum-based attacks that target the encryption of confidential data. Some service providers have already started adapting their consulting services to address this new challenge.

### **Identity and Access Management (IAM)**

In terms of cybersecurity topics, IAM holds significant importance, especially with the increasing digitalization of all areas and the need to protect not only users but also machines and certain areas within companies, such as Industry 4.0.

The growing number of users, devices and services necessitates effective management of digital identities, especially considering the rise in remote work due to the pandemic. Many employees are accessing corporate resources remotely, making regulation and control of access to data and systems even more important.

### **Data Leakage/Loss Prevention (DLP) and Data Security**

DLP solutions have witnessed increasing demand in Germany in the recent past due to various factors affecting data security within organizations. The importance of data, IP and corporate assets has significantly increased, making protection against unwanted data leaks, especially from private end devices used for business purposes, a major challenge for companies.



### Extended Threat Detection and Response (XDR)

XDR solutions have gained prominence and traction over the past two years as organizations aim to better understand and contextualize (correlate) information gathered from various security tools deployed in their IT infrastructure. Automation plays a central role in this, and leading providers offer behavioral and contextual analytics modules, as well as open integration with other endpoint and network detection and response products.

### Security Service Edge (SSE)

SSE solutions are still in the early stages of maturity and adoption by enterprises. SSE includes solutions that enable enterprises to securely access the cloud, facilitate remote work, secure edge computing and support digital transformation. The increasing number of remote and hybrid workers and the transition to the cloud have created the need for SSE solutions.

### Strategic Security Services

Amidst the acute crises arising from the Ukraine war and the effects of the COVID-19

pandemic, companies in Germany are facing several challenges concerning IT security and data protection. The growing threat landscape and resource scarcity create a greater need for orientation.

As cyberattacks become more intense and sophisticated, companies must protect their IT systems from damage. This challenge extends beyond well-known large companies and public authorities to small and midsize companies. However, the shortage of IT specialists further complicates this situation, especially for midsize companies. The midmarket is thus a segment that is growing at an above-average rate and is consequently becoming increasingly attractive.

### Technical Security Services

In the face of increasingly sophisticated cyberattacks and a shortage of skilled workers, companies and public authorities in Germany are relying more on external service providers to keep their IT security systems up to date.

Cybercriminals are taking advantage of careless user behavior, and thus incidents of Trojan, phishing and ransomware attacks are becoming

more common. Along with having updated security equipment, user training continues to play an important role.

IT security projects are often demanding and multifaceted, so service providers that offer a wide range of technical security services from a single source have an advantage here.

### Managed Security Services (SOC)

The increasing frequency and complexity of cyberattacks, along with the challenges posed by the current crises, have created a demand for managed security services in particular. The scarcity of qualified resources and the need for updated specialist knowledge are driving German companies to focus on these services.

Managed security services providers rely on AI and automation to combat cyberattacks, but human expertise remains indispensable.


Both large and midsize customers prefer SOCs located in Germany due to the increasing

importance of data protection. End-to-end security services, integrated solutions comprising IT and related security solutions, and innovation are crucial for staying ahead of cybercriminals.

Managed security services providers are increasingly using AI and automation to combat cyberthreats, combining machine efficiency with human expertise.


In the future, cybersecurity service providers must equip their customers to defend against quantum-based attacks.



 Provider Positioning

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




 Provider Positioning

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






 Provider Positioning


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



 Provider Positioning


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



 Provider Positioning


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



 Provider Positioning


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



 Provider Positioning


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



 Provider Positioning


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



 Provider Positioning

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



 Provider Positioning

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







## Provider Positioning

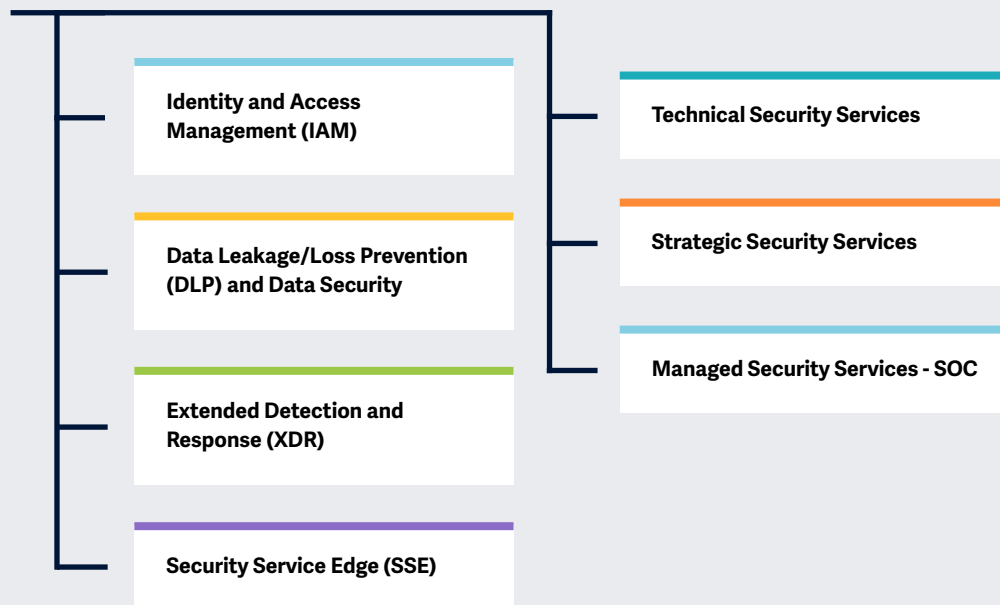
Page 11 of 11

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



## Focus areas of the Cybersecurity – Solutions & Services 2023 study.

Simplified Illustration Source: ISG 2023



### Definition

From a cybersecurity perspective, 2022 could be described as turbulent; despite declining data breaches, attacks this year were significantly more sophisticated and severe. In 2022, companies increased their investment in cybersecurity and placed a high priority on corresponding initiatives to prevent attacks and improve their security posture. They had learned their lesson from the 2021 attacks; executives and companies of all sizes and industries invested accordingly in measures to respond to and weather cybersecurity threats and cyberattacks.

Even small businesses are now aware of the dangers posed by cyberthreats and have realized that they are actively targeted and highly vulnerable to cyberattacks. This has increased the need for (managed) security services and cyber resiliency services that enable companies to quickly resume operations after a cyber incident. Service providers and vendors are therefore offering services and solutions to support recovery and business continuity.



Cybercriminals exploited major vulnerabilities such as Log4shell and continued to disrupt business activities with ransomware; the healthcare, supply chain, and public sectors were particularly targeted.

Enterprises responded by investing in capabilities such as identity and access management (IAM), data loss prevention (DLP), managed detection & response (MDR), and securing the cloud and endpoints. The market is shifting toward integrated solutions such as Security Service Edge (SSE) and Extended Detection & Response (XDR); using best-of-breed tools, staff expertise, and complementary behavioral and contextual intelligence and automation to improve security posture.



### Scope of the Report

In this ISG Provider Lens™ Quadrant Report, ISG covers the following seven quadrants for services/solutions: Identity and Access Management (IAM), Data Leakage/Loss Prevention (DLP) and Data Security, Extended Detection and Response (XDR), Security Service Edge (SSE), Strategic Security Services, Technical Security Services, Managed Security Services - SOC. Security Service Edge (SSE) solution providers are initially analyzed and positioned from a global perspective in this year's study, rather than from the perspective of individual countries and regions, as the market is currently still in its early stages and maturing process.

The ISG Provider Lens™ study Cybersecurity - Solutions and Services 2023 offers business and IT decision makers the following benefits:

- Transparent presentation of the strengths and weaknesses of relevant providers
- A differentiated positioning of suppliers by segment, based on competitive strengths and portfolio attractiveness

- Focus on regional markets

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 IT providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT 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 IT 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 Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have 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 (exceptions are 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.

**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.

**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.

**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 (IAM)

## Identity and Access Management (IAM)

### Who Should Read This Section

This quadrant is relevant to enterprises in Germany for evaluating IAM solution providers. It further assesses how each provider helps enterprises manage complex security challenges associated with securing user access and digital identities.

ISG defines the current positioning of IAM players with a comprehensive overview of the competitive market landscape.

In Germany, enterprises are taking a zero-trust approach to consolidate IAM and related tools. They are modernizing IAM systems to simplify their IAM infrastructure, reduce complexity and improve overall security posture by centralizing identity and access management policies and controls. By adopting a zero trust approach to IAM, organizations can further enhance security by implementing continuous monitoring, risk-based access controls and adaptive authentication mechanisms. Cloud-based IAM platforms support dynamic access controls and real-time risk assessments. Integrating IAM tools with AI and ML technologies is gaining traction as it is crucial for protecting

enterprises' sensitive data and systems from cyber threats. Real-time analysis of privileged account activity, user behavior and access requests to gain deeper insights into potential security threats and respond quickly to mitigate risks. This approach helps organizations comply with industry regulations and protect sensitive information from cyber threats. The rise of passwordless authentication is expected to continue as it improves UX and enables a frictionless login experience, essential for digital businesses driving enterprises to look for more secure authentication methods.



**Cybersecurity professionals** should read this report to understand how providers use technologies to address compliance and security concerns while offering a seamless experience to enterprise clients.



**Strategy professionals** should read this report to understand how IAM tools can enhance UX while improving the security and efficiency of their systems and data.

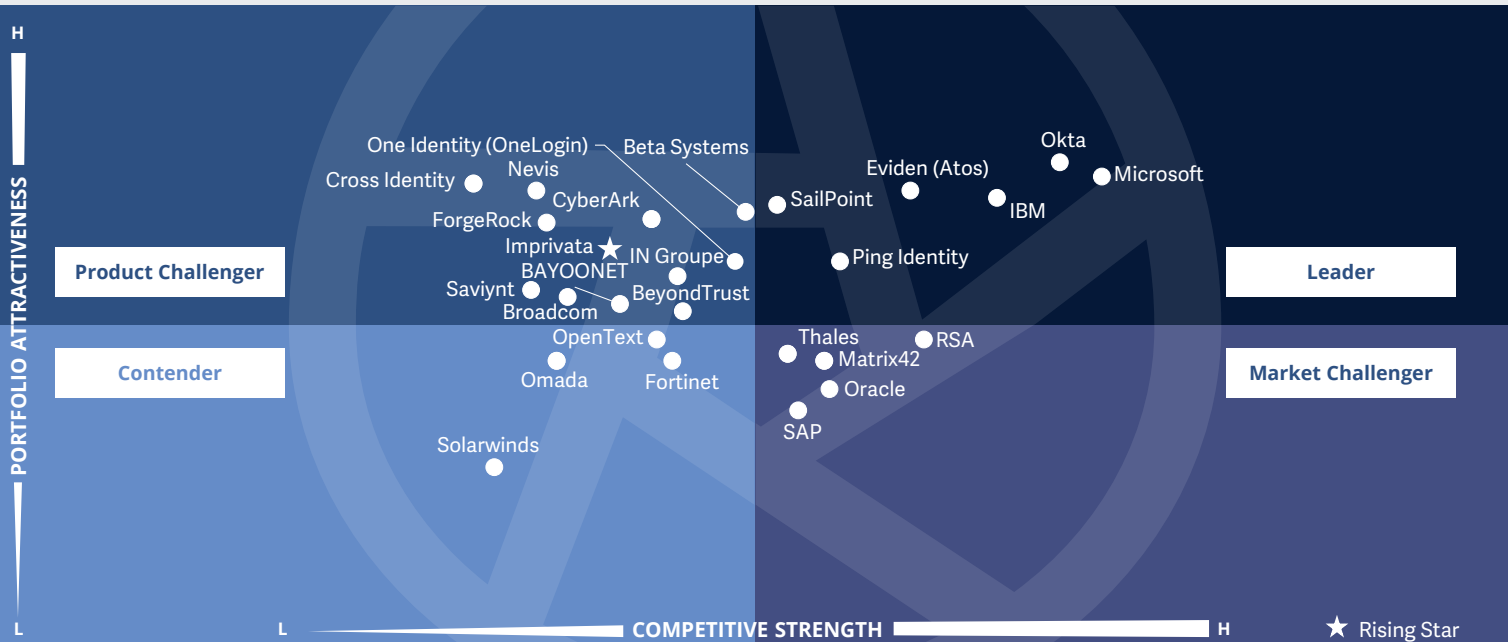


**Compliance and governance professionals** should read this report to understand better how to manage user access to systems and data to ensure regulatory compliance and streamline audits.



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

Germany 2023



This quadrant evaluates the **most relevant** IAM providers in Germany, excluding those that do not offer or operate their own software. The most important topics include **SSO** and **MFA**, with increasing significance placed on **passwordless authentication**.

Frank Heuer





## Identity and Access Management (IAM)

### Definition

IAM vendors and 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 does not include 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 or in the cloud (managed by a customer) or as an as-a-service model or a combination thereof.

IAM solutions are aimed at managing (collecting, recording and administering) user identities and related access rights and also 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 provide additional functionalities related to social media and mobile use to address specific security needs beyond traditional web and contextual rights management. Machine identity management is also included here.

### Eligibility Criteria

1. The solution should be capable of **deployment as an on-premises, cloud, identity-as-a-service (IDaaS) and a managed third-party model**
2. The solution should be capable of **supporting authentication as a combination of single-sign on (SSO), multi-factor authentication (MFA), risk-based and context-based models**
3. The solution should be capable of **supporting role-based access and PAM**
4. The IAM vendor should be able to provide **access management for one or more enterprise needs such as cloud, endpoint,**
5. The solution should be capable of **supporting one or more legacy and new IAM standards,** including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM
6. To support secure access, the portfolio should include one or more of the following – **directory solutions, dashboard or self-service management and lifecycle management (migration, sync and replication) solutions**



## Identity and Access Management (IAM)

### Observations

IAM is currently an important cybersecurity topic and will continue to be in the future. A major reason for the rising demand for IAM solutions is the increasing digitalization in all business areas, which necessitates the protection of not only user identities but also machines and certain company areas such as Industry 4.0. The number of digital identities to manage is constantly increasing, especially with the rise of remote work or home offices, emphasizing the importance of regulating and controlling access among corporate resources. This also results in even higher security and convenience requirements. Therefore, topics such as intuitive interfaces, passwordless authentication, and the use of biometrics and AI are becoming important.

In addition, enterprise applications and data are increasingly migrating to the cloud. This requires IAM solutions that can also secure cloud applications. The IAM market has witnessed a shift from on-premise operation to the cloud, with many providers offering both on-premises and cloud operations (identity as a

service). There is a rise in pure cloud providers, with the U.S. provider Okta being a prominent example. On the provider side, it is worth noting that Imprivata acquired OGiTiX, which qualified as a Rising Star last year. Atos, among other things, outsourced its cybersecurity business under brand Eviden (referred to as Eviden (Atos) in the current study).

Of the 261 providers evaluated in this study, 27 qualified for this quadrant. Of these, six achieved a position as Leader. One provider was identified as a Rising Star.



**Eviden (Atos)** is an innovative provider with a versatile IAM portfolio and offers customers flexibility in choosing their preferred operational solutions.



In the IAM market, **IBM** benefits from its broad range of services and strong market presence. With excellent performance, it also has high integration capabilities.

### Microsoft

**Microsoft** strategically expands its position in the IAM market with the help of proven marketing strategies and implementing technological improvements in products.

### Okta

**Okta's** cloud-based approach simplifies the adoption of IAM solutions, contributing to its continuous growth in the German IAM market.

### Ping Identity

**Ping Identity** offers an innovative and versatile IAM solution, which contributes to its increasing success in Germany.

### SailPoint

**SailPoint** has successfully established itself as one of the leading IAM providers in Germany. The use of AI and simplified IAM management of multicloud environments are some of the key reasons for its success.

### Imprivata

**Imprivata** is a Rising Star among IAM providers in Germany. Its specialization in the growing healthcare industry and flexible usage options contribute to its recognition in the market.





# Data Leakage/Loss Prevention (DLP) and Data Security

## Data Leakage/Loss Prevention (DLP) and Data Security

### Who Should Read This Section

This quadrant is relevant to enterprises in Germany for evaluating DLP and data security solution providers. It further assesses how each provider helps enterprises manage complex security challenges associated with data privacy and data loss.

ISG defines the current positioning of DLP players with a comprehensive overview of the competitive market landscape.

The demand for DLP solutions has significantly increased in recent years due to various factors affecting enterprise data security in Germany. As more enterprises move their data to the cloud, cloud DLP has gained momentum in the market. DLP solutions are integrated with cloud access security broker (CASB) solutions to provide comprehensive data protection across on-premises and cloud environments. This integration enables enterprises to monitor and control data flow between cloud services, providing visibility into shadow IT and unsanctioned cloud applications. DLP solution offering user behavior analytics (UBA) is an essential feature that gives enterprises a

better understanding of how users interact with sensitive data and detects unusual activity that may indicate a data breach. By combining the power of UBA with DLP, enterprises gain a more comprehensive view of their data security posture and proactively identify potential data theft and breaches. API-driven DLP is another crucial component of DLP solutions. API-driven DLP ensures that sensitive data is protected by automating data protection processes across on-premises and cloud-based applications. Enterprises also integrate data privacy and compliance measures into their DLP solutions to ensure they meet regulations such as General Data Protection Regulation (GDPR).



**Cybersecurity professionals** should read this report to understand how DLP solution providers address compliance and security challenges while providing a seamless experience to enterprises.



**Strategy professionals** should read this report to understand the vast potential of solution providers to differentiate themselves by meeting evolving customer demands.

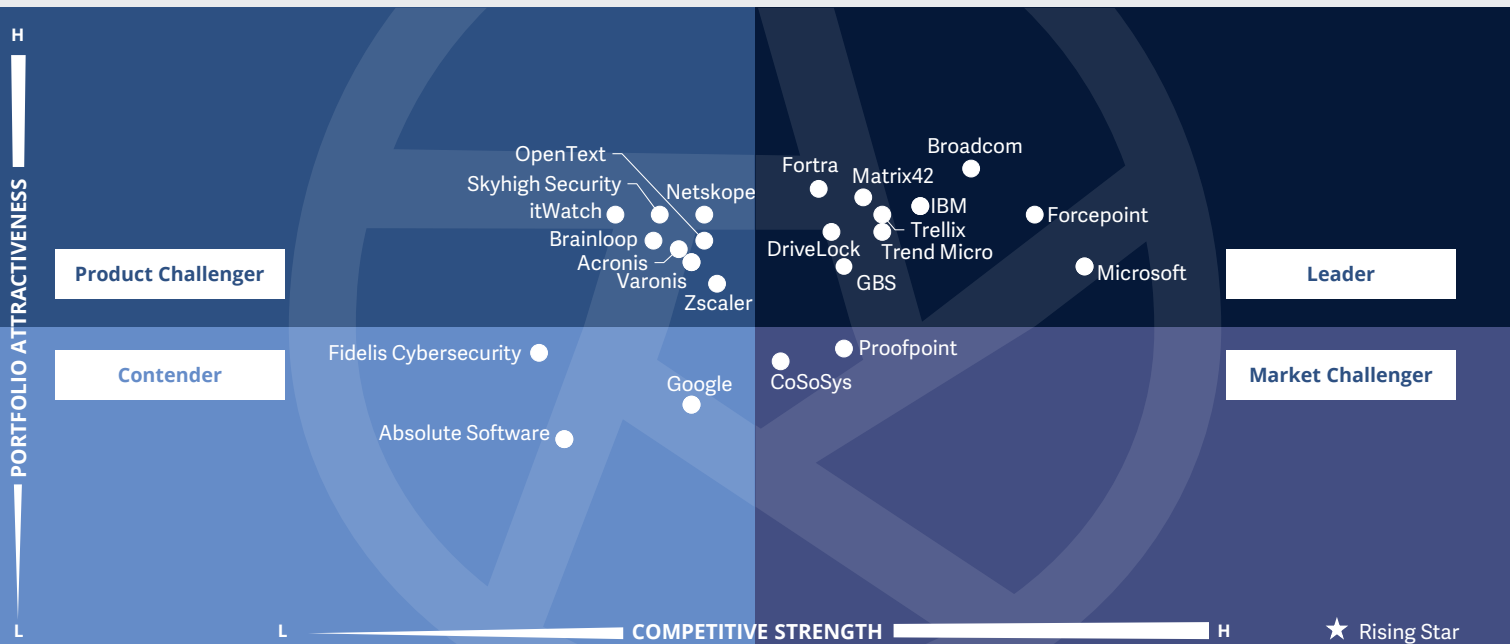


**Data management professionals** should read this report to understand how the providers offer information protection and privacy, information governance, data quality and data lifecycle management.



Cybersecurity – Solutions and Services  
Data Leakage/Loss Prevention (DLP) and Data Security

Germany 2023



This quadrant evaluates the **most relevant** DLP providers in Germany, excluding those that do not offer or operate their own software. The **relevance of data** and **IP protection** contributes to the market's importance.

Frank Heuer



## Data Leakage/Loss Prevention (DLP) and Data Security

### Definition

The DLP vendors and solution providers assessed for this quadrant are characterized by their ability to offer proprietary software and associated services. This quadrant also includes SaaS solutions based on proprietary software. It does not include 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 capable of providing visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers (more than a third of data violations are from an internal source). The number of devices, including mobile devices, used to store data is increasing in companies.

Equipped with an Internet connection, these devices can send and receive data without passing it through a central Internet 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 the security of their data at risk.

### Eligibility Criteria

1. The DLP offering should be based on **proprietary software** and not third-party software
2. The solution should be capable of supporting DLP **across any architecture such as the cloud, network, storage or endpoint**
3. The solution should be capable of **handling sensitive data protection across structured or unstructured** data, text or binary data
4. The solution should be offered with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance and advanced threat detection functionalities
5. The solution should be able to **identify sensitive data, enforce policies**, monitor traffic and improve data compliance



## Data Leakage/Loss Prevention (DLP) and Data Security

### Observations

Data and IP have become increasingly important corporate assets. This heightened significance has contributed to an increased interest in DLP solutions. Protection against undesired data outflows presents a particular challenge, especially with the increasing usage of private end devices in business settings. These devices often elude company administrations' configuration and control and may not be comprehensively monitored for legal reasons. DLP solutions must take these restrictions into account to ensure control without compromising operational security. The introduction of the GDPR has further emphasized the importance of data protection within companies.

The enormous increase in corporate data requires powerful DLP solutions capable of quickly detecting, classifying and safeguarding data from unauthorized actions such as copying or moving. Cloud storage solutions and applications introduce the risk of unintentional data leakage outside the corporate network during processing.

There is also the risk that company data is transferred to private cloud storage services. Social networks and other social media platforms create new communication channels through which data can flow out; email remains a common channel for data transfers. But it is not only unintentional data leakage through the fault of internal actors that can occur, and so companies must also protect themselves against disloyal actions by internal stakeholders.

On the provider side, it is worth mentioning that HelpSystems now operates under the name Fortra in the DLP market.

Of the 261 providers evaluated in this study, 23 qualified for this quadrant. Ten of these achieved a position as Leaders.

### Broadcom

**Broadcom's** DLP solution offers performance and flexibility that benefit both the company as well as its customers. Broadcom supports its customers through centralization and unification.



**DriveLock** scores with its trustworthiness and earns this trust in the market with the principles "Made in Germany" and "No Backdoor". DriveLock also stands out for its consistent use of ML algorithms.

### Forcepoint

**Forcepoint** helps users quickly address and alleviate their data loss backup challenges with its range of advanced solutions.

### Fortra

**Fortra** fully supports its customers with proactive data classification, advanced analytics and reporting services, and easy integration.

### GBS

**GBS** not only intensifies its activities to establish a stronger presence in the German market but also contributes to its success with sophisticated technology and the dual control principle.



**IBM** combines a strong market presence with a future-oriented DLP solution and scores with its competent combination of DLP with AI. The IBM solution also covers a universal range of applications and offers flexible usage options.

### Matrix42

**Matrix42** offers an efficient DLP solution with a broad range of functions. It has high acceptance among end users with its user-friendly low impairments, thus successfully promoting its solution.

### Microsoft

**Microsoft** continues to expand its position in the German market for DLP solutions. Integration and bundling, along with convincing performance features, contribute to Microsoft's increasing establishment in this region.



## Data Leakage/Loss Prevention (DLP) and Data Security

### Trellix

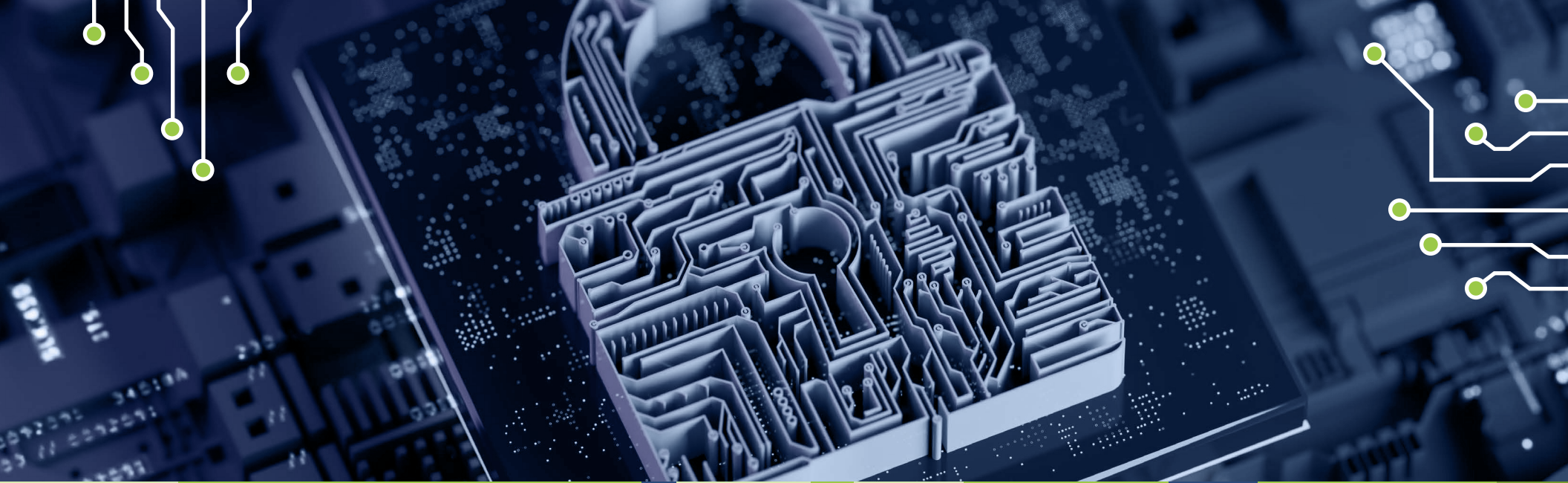
**Trellix** benefits from a dense distribution network in Germany with the acquisition of McAfee. Its strong local and international presence enables Trellix to offer versatile delivery options.

### Trend Micro

**Trend Micro** owes its success in the German market for data loss and data leakage prevention products, in particular, to the integrability, ease of deployment and use of its DLP solution.







# Extended Detection and Response (XDR)

## Extended Detection and Response (XDR)

### Who Should Read This Section

This quadrant is relevant to enterprises in Germany across industries for evaluating XDR solution providers. It further assesses how each provider helps enterprises increase visibility across all telemetry sources and obtain a unified view of threat detection and response.

ISG defines the current positioning of XDR players with a comprehensive overview of the competitive market landscape.

XDR is an advanced cybersecurity solution that integrates multiple security technologies, including endpoint detection and response (EDR), network detection and response (NDR) and security information and event management (SIEM) to provide more comprehensive threat detection and response capabilities. For enterprises with advanced security capabilities, XDR can provide compliance with multiple security concepts, including secure access service edge (SASE) and zero trust, by collecting and analyzing data from various security sources, including endpoints, networks and cloud environments. XDR uses advanced analytics and ML to identify

and prioritize threats and provides automated response actions to mitigate them. By integrating XDR with SSE, enterprises can gain end-to-end visibility and control across their entire security environment, including remote workers, branch offices and cloud applications. This provides a comprehensive threat detection and response approach and simplified compliance and reporting. Since XDR solutions are complex, it requires significant expertise to deploy, configure and maintain. XDR must incorporate leading-edge AI and ML innovation to hunt for threats, anticipate attacks and help enterprises respond to advanced threats in the rapidly evolving threat landscape.



**Cybersecurity professionals** should read this report to gain insights into XDR solutions that aid enterprises in enhancing visibility across endpoints to enable unified threat detection and response.



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

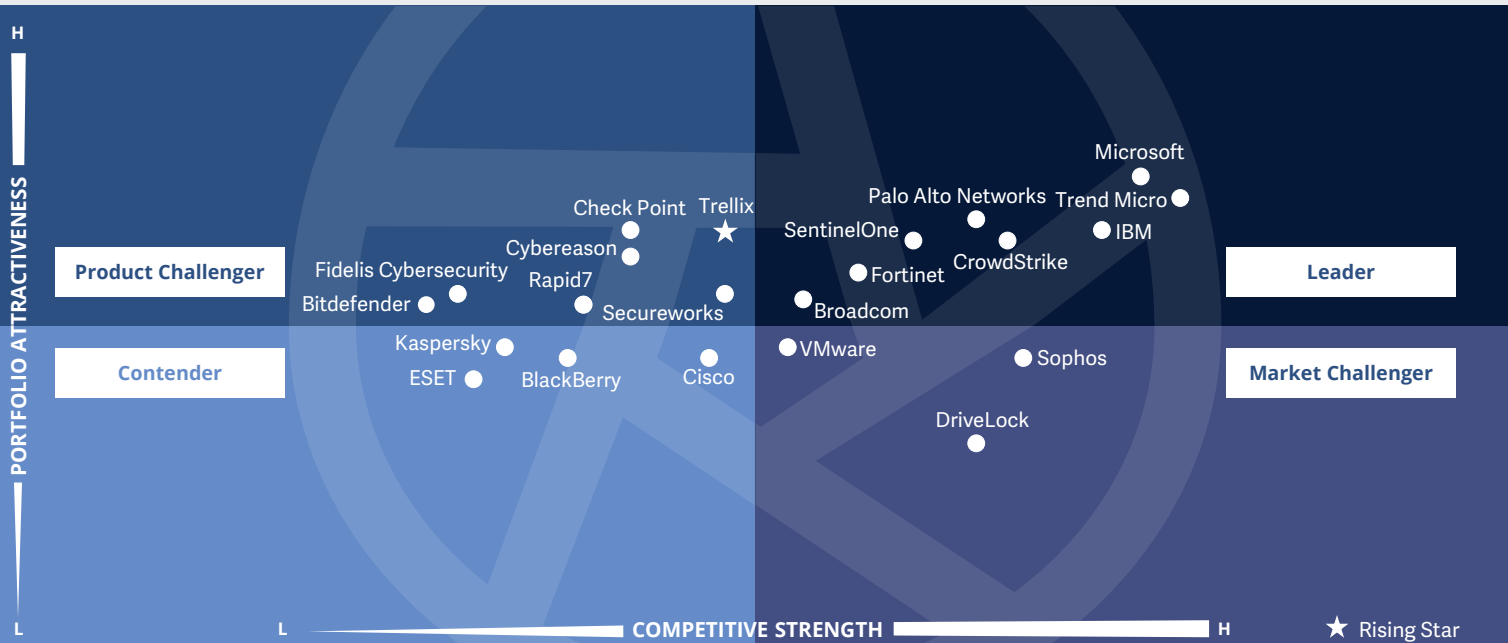


**Strategy professionals** should read this report to understand XDR providers' capabilities to help enterprises effectively manage security risks and make informed decisions about their security strategy.



Cybersecurity – Solutions and Services  
Extended Detection and Response (XDR)

Germany 2023



The XDR solution providers evaluated in this quadrant excel at providing a platform that **integrates** and **correlates** data and alerts from **multiple sources** for **threat defense**, detection and response.

Frank Heuer



## Extended Detection and Response (XDR)

### 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 from weak individual signals to enable accurate detections. XDR solutions consolidate and integrate multiple products and are designed to provide comprehensive workspace security, network security or workload security. Typically, XDR solutions are aimed at vastly improving visibility and improving context to the identified threat across the enterprise. Therefore, these solutions include specific characteristics, including telemetry and contextual data analysis, detection and response. XDR solutions comprise multiple products and solutions integrated into a single pane of glass to view, detect and respond with sophisticated capabilities. High automation maturity and contextual analysis offer unique

response capabilities tailored to the affected system, and prioritize alerts based on severity against known reference frameworks. **Pure service providers that do not offer an XDR solution based on proprietary software are not included here.** XDR solutions aim to reduce product sprawl, alert fatigue, integration challenges and operational expense, and are particularly suitable for security operations teams that have difficulty in managing a best-of-breed solutions portfolio or getting value from a security information and event management (SIEM) or security, orchestration, automation and response (SOAR) solution.

### Eligibility Criteria

1. The XDR offering should be based on **proprietary software** and not on third-party software
2. An XDR solution needs to have two primary components: **XDR front end and XDR back end**
3. The front end should have **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. The solution provides **comprehensive and total coverage and visibility of all endpoints** in a network
5. The solution demonstrates **effectiveness in blocking sophisticated threats such as advanced persistent threats, ransomware** and malware
6. The solution leverages **threat intelligence**, and analyzes and offers **real-time insights on threats** emanating across endpoints
7. The solution should include **automated response features**



## Extended Detection and Response (XDR)

### Observations

XDR solutions have gained prominence and traction over the past two years as organizations seek to better understand and contextualize (correlate) the information gathered from their diverse security tools deployed in their IT infrastructure. The market consists of open and native XDR tools, and this quadrant includes native XDR providers that are preferred by enterprises for their ability to readily offer an integrated suite of products.

Service providers have built their XDR capabilities on top of their existing presence in the endpoint detection and response (EDR) market, with some benefiting from their networking and cloud portfolios. Native XDR offers immediate and advantageous integration capabilities with existing native or proprietary products, meeting enterprises' preference for single-provider platforms that streamline purposes. XDR solutions are highly automated and correlate logs, alerts and notifications from internal and external sources, resulting in improved threat intelligence.

Leading products in the market include behavioral and contextual analytics modules to enhance the understanding of attack vectors and the attack chain. These products have gained traction over the past year. Most leading providers also offer open integration with other EDR and NDR products to facilitate integration. Strong XDR products feature clear dashboards and a unified console.

Of the 261 providers evaluated in this study, 22 qualified for this quadrant. Of these, eight achieved a position as Leader. One provider was identified as a Rising Star.

### Broadcom

**Broadcom** provides real-time visibility and threat management across on-premises, cloud-based or hybrid infrastructures through a unified console.

### CrowdStrike

**CrowdStrike's** cloud-native, AI-powered platform detects and analyzes security threats in real time based on behavioral patterns.

### Fortinet

**Fortinet** provides a robust foundation for XDR with a common data structure and unified visibility. The solution enables automated analytics, incident investigation and predefined threat responses.

### IBM

**IBM's** acquisition of ReaQta has strengthened its XDR portfolio and market presence. The company benefits from its comprehensive security solutions and the QRadar suite and can thus offer a strong XDR solution.

### Microsoft

**Microsoft** has gained significant market traction due to the ease of use and advanced features of its endpoint solution.

### Palo Alto Networks

**Palo Alto Networks** has developed a powerful XDR solution based on its portfolio and AI, providing broad coverage and enabling faster prioritization and investigations.

### SentinelOne

**SentinelOne's** has acquired Attivo Networks to leverage the capabilities of the Singularity XDR platform, enabling effective threat mitigation across endpoints, cloud workloads, IoT devices, mobile devices and data.

### Trend Micro

**Trend Micro** enables users with security and investigation capabilities, providing threat detection, response and analysis through a single agent.

### Trellix

**Trellix (Rising Star)** leverages a wide range of capabilities and real-time threat data to monitor and combat cyberattacks. The company uses AI-driven analytics to quickly prioritize and mitigate threats.





# Security Service Edge (SSE)

## Security Service Edge (SSE)

### Who Should Read This Section

This report is relevant to enterprises across regions 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 (SWG). Moreover, it evaluates how each provider helps enterprises ensure security across hybrid and multicloud ecosystems.

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

With increasing cloud adoption, businesses need a robust security solution to protect digital assets and grant secured access to a remote workforce. These solutions focus on user-centricity and deliver security to end users through the cloud rather than allowing users to access enterprise applications and databases over dedicated networks centrally. As enterprises consolidate security and remote access services under a single framework,

SSE offerings provide a unified management console for real-time visibility of security events across the entire infrastructure. This unification helps businesses maintain compliance with various security regulations and standards by providing a single control point for security policies and configurations.

SSE solutions improve the efficiency of enterprises' security operations and are gaining popularity as a trial run before implementing secure access service edge (SASE) solutions. SSE providers must offer adequate technical support and robust integration between multiple security components. Enterprises increasingly embrace security features specific to web apps and APIs and automated advanced analytics features such as user entity behavior analytics (UEBA).



**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** can benefit from this report because it outlines how SSE providers assist enterprises in adopting an enterprise-wide, zero trust framework to improve their security posture.

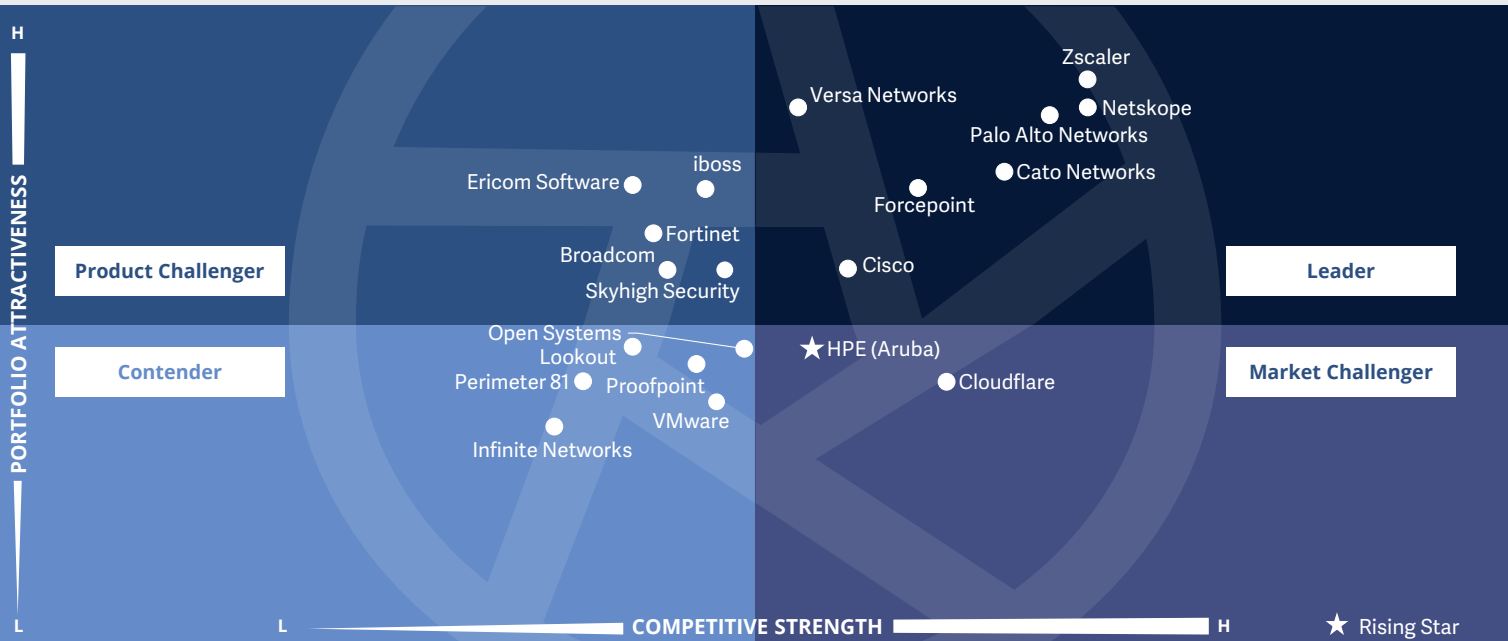


**Strategy professionals** will gain insights into SSE providers' critical capabilities and focus on user-centricity, delivering security to end users at the edge or devices through the cloud.



**Cybersecurity – Solutions and Services**  
**Security Service Edge (SSE)**

Global 2023



The SSE solution providers evaluated in this quadrant excel at enabling **secure access** to cloud services, SaaS applications, web services and private applications.

*Gowtham Kumar Sampath*





## Security Service Edge (SSE)

### Definition

The SSE solution providers assessed for this quadrant offer cloud-centric solutions that combine proprietary software, and/or hardware and associated services, enabling secure access to cloud services, SaaS applications, 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 loss/leakage prevention (DLP), browser isolation and next-generation firewall (NGFW) to offer secure access to applications on the cloud and on-premises.

Vendors showcase experience in satisfying local, regional and domestic laws (such as for data sovereignty) for global clients.

The network components of secure access secure edge (SASE), such as SD-WAN or micro-segmentation, are not included in this quadrant but are covered in the “Network - Software Defined Solutions and Services” study.

SSE solutions strongly focus on usercentricity, delivering security to end users at the edge or devices through the cloud — rather than allowing users to centrally access enterprise applications and databases — over dedicated networks. ZTNA creates exclusive connectivity between a user and an application, using context-based behavioral analysis to control access. CASB offers visibility, enforces security policies and compliance, and allows control of 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, and assesses user experience with advanced automation.

### Eligibility Criteria

1. The SSE should be offered as an **integrated solution** and must have these essential components: **zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS)**
2. The above components must be **predominantly based on proprietary software**, they may **partially rely on partner solutions but cannot completely rely on third-party software**
3. Vendors should have **globally located PoPs** to deliver these solutions
4. The solution should be capable of **delivering SSE to both cloud and on-premises** environments (including hybrid environments)
5. The solution should exhibit **contextual and behavioral evaluations and analysis (user entity and behavior analytics/UEBA)** to detect and prevent malicious or suspicious intent
6. The solution should be offered with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. The solution should be **fully and globally available**



## Security Service Edge (SSE)

### Observations

Security Service Edge (SSE) is a new quadrant being analyzed on a global scale as this topic is in its early stages of maturity and adoption by enterprises. SSE includes solutions that enable secure cloud access, facilitate remote work, secure edge computing, and support digital transformation.

The rise of remote and hybrid employees, and the transition to the cloud, have created a need for SSE solutions. The use of VPNs increases the risk of security breaches due to the lack of unpatched vulnerabilities. For this reason, SSE is emerging as a viable option for secure access to corporate data. However, enterprises face budget constraints and hesitate to invest in premium solutions such as AWS Direct Connect or Microsoft ExpressRoute in terms of return on investment.

SSE providers enable a unified view of the system by combining operational and device data to provide enhanced visibility across the enterprise with automated alerts, remote monitoring and management, and security

monitoring. They market offers open and native SSE products, but enterprises prefer native or converged SSE solutions to take advantage of an integrated product suite and improved interoperability with existing security tools. Service providers are continually investing in innovation to address emerging threats. In addition to secure cloud access, SSE helps enterprises gain comprehensive visibility into shadow IT, including unauthorized applications, devices and Internet usage.

Of the 261 providers evaluated in this study, 20 qualified for this quadrant. Of these, seven achieved a position as Leader. One provider was identified as a Rising Star.

### Cato Networks

**Cato Networks** offers a native, converged solution with strong SASE capabilities. The company has positioned its SSE 360 as the core of its portfolio, catering to the growing interest in adopting SSE to realize SASE.

### Cisco

**Cisco's Umbrella** is a converged solution based on an in-house AI engine and playbooks incorporating DLP, XDR and threat hunting. This comprehensive solution improves visibility, efficiency, threat investigation and remediation.

### Forcepoint

**Forcepoint** has expanded its SSE architecture and roadmap through strategic acquisitions, including BitGlass and Cyberinc. These acquisitions have strengthened its data-driven SSE platform.

### Netskope

**Netskope experienced significant growth** in SSE significantly in 2022, building on its SASE capabilities. The company has added real-time controls to its offering and placed a greater focus on improving usability and performance.

### Palo Alto Networks

**Palo Alto Networks** grew significantly with SSE last year. With the strategy to address ZTNA 2.0, the company targets the need for securing hybrid enterprises and remote workforces with out-of-the-box configurations.

### Versa Networks

**Versa Networks** offers several products designed to address the challenges of zero trust and remote work. Its SSE solution uses AI to monitor the security posture of users and devices to improve the accuracy of threat detection.



## Security Service Edge (SSE)



**Zscaler** continues to remain the market leader in SASE with Zero Trust Exchange solution. The solution aims to address business risk and help enterprises with digital transformation.



**Hewlett Packard Enterprise**

**HPE (Aruba) (Rising Star)** has entered the SSE market and gained momentum with the acquisition of Axis Security. Combined with the partnership with Lookout, HPE's SSE capabilities help customers to improve shadow IT monitoring.





# Technical Security Services

## Technical Security Services

### Who Should Read This Section

This quadrant report is relevant to enterprises across industries in Germany for evaluating technical security service (TSS) providers specializing in implementing and integrating security products or solutions. The report focuses on providers not limited to their proprietary products but can integrate other vendors' solutions.

In this quadrant, ISG defines the current market positioning of TSS providers and highlights how each provider addresses critical security challenges.

The growing complexity of security threats and the need for specialized expertise required to address sophisticated threats contribute to the demand for technical expertise. With the rise of OT security, there is a greater emphasis on collaboration between IT and OT teams to ensure that security measures are integrated across all systems and devices. Regular vulnerability assessments and penetration testing can help identify and address potential security risks, while deploying cloud-based security solutions can help neutralize

cyberattacks on connected OT devices. Enterprises seek help implementing security architecture frameworks that offer standardized playbooks and roadmaps to help clients transform their existing security environment using best-of-breed tools and security design methodologies. This helps simplify security management, reduce costs and improve the effectiveness of security measures.

Technology consolidation is also driving the demand for technical expertise and implementation engineering as enterprises need to simplify security management, reduce costs and improve the effectiveness of security measures. Implementation of identity and privilege access management solutions is also on the rise.



**Technology professionals** should read this report to understand providers' integration capabilities that help reduce threat impact using advanced technologies to transform legacy systems.



**Business professionals** should read this report to balance data security, CX and privacy amidst digital transformation at the forefront of businesses today.

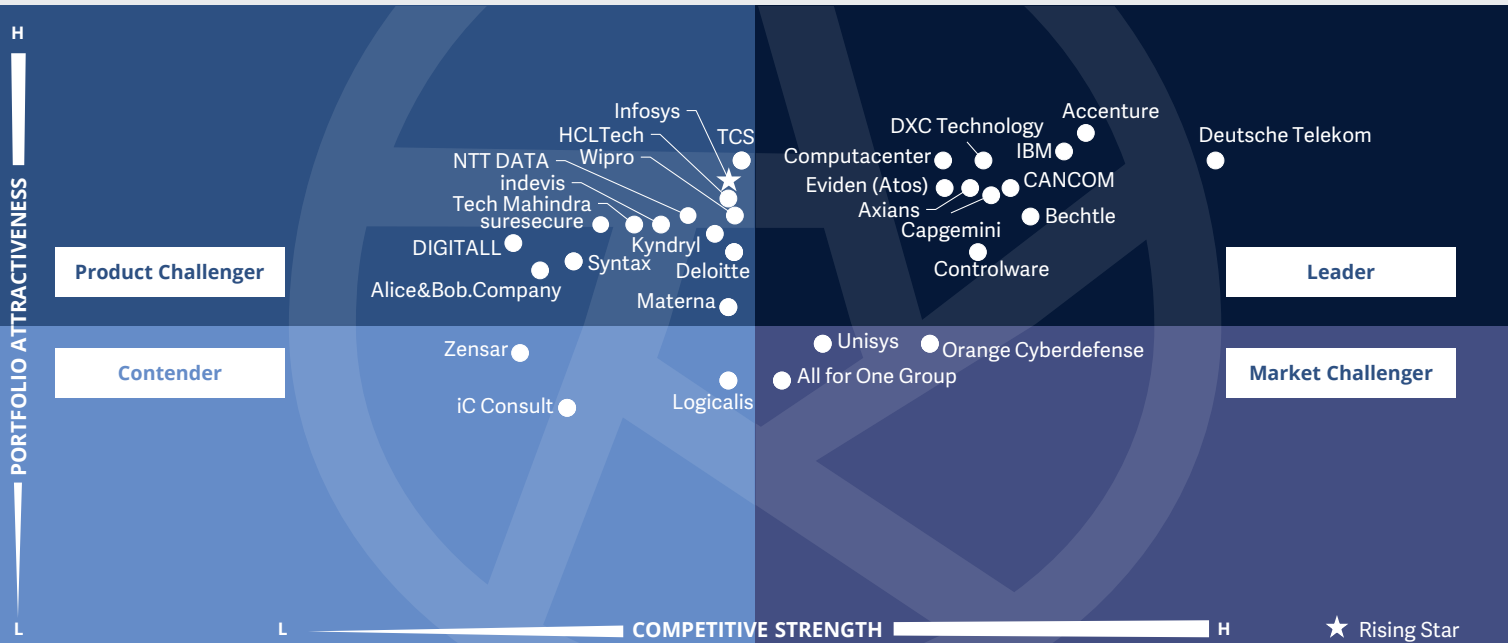


**Security and data professionals** should read this report to gain insights into how providers comply with security and data protection laws to stay updated with market trends.



Cybersecurity – Solutions and Services  
 Technical Security Services

Germany 2023



This quadrant evaluates the **most relevant** service providers for technical security services, excluding providers whose services only relate to their own products. External service providers are becoming **increasingly important for** keeping IT security systems up to date.

Frank Heuer



## Technical Security Services

### Definition

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

TSS providers offer standardized playbooks and roadmaps 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 the complete or individual transformation of an existing security architecture with relevant products 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. The providers also leverage sophisticated solutions that enable comprehensive vulnerability scanning across applications, networks, endpoints and individual users to uncover weaknesses and mitigate external and internal threats.

TSS providers invest in establishing partnerships across security technology, cloud, data and network domains to gain specialized accreditations and expand the scope of their work and portfolios. This quadrant also encompasses classic managed security services, i.e. those provided without a security operations center (SOC).

**This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.**

### Eligibility Criteria

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



## Technical Security Services

### Observations

The increasing frequency of sophisticated, complex and constantly evolving cyberattacks poses a challenge for companies in Germany. The lack of cybersecurity experts further complicates this situation, leading companies to increasingly rely on external service providers.

Midsize companies, particularly, continue to face a pressing need to catch up as they often struggle with a lack of IT specialists, excessive demand and resource constraints. However, the increasing complexity of security threats and stricter legal regulations are prompting these companies to take more frequent actions, often requiring external support. In this context, midsize companies often appreciate the local presence of service providers within short distances that provide uncomplicated, fast support.

IT security projects are often demanding and multifaceted. Service providers that offer comprehensive technical security services from a single source, therefore, have a competitive advantage. Collaborating with

renowned technology providers and employing certified professionals further strengthen their value proposition.

In addition, to be successful in the demanding key account market, suppliers must demonstrate significant experience and large international teams.

Service providers with a balanced customer base of large and midsize companies reap benefits both from the extensive budgets of large customers and capitalize on the above-average growth in demand from midsize companies.

In addition, service providers that offer end-to-end security services and associated IT solutions from a single source have an advantage.

Of the 261 providers evaluated in this study, 31 qualified for this quadrant. Of these, 11 achieved a position as Leader. One provider was identified as a Rising Star.



**Accenture's** Security Automation Factory supports the transformation of process- and resource-intensive tasks through RPA. Accenture covers a very extensive range of topics and services.



**Axians** maintains partnerships with numerous renowned cybersecurity technology providers. Axians' technical IT security services cater to customers' diverse needs.



**Bechtel** has a strong local presence in Germany, with numerous locations. It stands out as a high-profile provider of technical security services for the dynamically growing market segment of midsize companies.

### CANCOM

**CANCOM's** technical security services cover a comprehensive range of topics and services, with a strong focus on midsize companies.



**Capgemini** is a security services provider that demonstrates thought leadership and uses advanced technologies such as security automation and AI as part of its clients' cybersecurity projects.



**Computacenter** offers a wide range of technical security services, partnering with numerous large IT security manufacturers as well as many smaller and emerging providers.





## Technical Security Services

### Controlware

With its German origins, **Controlware** is particularly well positioned in the upper midmarket segment, which particularly values service providers with local roots. Controlware's modular offering is structured in line with client requirements.



**Deutsche Telekom** offers seamless technical security services that cover a complete range of topics. Its cybersecurity team has many experts, and with the motto of Security made in Germany, Deutsche Telekom can score points, especially for midsize customers.

### DXC Technology

**DXC Technology's** portfolio includes integrated solutions in cybersecurity and connected IT technology, backed by its global presence and resources. Despite its extensive manpower, DXC Technology continues to develop automation and blueprints.



**Eviden (Atos)** is familiar with the requirements and legal regulations related to security projects and supports its customers in complying with these requirements. It takes a holistic approach to cybersecurity that also emphasizes business relevance.



**IBM** is an experienced and successful cybersecurity technology provider and possesses a deep understanding of IT security solutions. In the German market, the company offers one of the broadest portfolios of IT security services.



A comprehensive, innovative portfolio and strong growth make **Infosys** the Rising Star for Technical security services in Germany. The Cyber Security Center of Excellence also contributes to innovation.





“Together with its extensive partner network, Computacenter offers optimal security solutions for its customers based on experience and competence.”

Frank Heuer

# Computacenter

## Overview

Computacenter is a leading information technology service provider based in Hatfield, U.K. In 2022, it generated revenue of around £6.5 billion with around 20,000 employees. Computacenter Germany has its headquarters in Kerpen and employs around 7,000 people. Computacenter’s technical security services include cyber defense, cloud security, infrastructure security, workplace security, IAM, IT governance, risk and compliance, and industrial security.

## Strengths

**Strong partner ecosystem:** Computacenter has a very extensive partner ecosystem and maintains relationships with numerous large IT security vendors and emerging ones. This extensive ecosystem provides deep insight into vendors’ product portfolios, enabling Computacenter to identify the best-suited vendors for each customer and implement individually tailored solutions.

**Know-how and experience:** Computacenter combines its strong relationships with product vendors with in-depth technical knowledge gained through years of experience in large transformation projects.

## Confirmed quality of collaboration:

Computacenter’s performance is confirmed by technology partners and is attested by numerous awards, including those from Check Point, Cisco, CyberArk, Fortinet, Palo Alto Networks, Proofpoint and Trend Micro.

**Commitment to sustainability:** In recent years, Computacenter’s investment in sustainability and the development of its corporate values have given customers additional reasons to work with the company.

## Caution

Consideration may be given to the selective expansion of Computacenter’s portfolio. Although Computacenter offers numerous technical security services for a wide range of technologies, predictive maintenance and support for developers and administrators have not yet been included.





# Strategic Security Services

### Who Should Read This Section

This quadrant is relevant to enterprises in Germany across industries for evaluating service providers specializing in strategic security services (SSS). These providers can assess security maturity and risk posture and define tailored cybersecurity strategies for enterprises.

In this quadrant, ISG defines the current positioning of SSS providers, offering a comprehensive overview of the competitive market landscape.

Enterprises are increasingly looking for ways to reduce cyber risks with security transformation efforts. They must secure their digital assets and business-critical data, reduce their exposure to threats and be prepared to address security issues in the ever-changing threat landscape. Security consulting providers are helping enterprises with comprehensive risk assessments through complex security testing exercises such as red and purple teaming to identify security gaps. Along with assisting enterprises with robust security strategies and roadmaps, providers also help

them develop a security culture. They provide security awareness and training services to help enterprise board members, key business executives and employees develop cyber literacy and establish best practices to respond better to actual threats and cyberattacks. Enterprises improve their security function by working with security consulting providers and strengthening CISO's role. Enterprises must also integrate regulatory and compliance mandates within their security programs and require governance models to improve and sustain their cyber risk posture. They continuously use the insights gained from monitoring and reporting on critical KPIs, such as the number of security incidents detected and resolved to equip themselves to prioritize the proper controls, policies, technologies and procedures and identify compliance risks.



**Cybersecurity professionals** should read this report to gain a broader outlook on security trends. It highlights providers' capabilities in helping enterprises devise robust security strategies.



**Technology professionals** should read this report to gain insights into the emerging trends in the security landscape and providers' abilities to develop tailored security platforms.

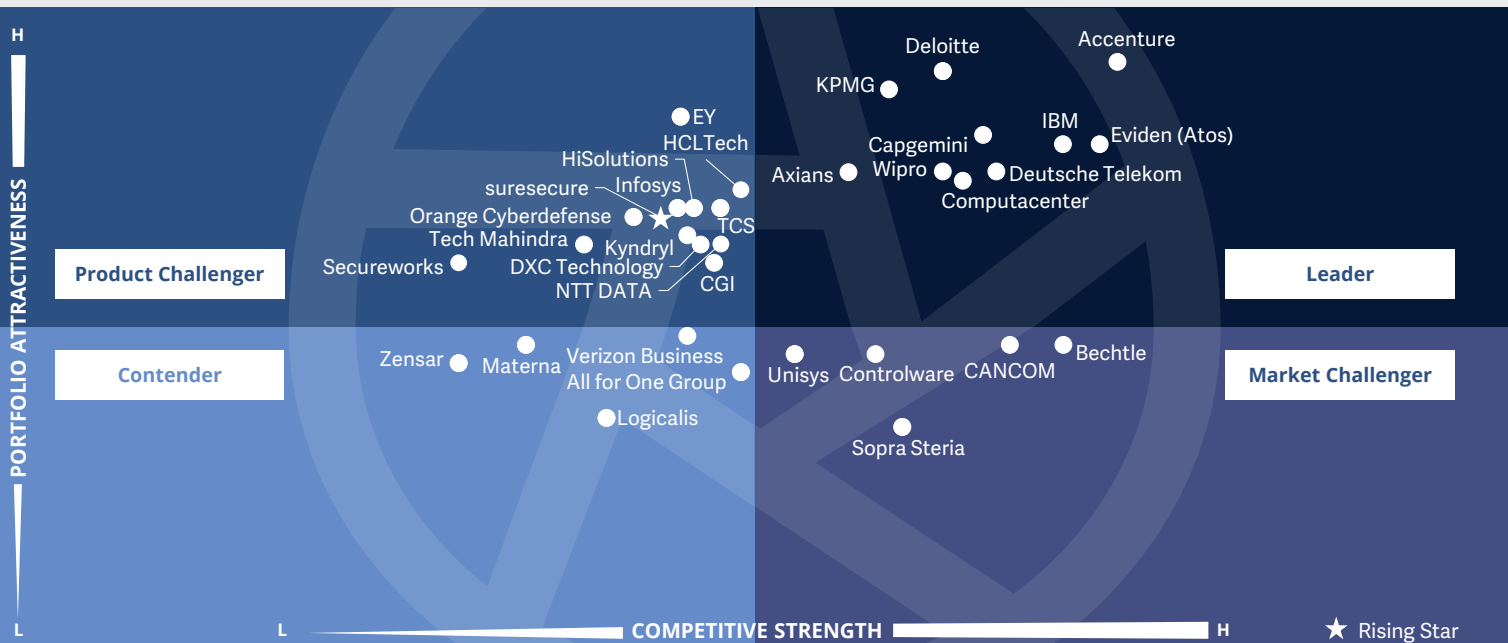


**Strategy professionals** should read this report to understand service providers' relative positioning and capabilities in supporting the decision-making process on partnerships and cost-reduction initiatives.



Cybersecurity – Solutions and Services  
Strategic Security Services

Germany 2023



This quadrant evaluates the **most relevant** cybersecurity consultants in Germany whose services are not limited to their own products. Due to **increasing** cyberthreats, companies are increasingly looking for **external support** and guidance.

Frank Heuer



## Strategic Security Services

### Definition

The Strategic Security Services (SSS) providers assessed for this quadrant offer consulting for IT and OT security. The services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategies for enterprises (tailored to specific requirements).

SSS providers should employ security consultants that have 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 vCSIO (virtual chief security information officer) services. Given the increased focus on cyber resiliency, providers offering SSS should be able to formulate business continuity roadmaps 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, especially OT security and SASE.

### Eligibility Criteria

1. Service providers should demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, architecture consulting and risk advisory**
2. Service providers should **offer at least one of the above strategic security services in the respective country**
3. The ability to **execute security consulting services using frameworks** will be an advantage
4. **No exclusive focus on proprietary products or solutions**



## Strategic Security Services

### Observations

Cyber threats continue to grow, currently fueled by the Ukraine war. This, combined with resource limitations, has intensified the need for cybersecurity guidance. In addition, new and technically sophisticated threats are emerging.

Companies face significant challenges in safeguarding their IT systems against the growing intensity and sophistication of cyberattacks. This predicament no longer affects just large companies and public authorities, small and midsize companies are increasingly affected as well. Additionally, the shortage of IT specialists continues to make this situation more difficult, posing a greater challenge for midsize companies in particular.

These factors mean that companies increasingly need external support, often starting with consulting.

Large companies continue to be among the most important customers for Strategic Security Services, and now midsize companies are also recognizing their services and value. Service providers with a balanced customer portfolio that includes both large and

medium-sized businesses benefit from substantial budgets of larger clients, as well as the growing demand from medium-sized companies.

Furthermore, service providers that can offer their customers not only security consulting but also implementation and operation so that the strategy can be seamlessly put into practice have an advantage, as do providers that can offer not only security consulting but also associated IT solutions from a single source.

First moving consultants are gearing up to defend clients against quantum-based cyberattacks.

Of the 261 providers evaluated in this study, 33 qualified for this quadrant. Of these, 10 achieved a position as Leader. One provider was identified as a Rising Star.

We are aware of PwC's market presence, but have decided not to consider the company in the study this year due to insufficient information.

### accenture

**Accenture's** consultants possess great competence and experience, granting them access to board-level discussions. The service portfolio is extensive and is being systematically developed.

### axians

**Axians** excels in the German cybersecurity consulting market with pragmatic and targeted solutions, especially for midsize companies. Axians is also dynamically developing its portfolio.

### Capgemini

**Capgemini** offers a wide range of cybersecurity consulting services with a focus on ongoing expansion. The company distinguishes itself with its experienced team of consultants who not only understands the theory but also excels in practical implementation.

### Computacenter

**Computacenter** positions itself as a strategic partner, approaching security with a holistic perspective and an understanding of customers' infrastructure and business requirements. The company's consulting portfolio covers a broad range of security topics.

### Deloitte

**Deloitte**, with its strong global presence, possesses a deep understanding of the specific business needs of its clients in Germany when it comes to security consulting.

### T

**Deutsche Telekom** provides customers with end-to-end services from a single source and also has expertise in challenging environments backed by years of certified cybersecurity competence.



## Strategic Security Services



**Eviden (Atos)** adopts a holistic approach to cybersecurity consulting, establishing trust with its (potential) customers through numerous certifications as part of its security consulting services.



**IBM's** cybersecurity consulting portfolio is comprehensive, integrated and innovative. The company uses its deep technical insights gained from its experience as a security product provider.



**KPMG** skillfully combines business and technical understanding in its cybersecurity consulting, while its consultants possess a high level of strategic competence in the security consulting space.



**Wipro** offers an extensive cybersecurity consulting portfolio and has great technical expertise that contributes to its excellence in this space.



With its dynamic development, **suresecure** is profiling itself as a **Rising Star** for strategic security services in Germany. The company's consulting services cover a wide range of areas, especially for a young service provider.







“Computacenter combines a comprehensive range of consulting services with a holistic approach to benefit its customers.”

Frank Heuer

# Computacenter

## Overview

Computacenter is a leading information technology service provider based in Hatfield, U.K. In 2022, it generated revenue of around £6.5 billion with around 20,000 employees. Computacenter Germany has its headquarters in Kerpen and employs around 7,000 people. Computacenter’s strategic security services include cyber defense, cloud security, infrastructure security, workplace security, IAM, IT governance, risk and compliance, and industrial security.

## Strengths

### End-to-end services are offered:

Computacenter is not only a high-performance cybersecurity consultant but also very competent in the technical implementation of IT security projects. The company also offers managed security services.

### Holistic approach to consulting:

Computacenter positions itself as a strategic partner with a holistic approach to security and an understanding of customers’ infrastructure and business requirements. Cybersecurity is an integral part of most projects and services Computacenter offers, and it can be purchased as a standalone service.

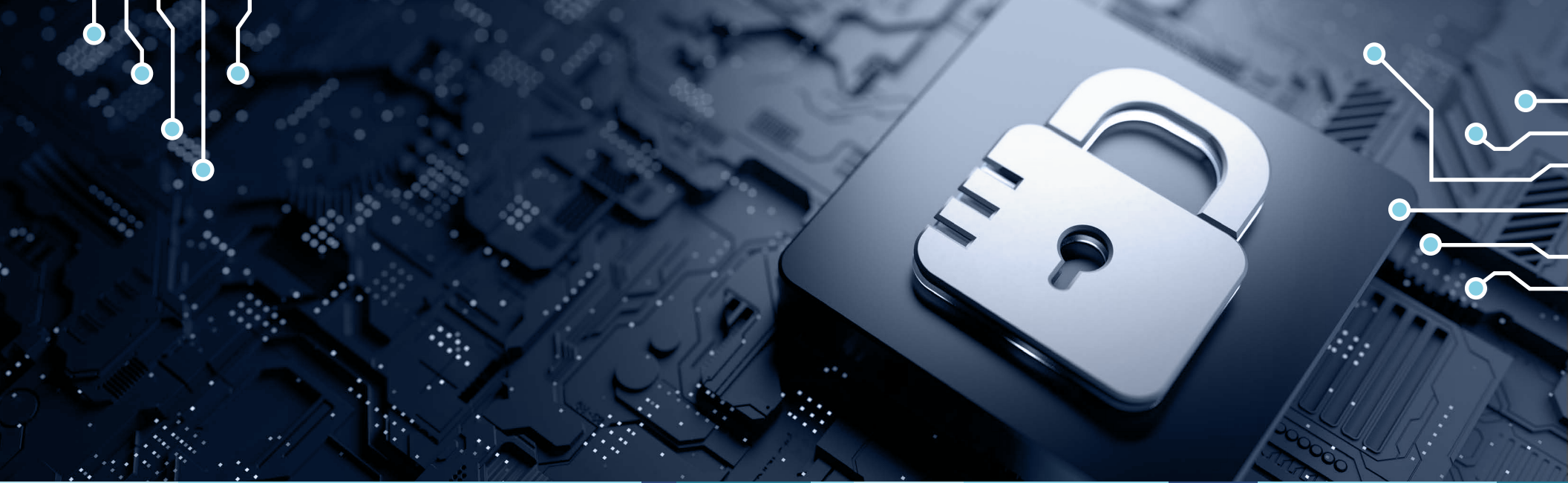
## Extensive consulting portfolio:

Computacenter offers a wide range of consulting services covering diverse security topics. The provider addressed OT security concerns at an early stage. Particularly noteworthy is Computacenter’s detailed knowledge of the offerings of the security product providers. Computacenter also has a comprehensive roadmap for the further development of its cybersecurity consulting portfolio and is constantly updating its portfolio, ensuring alignment with the changing security landscape and customer requirements.

## Caution

It is advisable to consider expanding the international presence. Though Computacenter operates in over 20 countries, it is worth considering expansion to attract internationally active customers and compete better with leading global competitors. Considering additional countries is recommended.





# Managed Security Services - SOC

## Managed Security Services - SOC

### Who Should Read This Section

This quadrant is relevant to enterprises across industries in Germany for evaluating service providers specializing in managed security services (MSS) and thus helping enterprises combat security threats. It also provides insights into how each provider addresses critical market challenges.

In this quadrant, ISG defines the current positioning of MSS providers, offering a comprehensive overview of the competitive market landscape.

Businesses have become more vulnerable to cyber-attacks with the shift to remote work and the increased use of cloud-based applications and services. Managed detection and response (MDR) services provide a critical layer of protection against these threats, ensuring that remote workers and cloud-based assets are secure. Enterprises need continuous monitoring, advanced threat detection capabilities, incident response and remediation support to help prevent data breaches and ensure business continuity.

The importance of compliance regulations and data privacy laws drives the demand for MDR services. Ransomware detection and readiness are still high on the agenda as enterprises seek to protect their valuable data and systems from being compromised by malicious actors. It allows enterprises to prepare for the ransomware threat proactively. Advanced analytics, AI, ML and deep learning techniques for behavior-based threat analysis are gaining interest. Threat intelligence feeds allow proactive risk identification, monitoring and accurate detection and threat intelligence as a service is picking up. With the increasing adoption of zero trust and SASE and the scarcity of qualified resources and expertise, the need for managed services is increasing.



**Cybersecurity professionals** should read this report to understand the emerging trends and immediate threats to aid their strategic decision-making, enhance productivity and reduce security complexity.



**Technology professionals** should read this report to keep pace with the changing security landscape, as it provides insights on emerging trends, tailored security platforms and strategic objectives.

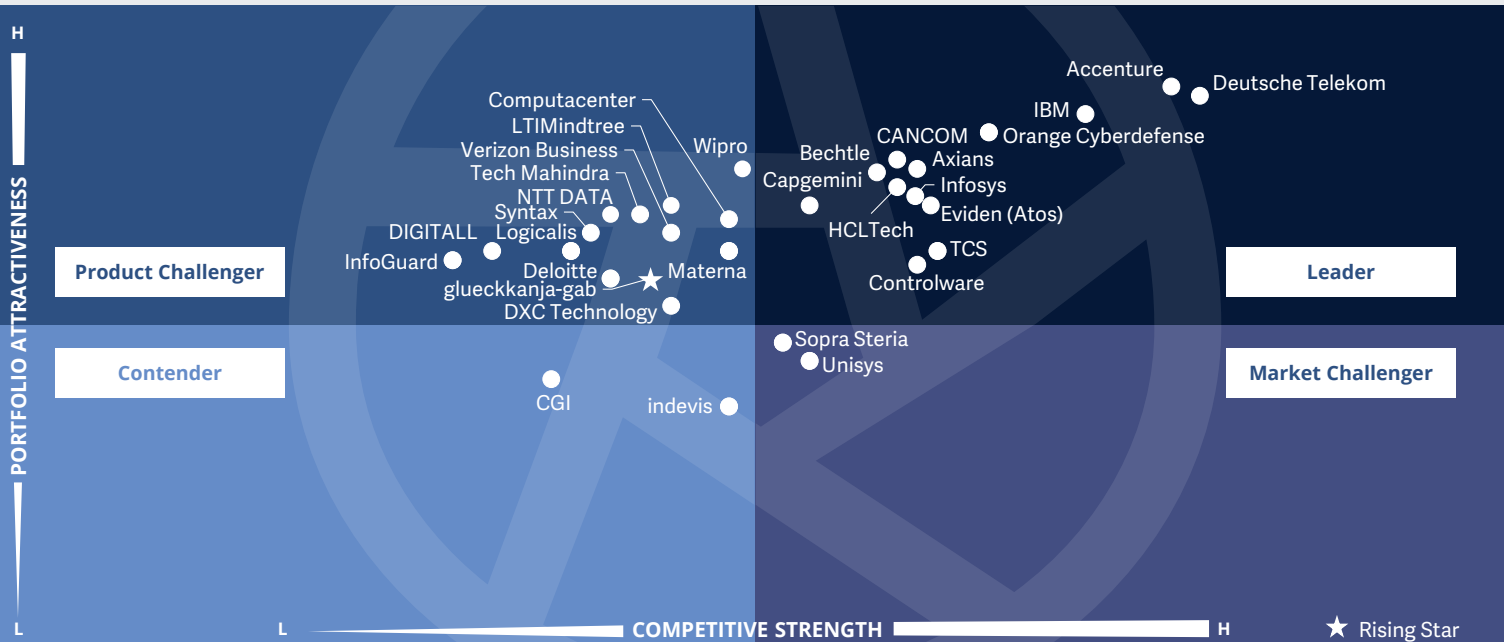


**Business professionals** should read this report to gain valuable insights on simplifying security operations. It also offers practical solutions to reduce complexity and enhance efficiency.



**Cybersecurity – Solutions and Services  
Managed Security Services - SOC**

Germany 2023



This quadrant evaluates the **most relevant** managed security service providers in Germany, excluding those providers that do not solely rely on their own products. The demand for external operations by **SOCs** is on the rise.

Frank Heuer



## Managed Security Services - SOC

### Definition

The providers assessed in the Managed Security Services (SOC) (MSS (SOC)) quadrant offer services related to the operations and management of IT and OT security infrastructures 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 resolution.

There is an increasing demand for providers to assist enterprises in enhancing their overall IT security posture and maximizing the effectiveness of their security programs over the long term with continuous improvement. To accomplish this, MSS (SOC) providers must combine traditional managed security services with innovation to fortify their 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,

infrastructure and experts skilled in threat hunting and incident management, allowing enterprises to actively detect and respond through threat mitigation and containment. Owing to the growing customer expectations around proactive threat hunting, providers are enhancing their SOC environments with security intelligence, with significant investments in technologies such as automation, big data, analytics, AI and machine learning. These sophisticated SOCs should support expert-driven security intelligence response, while 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, firewall operations, anti-virus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations** and all other operating services to provide ongoing, real-time protection, without compromising on business performance. In particular, secure access service edge (SASE) is included
2. Ability to provide security services, such as **detection and prevention; security information and event management (SIEM)** and security advisor and auditing support, remotely or at a client's site
3. Possesses **accreditations** from security tools vendors
4. **SOCs ideally owned and managed by the provider** and not predominantly by partners
5. Maintains **certified staff**, for example with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)



## Managed Security Services - SOC

### Observations

Increasingly sophisticated, frequent, complex and versatile cyberattacks are driving the demand for managed security services. German companies are now prioritizing these services due to the scarcity of qualified resources and the constant need for updated specialist knowledge.

Globally distributed security operations centers (SOCs) play a special role for large enterprises due to their international presence. However, these enterprises also appreciate SOC locations in Germany for data protection and compliance with legal regulations.

Midsize companies are facing greater cybersecurity skills shortages and are increasingly dependent on external service providers to address these growing challenges. They are now increasingly interested in managed security services, and SOC locations in Germany are seen as a positive aspect. Moreover, having German-speaking contacts is important for this customer group.

Providers need to be highly innovative to stay ahead in the race against cybercriminals. This involves expanding SOC locations into cyber defense centers and countering complex threats with AI and automation. The emergence of Cyber Fusion Centers as a supplement to existing SOC locations allows targeted and future-oriented cybersecurity management as cybercriminals also adopt AI in their tactics.

Of the 261 providers evaluated in this study, 31 qualified for this quadrant. Of these, 13 achieved a position as Leader. One provider was identified as a Rising Star.

### accenture

**Accenture** offers its clients a comprehensive range of services, covering all topics from a single source. Its international presence allows Accenture to effectively meet the requirements of its often globally active major clients.

### axians

**Axians** covers a wide range of managed security topics as part of its managed security services offering. For particularly vulnerable data and systems, Axians' global cyber defense center offers enhanced security and flexible solutions.



**Bechtle's** managed security services cover a wide range of services and technologies, with the added advantage of modular adaptability. In addition to various other countries, Bechtle also operates a dedicated SOC in Germany with German-speaking support.

### CANCOM

**CANCOM's** managed security services portfolio covers a wide range of managed technologies and services, along with a dedicated SOC in Germany.

### Capgemini

As part of its managed security services, **Capgemini** offers a wide range of managed security topics. The company has a large team of experts in Germany, serving numerous existing customers.

### Controlware

Measured specifically in terms of the number of customers, **Controlware** maintains a large team of experts in Germany and offers its customers modular and customizable managed security services.



**Deutsche Telekom** operates managed security services in Germany and other countries, maintaining an extensive team in this field. The provider continuously enhances its already comprehensive offerings.



## Managed Security Services - SOC



**Eviden (Atos)** has a SOC location in Germany, attracting interest from many large companies. Its managed security services cover a broad spectrum of topics.

### HCLTech

**HCLTech** operates several dedicated SOC in Germany alone, with a strong workforce dedicated to managed security services. Its portfolio covers a wide range of services and technologies.



**IBM** presents one of the broadest portfolios for IT security services, offering high-performance, in-house technology for managed security services. Its worldwide network of SOCs enables global operations.



**Infosys'** managed security services are highly comprehensive. The company is also well-positioned in terms of personnel skilled in managed security services in Germany.



**Orange Cyberdefense** operates SOCs worldwide, enabling global cybersecurity solutions. They company has SOC in Germany.



**TCS's** managed security services enable the operation of all cybersecurity technologies, including OT security. The company maintains a large team in Germany, both in absolute terms and in terms of the number of customers.

### glueckkanja-gab

**glueckkanja-gab** is the Rising Star for managed security services in Germany, owing to its proactive, qualified customer services.





# Appendix



## Methodology & Team

The market research study ISG Provider Lens™ Cybersecurity – Solutions and Services 2023 report analyzes the relevant software vendors/service providers in the German market, based on a multi-stage market research and analysis process and positions these providers based on the ISG Research™ methodology.

**Lead Author:**

Frank Heuer

**Editor:**

Maria Mueller

**Research Analyst:**

Bhuvaneshwari Mohan

**Data Analysts:**

Rajesh Chillappagari and Shilpashree N

**Consultant Advisor:**

Roger Albrecht

**Project Manager:**

Donston Sharwin

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 June 2023, 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 & 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 & Editor Biographies

Author



**Frank Heuer**  
**Principal Analyst**

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

His main responsibilities include advising ICT vendors on strategic and operational marketing and sales.

Mr. Heuer is a speaker at conferences and webcasts on his main topics and is a member of the IDG expert network. Mr. Heuer has been active in the IT market as an analyst and consultant since 1999.

Author



**Gowtham Kumar Sampath**  
**Assistant Director and Principal Analyst**

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 & Editor Biographies



*Research Analyst*

**Bhuvaneshwari Mohan**  
**Senior Research Analyst**

Bhuvaneshwari is a senior research analyst at ISG responsible for supporting and co-authoring Provider Lens™ studies on Banking, Cybersecurity, Supply Chain, ESG and Digital Transformation. She supports the lead analysts in the research process, authors the global summary report and develops content from an enterprise perspective. Her core areas of expertise lie in Cybersecurity, Cloud & Data transformation, AI/ML, Blockchain, IoT, Intelligent Automation and Experience Engineering. She has 7 years of hands-on experience and has delivered insightful reports across verticals.

She is a versatile research professional having experience in Competitive Analysis, Social Media Analytics, Glassdoor Analysis and Talent Intelligence. Prior to ISG, she held research positions with IT & Digital Service Providers and was predominantly part of Sales Enablement teams.



*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](mailto:contact@isg-one.com), call +1.203.454.3900, or visit [research.isg-one.com](http://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 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 more than 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](http://isg-one.com).





**AUGUST, 2023**

---

**REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES QUADRANT REPORT**