ISG Provider Lens®

Cybersecurity – Services and Solutions

An analysis of the cybersecurity market comparing the attractiveness of providers' portfolios and their competitive strength

Customized report courtesy of:

QUADRANT REPORT | JUNE 2026 | GERMANY

Table of Contents

Report Author: Frank Heuer

The technological revolution, uncertainty and a shortage of skilled workers are driving the German cybersecurity market

This ISG Provider Lens® study compares providers in Germany that offer cybersecurity services in the areas of consulting (specifically including post-quantum encryption), technical services and next-gen SOC/MDR services, as well as providers of data leakage/loss prevention (DLP) products. The provider assessment covers the customer segments of large and midsize enterprises and examines how providers enable companies to address challenges related to cybercrime, regulation and efficiency improvements.

A challenging market environment

In 2026, Germany faces a challenging economic and security environment. Geopolitical tensions, particularly around the Strait of Hormuz, continue to cause uncertainty in international markets. As one of the most important trade routes for oil and gas, the region has a significant influence on energy prices. Even minor escalations could drive inflation higher again and place additional strain on Germany's already fragile economic development.

The economic environment remains tense. According to the Federal Statistical Office, gross domestic product grew by only 0.3 percent in the first quarter of 2026 compared with the previous quarter. Many economists view this as a short-term stabilization rather than a sustainable upswing. Companies continue to act cautiously when it comes to investments as long as high costs and global uncertainties impair competitiveness.

At the same time, the shortage of skilled workers is intensifying, particularly in the field of cybersecurity. The digitalization of the economy is significantly increasing the demand for specialized IT and security experts. At the same time, there is a shortage of qualified professionals to effectively protect companies and critical infrastructure against digital threats. This trend is becoming even more significant as regulatory requirements continue to increase.

A challenging market environment is driving demand for external security services.

The European NIS2 Directive significantly tightens requirements for cybersecurity, risk management and reporting obligations. As a result, many companies are under considerable organizational and financial pressure.

Added to this is a significant rise in cybercrime. Criminal groups are increasingly using sophisticated and rapidly evolving attack methods, including AI-powered, automated phishing campaigns, ransomware and supply chain attacks. The threat landscape is constantly evolving and requires continuous investment in technology, personnel and security strategies. One example is the threat to the encryption of confidential data posed by quantum technology. Although this technology will not become commercially available for several years, criminals are already active with the Harvest Now, Decrypt Later (HNDL) approach.

Managed security services and cost-optimized solutions are in demand

ISG's latest IT budget study shows that data security and protection are among the top priorities for companies in Western Europe. For 96 percent of respondents at Western European companies, this is an important issue, and for 36 percent, it is even a critical one. This reflects, on the one hand, the tense geopolitical situation described above and, on the other hand, the increased threat posed by cybercrime. While large enterprises were primarily affected until a few years ago, small and midsize businesses and local government agencies have increasingly become the focus of cyberattacks, as they are often perceived, not without reason, as easy targets. Consequently, demand for cybersecurity services is growing particularly strongly in these target segments. These customer groups expect cost-optimized and modular offerings tailored to their needs. In addition, small and midsize enterprises (SMEs) want straightforward solutions that allow them to focus on their core business. Due to current geopolitical conditions, data sovereignty is an increasingly expected feature of (managed) security services; for some time now, SMEs have increasingly preferred operations and delivery from Germany or the EU.

Threats posed by AI-based attacks are becoming increasingly significant. According to the latest cybersecurity market study by ISG, these attacks will rank among the top five cybersecurity challenges for companies with at least 1,000 employees in Western Europe over the next two years. For 15 percent of respondents, this is even the most critical issue. Publications by Anthropic AI regarding the detection of software vulnerabilities have brought this topic into the spotlight of public discussion from a specific angle. At the same time, 41 percent of decision-makers in Western European companies cite a lack of AI expertise as an important organizational challenge, and 10 percent of respondents even name it as the most important one. The general shortage of cybersecurity professionals remains a top five organizational security challenge for 28 percent of respondents; this figure is likely even higher among small and midsize enterprises.

It is therefore not surprising that for nearly half of the aforementioned group of respondents, continuous threat protection and response, such as through a Security Operations Center (SOC), is among the top five priorities for cybersecurity implementation; for 12 percent, it is the top priority. This trend is also reflected in the expected growth of the German market for managed security services in 2026, which is projected to exceed 15 percent year-over-year.

Nevertheless, the subdued overall economic situation is also evident in cybersecurity budgets. For 18 percent of respondents in Western Europe, budget constraints are a top three challenge. Adaptable and cost-effective solutions are also important for large enterprises.

A wide range of technical and organizational options for competitive differentiation

In the German market, cybersecurity providers that are best able to meet the needs of their client companies have a particular advantage. Among others, service providers that can offer their clients seamless, end-to-end services and integrate IT and security solutions from a single source stand to benefit. In addition, consultants with in-depth knowledge of regulatory requirements can distinguish themselves. Service providers that already offer consulting on post-quantum encryption have an advantage in customer segments where corporate assets are heavily based on digital assets, such as banks and insurance companies.

In the technical security services (TSS) market, there is particular demand for service providers that can offer a broad range of services from a single source, as IT security projects are often complex and multifaceted.

The increasingly complex nature of cyberattacks is also driving demand for Security Operations Centers (SOCs) and Managed Detection & Response (MDR) services. The shortage of qualified professionals and the need for constantly up-to-date specialist knowledge make these services even more attractive to German companies.

Preference is given to providers that operate SOCs located in Germany or the EU, as more and more prospective clients value such SOCs due to the increased importance of data protection (digital sovereignty). A high level of innovation is essential to stay one step ahead in the race against cybercriminals. To combat cyber threats, managed security services providers are increasingly leveraging automation and AI. The ideal approach combines machine efficiency with comprehensive human expertise. Up-to-date threat intelligence is a key competitive factor, enabling the most direct possible response to threats. Providers of SOC/MDR services who are also network operators have a particular advantage here, as they can detect threats within the network more quickly than other network users (through threat intelligence).

In the DLP product sector, vendors that offer a *no backdoor* guarantee, ensuring that third parties cannot gain covert access, are increasingly valued. Furthermore, DLP products that reduce the workload on IT staff through a high degree of automation are recommended. The ability to respond promptly to security incidents using defined processes for investigation and mitigation is a key differentiator. Prebuilt policy templates that comply with the EU General Data Protection Regulation are also welcomed by user companies.

In the German cybersecurity market, providers are particularly successful when they address a balanced mix of target groups. Of particular note is the ability to address both the requirements of large enterprises and the needs of small and midsize businesses. This allows these providers to benefit from both the substantial budgets of large clients and the dynamically growing demand from midsize companies.

Outlook: Challenges and Opportunities

The cyber threat landscape in Germany will continue to intensify; (misused) technologies and the shortage of skilled workers are contributing to this. This presents challenges for user companies, but also opportunities for providers of cybersecurity solutions.

Over the next two years, AI-powered cyberattacks will become significantly more sophisticated and harder to detect. AI enables attackers to create highly personalized phishing emails, realistic deepfakes, and automated social engineering attacks on a large scale. At the same time, malware is becoming increasingly adaptive and can dynamically bypass security mechanisms. The speed of attacks is also increasing, as AI automatically identifies and exploits vulnerabilities. This presents companies with a growing challenge: traditional security approaches will no longer suffice in the future. To keep pace with the increasing dynamism and complexity of modern cyber threats, AI-based defense systems, rapid response processes, and well-trained staff are crucial.

At the same time, the acute shortage of skilled workers in the cybersecurity sector will remain a significant issue for the foreseeable future, even as AI takes on more and more tasks. Midsize companies remain particularly affected by this. In addition to SMEs, governments (local) are also expected to continue to be increasingly targeted by cybercriminals. As a result, demand from these target groups for external services, particularly SOC/MDR services, will continue to grow at an above-average rate. Due to the geopolitical tensions expected to persist in the near future, digitally sovereign solutions will be highly preferred.

The threat to data encryption posed by quantum computers will become increasingly acute in the coming years. Q-Day is drawing nearer; it is becoming increasingly dangerous not to prepare for the threats posed by this new technology, as the Harvest Now, Decrypt Later approach becomes more lucrative with each passing day. Timely consultation and action are recommended.

Executive Summary

In the near future, cybersecurity providers that have a comprehensive grasp of security for, with, and against AI will have an advantage. Furthermore, service providers with a balanced customer base and clients from the public sector who can also demonstrate SOC operations based in Germany will benefit. Above-average growth opportunities are available to consultants who offer post-quantum encryption consulting and address the breadth of the market from a long-term perspective.

Quantum technology is becoming a threat to users faster than expected, but like AI, it also offers new opportunities for cybersecurity service providers. Providers that offer tailored, secure solutions, target a diverse audience and have a firm grasp of both technical and regulatory aspects will have an advantage.

Provider Positioning

Page 1 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
8com	Not In	Not In	Not In	Product Challenger	Not In	Not In
Absolute Software	Not In	Not In	Not In	Not In	Not In	Contender
Accenture	Leader	Leader	Leader	Not In	Leader	Not In
Acronis	Not In	Not In	Not In	Not In	Not In	Product Challenger
All for One Group	Contender	Contender	Not In	Not In	Not In	Not In
Argos Security	Not In	Product Challenger	Market Challenger	Rising Star ★	Not In	Not In
Atos	Leader	Leader	Leader	Not In	Not In	Not In
Axians	Leader	Leader	Leader	Leader	Not In	Not In
Bechtle	Market Challenger	Leader	Leader	Leader	Rising Star ★	Not In
Brainloop	Not In	Not In	Not In	Not In	Not In	Product Challenger
Broadcom	Not In	Not In	Not In	Not In	Not In	Leader

Provider Positioning

Page 2 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
CANCOM	Market Challenger	Leader	Product Challenger	Leader	Not In	Not In
Capgemini	Leader	Leader	Leader	Not In	Not In	Not In
CGI	Contender	Not In	Not In	Contender	Not In	Not In
Computacenter	Leader	Leader	Product Challenger	Contender	Not In	Not In
Controlware	Leader	Leader	Leader	Leader	Not In	Not In
CoSoSys (Netwrix)	Not In	Not In	Not In	Not In	Not In	Contender
DATAGROUP	Not In	Not In	Market Challenger	Leader	Contender	Not In
Deloitte	Leader	Product Challenger	Product Challenger	Not In	Leader	Not In
Deutsche Telekom	Leader	Leader	Leader	Leader	Not In	Not In
DriveLock	Not In	Not In	Not In	Not In	Not In	Leader

Provider Positioning

Page 3 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
DXC Technology	Contender	Leader	Contender	Not In	Not In	Not In
EY	Leader	Not In	Product Challenger	Not In	Leader	Not In
Fidelis Security	Not In	Not In	Not In	Not In	Not In	Contender
Forcepoint	Not In	Not In	Not In	Not In	Not In	Leader
Fortra	Not In	Not In	Not In	Not In	Not In	Leader
GBS	Not In	Not In	Not In	Not In	Not In	Leader
Getronics	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In
glueckkanja	Not In	Not In	Rising Star ★	Leader	Not In	Not In
Google	Not In	Not In	Not In	Not In	Not In	Contender
HCLTech	Leader	Leader	Leader	Product Challenger	Not In	Not In

Provider Positioning

Page 4 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
HiSolutions	Product Challenger	Not In	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Leader	Not In	Leader	Leader
InfoGuard	Not In	Product Challenger	Leader	Leader	Not In	Not In
Infosys	Product Challenger	Product Challenger	Leader	Not In	Not In	Not In
itWatch	Not In	Not In	Not In	Not In	Not In	Product Challenger
KPMG	Leader	Not In	Not In	Not In	Leader	Not In
Kyndryl	Product Challenger	Product Challenger	Contender	Not In	Not In	Not In
Logicalis	Contender	Contender	Not In	Product Challenger	Not In	Not In
LTM	Not In	Not In	Not In	Product Challenger	Not In	Not In
ManageEngine	Not In	Not In	Not In	Not In	Not In	Leader

Provider Positioning

Page 5 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
Materna	Leader	Market Challenger	Not In	Not In	Not In	Not In
Microsoft	Not In	Not In	Not In	Not In	Not In	Leader
Mimecast	Not In	Not In	Not In	Not In	Not In	Product Challenger
Netskope	Not In	Not In	Not In	Not In	Not In	Product Challenger
NTT DATA	Rising Star ★	Product Challenger	Product Challenger	Product Challenger	Leader	Not In
OpenText	Not In	Not In	Not In	Not In	Not In	Product Challenger
Orange Cyberdefense	Product Challenger	Market Challenger	Leader	Not In	Not In	Not In
ORBIT	Contender	Contender	Not In	Not In	Not In	Not In
pco	Not In	Not In	Contender	Product Challenger	Not In	Not In
Proofpoint	Not In	Not In	Not In	Not In	Not In	Market Challenger

Provider Positioning

Page 6 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
PwC	Product Challenger	Not In	Not In	Not In	Product Challenger	Not In
q.beyond	Not In	Not In	Not In	Product Challenger	Not In	Not In
Rohde & Schwarz	Not In	Not In	Not In	Not In	Product Challenger	Not In
secunet	Not In	Not In	Not In	Not In	Product Challenger	Not In
SITS	Product Challenger	Product Challenger	Not In	Product Challenger	Market Challenger	Not In
Skaylink	Not In	Not In	Not In	Contender	Not In	Not In
Skyhigh Security	Not In	Not In	Not In	Not In	Not In	Product Challenger
Sopra Steria	Market Challenger	Not In	Market Challenger	Market Challenger	Not In	Not In
suresecure	Product Challenger	Product Challenger	Product Challenger	Leader	Not In	Not In
SVA	Not In	Not In	Not In	Product Challenger	Not In	Not In

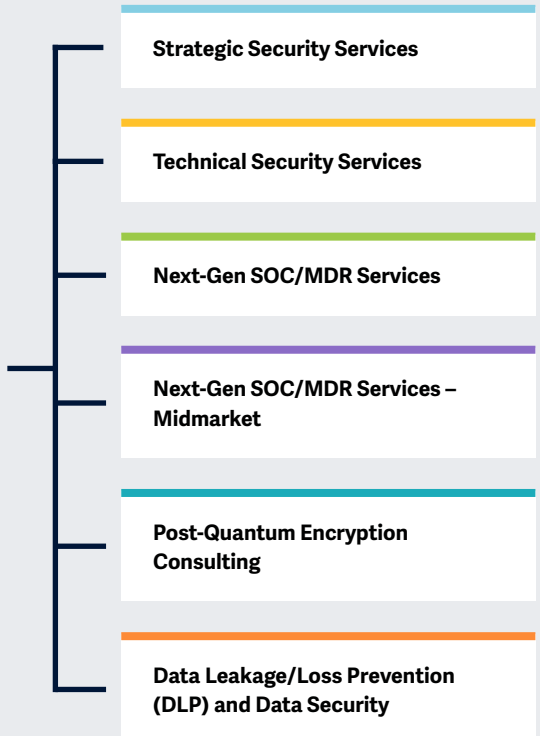
Provider Positioning

Page 7 of 7

	Strategic Security Services	Technical Security Services	Next-Gen SOC/MDR Services	Next-Gen SOC/MDR Services – Midmarket	Post-Quantum Encryption Consulting	Data Leakage/Loss Prevention (DLP) and Data Security
Syntax	Not In	Product Challenger	Contender	Market Challenger	Not In	Not In
TCS	Product Challenger	Product Challenger	Leader	Not In	Product Challenger	Not In
Tech Mahindra	Not In	Product Challenger	Product Challenger	Product Challenger	Not In	Not In
Trellix	Not In	Not In	Not In	Not In	Not In	Leader
Unisys	Market Challenger	Market Challenger	Contender	Not In	Not In	Not In
Varonis	Not In	Not In	Not In	Not In	Not In	Product Challenger
Verizon Business	Not In	Not In	Product Challenger	Not In	Not In	Not In
Wavestone	Product Challenger	Not In	Not In	Not In	Product Challenger	Not In
Wipro	Leader	Product Challenger	Product Challenger	Not In	Contender	Not In
Zscaler	Not In	Not In	Not In	Not In	Not In	Product Challenger

Key focus areas of the study **Cybersecurity – Services and Solutions** 2026.

Simplified Illustration Source: ISG 2026



Definition

In 2026, the cybersecurity landscape is expected to witness an increase in threat sophistication, expanding regulatory demands and a rapid shift toward intelligence-driven defense models. Enterprises across industries are under pressure to secure their increasingly distributed architectures, protect sensitive data across hybrid environments and respond to the surge in AI-enabled attacks. Meanwhile, boards and regulators seek demonstrable cyber resilience and verifiable control effectiveness, paving the way for security programs as part of digital transformation agendas.

In this light, the market is reorganizing itself into clearly defined capability domains. While technical security services (TSS) ensure configuration integrity, secure implementations and continuous hardening, strategic security services (SSS) are gaining importance as executives prioritize cybersecurity with governance, risk and architectural alignment.

Next-generation SOCs and managed detection and response (MDR) services are also gaining traction, driven by the demand for 24/7 threat monitoring, AI-supported analysis and outcome-based response models. Additionally, risk-based vulnerability management reinforces preventive security by prioritizing exposures using business context and attack path insights. Finally, post-quantum encryption consulting enters the market scope as organizations begin preparing cryptographic inventories and transition strategies to safeguard long-term data confidentiality.

This IPL study covers the mentioned capability domains, among others, and offers a comprehensive view how providers differentiate in an environment defined by speed, intelligence and resilience.

Scope of the Report

This ISG Provider Lens® Quadrant Report covers the following six quadrants for services/ solutions: Strategic Security Services, Technical Security Services, Next-Gen SOC/MDR Services, Next-Gen SOC/ MDR Services – Midmarket, Post-Quantum Encryption Consulting and Data Leakage/Loss Prevention (DLP) and Data Security.

This ISG Provider Lens® study offers IT decision-makers:

- Transparency regarding the strengths and weaknesses of the respective providers and software vendors
- A differentiated positioning of providers by segment (quadrant)
- A focus on the regional market

The study thus provides a key basis for decision-making regarding positioning, relationship management and go-to-market strategies. ISG Advisors and corporate clients also use information from these reports to evaluate their current and potential new vendor relationships.

Provider Classifications

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

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

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

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

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

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

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

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

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

Strategic Security Services

Who Should Read This Section

This report is valuable for providers offering **strategic security services (SSS) in Germany** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence.

Cybersecurity professionals

Should read this report to better manage evolving risks, strengthen threat detection capabilities, and understand how providers address advanced threats using emerging technologies such as AI. The insights help align cybersecurity strategies with broader business objectives while staying current on key security and risk management trends.

Technology professionals

Should read this report to identify security partners that embed protection into digital initiatives. The analysis highlights how providers leverage AI, automation, and tailored security services to counter advanced threats, integrate security across complex environments and support secure innovation within large-scale digital transformation programs.

Strategy professionals, CFOs and CEOs

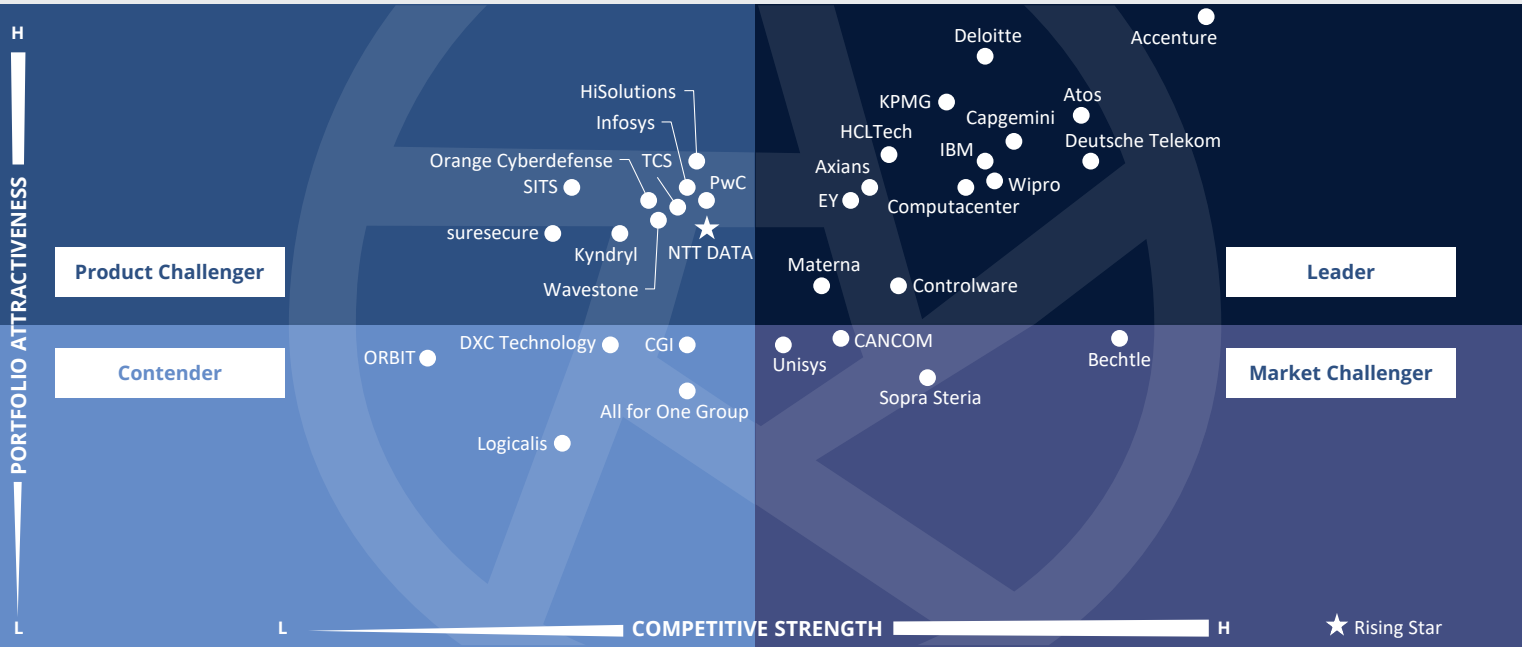
Should read this report to assess providers' partnership capabilities, scalability and potential for cost optimization. CFOs and CEOs can use the insights to evaluate cost-effective security solutions, strengthen enterprise cybersecurity posture and ensure investments align with long-term business resilience and strategic priorities.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Strategic Security Services

Germany 2026



This quadrant focuses on the **most relevant** cybersecurity consultants in Germany who offer services **beyond their own products.** Increasing cyber threats with new criminal strategies **are driving up demand.**

Frank Heuer

Definition

This quadrant evaluates service providers that deliver consulting-led cybersecurity services focusing on strategy, governance, risk management and organizational transformation for IT and OT environments. These providers assess security maturity, quantify risks, define target operating models and develop cybersecurity strategies, policies and roadmaps aligned with business objectives and regulatory requirements. Their offerings include audits, assessments, security awareness programs, business continuity planning, tabletop exercises and advisory on technology selection. These providers also employ experienced consultants who guide enterprises through program design, governance improvements and capability development, including virtual Chief Information Security Officer (vCISO) models for ongoing or on-demand strategic leadership. Unlike TSS, which emphasize hands-on integration and engineering, SSS providers focus on advisory outcomes rather than operational monitoring or proprietary product execution.

Eligibility Criteria

1. **Vendor-neutral security consulting** in the areas of maturity assessment, strategy development, policy design, governance models, and roadmap creation
2. Proven **capabilities in strategic areas** such as risk quantification, regulatory readiness, vendor selection, business continuity planning, and consulting on cyber risks in the broader sense
3. **Application** of **recognized frameworks** and adherence to standards (such as ISO 27000, NIST CSF, CIS Controls) in the management of enterprise programs
4. **Delivery of at least one of the above** strategic security services in the target region by **qualified and certified** consultants
5. Submission **of documented evidence** of projects that have improved clients' security posture, governance structures, regulatory readiness, or risk-based decision-making
6. Provision of **structured consulting methodologies**, templates, or playbooks for assessments, strategic planning, or organizational transformation
7. Operating as **a consulting-oriented service provider** rather than a product vendor, but utilizing proprietary frameworks or tools to support the consulting service
8. **No exclusive focus** on proprietary products

Observations

Cybersecurity challenges are diverse, evolving at an ever-faster pace, becoming increasingly threatening and affecting new target groups. Consulting services must adapt to these challenges to provide effective guidance and support.

The growing need for consulting services stems from global conflicts and tensions, as well as from commercial cybercrime, which continues to employ ever-evolving methods. Added to this is the realization that a zero-trust approach is essential.

In addition to these threats, regulatory requirements and the need to account for business conditions pose a growing challenge. European companies also increasingly require assessments of digital sovereignty, as geopolitical tensions heighten concerns regarding data location. Consequently, service providers that can demonstrate expertise in both technical and business/compliance matters have a distinct advantage.

Similar to large enterprises, many SMEs are currently affected in multiple ways. As perceived easy targets, they are increasingly being targeted by cybercriminals. Furthermore, due to the NIS 2 Directive, numerous SMEs are now classified as critical infrastructure and must consequently implement (additional) cybersecurity measures. At the same time, the shortage of IT specialists continues to exacerbate this situation; SMEs are particularly hard hit by the skills shortage. Due to these factors, companies increasingly require external support. This process often begins with consulting.

Materna has risen from Rising Star to Leader this year. NTT DATA is the new Rising Star. PwC and SITS are new entrants to the quadrant.

Of the 71 providers evaluated in this study specifically for the German market, 33 qualified for this quadrant. Of these, 14 achieved Leader status. One provider was identified as a Rising Star.

accenture

Leading expertise and experience, along with a systematically developed, comprehensive range of services, contribute to **Accenture's** strong success in cybersecurity consulting in Germany.

Atos

Atos stands out as a leader in the German cybersecurity consulting market with its holistic approach.

axians

With its targeted, pragmatic approach to cybersecurity consulting, **Axians IT Security** particularly meets the needs of the midmarket.

Capgemini

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

Computacenter

Computacenter supports its clients with cybersecurity consulting integrated into a holistic end-to-end approach, positioning itself as a strategic partner with a deep understanding of clients' infrastructure and business requirements.

controlware

With a large, qualified team of experts and a strong customer focus, **Controlware** is steadily growing in the German strategic security services market and successfully positioning itself as a leading provider.

Deloitte.

Deloitte has a strong global presence and specializes in integrating business and technology consulting within cybersecurity consulting.

With extensive experience in demanding environments and end-to-end services from a single source, **Deutsche Telekom** stands out as a cybersecurity consultant in Germany.

EY

EY stands out with a holistic consulting approach, extensive experience and innovative services, thereby securing a leading position in the German market for strategic security services.

HCLTech

Through an innovative, broad-based, and customer-oriented portfolio, **HCLTech** has successfully positioned itself as a leading provider of strategic security services in Germany.

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

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

Materna is becoming increasingly successful and is evolving from a Rising Star into a leading provider of cybersecurity consulting services in Germany.

Wipro impresses its clients in Germany with comprehensive technical expertise and extensive cybersecurity consulting.

Thanks to an innovative, attractive portfolio and growing market presence, **NTT DATA** is the new **Rising Star** for strategic security services in Germany.

Leader

"Extensive experience and expertise in demanding environments contribute to Deutsche Telekom's success and leading position in the German cybersecurity consulting market."

Frank Heuer

Deutsche Telekom

Overview

Headquartered in Bonn, Germany, Deutsche Telekom employs more than 198,000 people in 50 countries. In FY25, the company generated €119.1 billion in revenue. In 2020, Telekom Security was transformed into a separate legal entity, Deutsche Telekom Security GmbH, within the Deutsche Telekom Group. Deutsche Telekom / T-Systems (hereinafter "Deutsche Telekom") employs more than 2,600 people in the security sector worldwide. In addition to managed security services and Technical Security Services, the company also offers Strategic Security Services.

Strengths

Long-standing certified cybersecurity expertise: Deutsche Telekom draws on over 25 years of security and project expertise and has built one of the largest databases for threat intelligence. Deutsche Telekom's employees are highly certified consultants for various standards and technologies.

Expert in demanding environments: Deutsche Telekom specializes in the security of critical national infrastructure. The company's security consultants possess expertise regarding the specific requirements of regulated industries.

Combined IT and telecommunications expertise: Deutsche Telekom is able to combine IT and telecommunications security and integrate various technologies from leading providers, which is particularly important for SASE solutions.

Provider of end-to-end services: Deutsche Telekom is not only a capable cybersecurity consultant but, in particular, a renowned provider of managed security services; it is also highly competent in the technical implementation of IT security projects and thus able to put its own recommendations into practice seamlessly and as a cohesive whole.

Caution

It is advisable to assess whether further expansion of the global presence is possible. Deutsche Telekom is now represented on three continents, but compared to other outstanding, leading providers, its international presence still has room for growth.

Technical Security Services

Who Should Read This Section

This report is valuable for providers offering **technical security services (TSS) in Germany** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence.

Technology professionals

Should read this report to understand how providers are addressing compliance requirements, evolving market dynamics, and integration challenges. The insights help inform decisions on adopting advanced technologies that enable innovation, improve scalability, and reduce security threats while supporting resilient, future-ready digital architectures.

Security and data professionals

Should read this report to gain a deeper understanding of provider compliance approaches, key market trends, and the role of vendor-neutral solutions. The findings support informed decision-making for large-scale architecture transformations that prioritize interoperability, improved security posture and long term data protection.

Business professionals

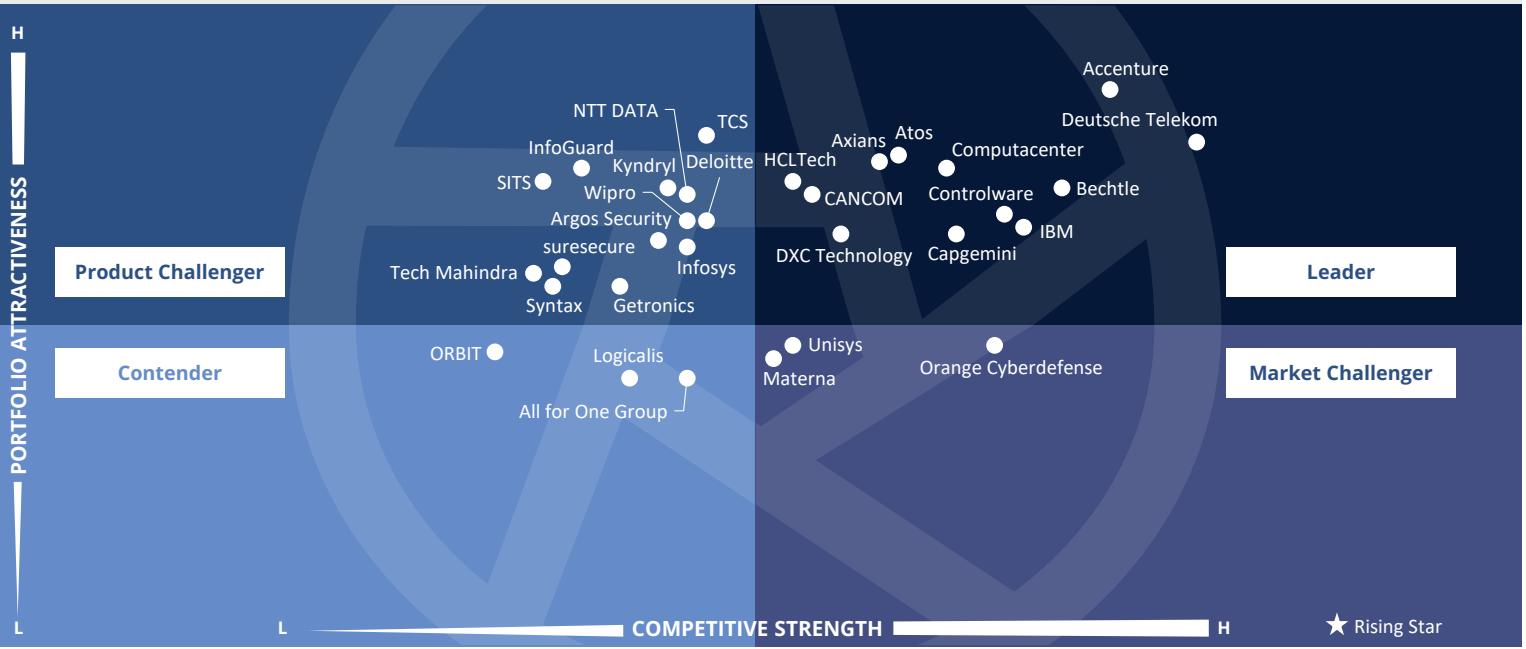
Should read this report to better balance data security, customer experience and privacy requirements. The insights highlight how organizations can manage risk and trust while enabling digital transformation initiatives central to modern business growth, regulatory compliance and competitive differentiation.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services

Germany 2026



This quadrant focuses on the **most relevant** providers of TSS in Germany whose offerings extend **beyond their own products.** Due to increasing challenges and a shortage of skilled workers, **external providers** are becoming increasingly **important.**

Frank Heuer

Definition

This quadrant evaluates service providers that design, integrate, implement and modernize IT and OT security technologies across multi-vendor environments. Their services include deploying and configuring security controls for identity and access management, cloud and data centers, SASE/SSE, endpoints, networks, OT and industrial control systems (ICS), and related domains. Providers use reference architectures, automation frameworks and proprietary accelerators to deliver engineering-led transformations that streamline implementation and enhance control effectiveness. They maintain strong partnerships with security vendors, hold specialized certifications and support lifecycle tasks such as hardening, tuning, patching and device management. Unlike SSS, which focus on advisory and governance, TSS providers emphasize hands-on technical execution. They do not offer SOC-based monitoring or MDR operations but may provide traditional managed security services.

Eligibility Criteria

1. Proven experience in the **development, integration, and implementation** of IT and/or OT security technologies, supported by certifications from multiple vendors and OEM partnerships
2. Use of **accelerators, proprietary tool sets, or reference architectures** that improve implementation quality, interoperability, and time to value
3. **Certified engineers and architects** with experience in configuring, customizing, and optimizing security solutions for cloud, network, endpoint, and OT environments
4. **Demonstration of a structured, method-driven approach** to the evaluation, selection, and integration of security technologies that aligns with customer requirements, risk profiles, and architectural constraints
5. **Lifecycle engineering** services such as configuration management, policy tuning, patching, control hardening, and technology modernization
6. Presentation of documented **case studies** demonstrating the successful deployment of security technologies or their transformation in the target region
7. Operating as **a service-oriented integrator** rather than an independent ISV, but incorporating proprietary accelerators or internally developed tools to support service delivery
8. **No exclusive focus** on proprietary products

Observations

The increasingly intense and ever-evolving cyberattacks remain a challenge for companies in Germany, a challenge further compounded by the shortage of cybersecurity experts. This situation is driving demand for external services. Providers that master current technologies and know how to address various target groups have an advantage.

Identity security remains a central issue for German companies and is gaining additional significance as non-human identities are protected. Given the increasing adoption of AI in companies, AI security, platform protection and secure AI infrastructure are becoming increasingly important. In addition to security *for* AI, security *enabled by* AI is becoming increasingly important. The updating of threat intelligence deserves special mention in this context. Data security, both on-premises and in the cloud, remains a high-priority challenge, accompanied by corresponding requirements for data security posture management.

Providers with a balanced customer base comprising both large enterprises and midsize companies benefit from both the substantial budgets of large enterprises and the above-average demand growth from midsize companies.

Argos Security emerged from the merger of the German providers indevis and Data-Sec and is now represented in the Quadrant in place of indevis. The Swiss service providers InfoGuard and SITS have also successfully entered the Quadrant. Riedel Networks has not yet qualified for the Quadrant but shows strong potential for the future. The Brazilian service provider Stefanini is expanding in Germany and has a good chance of being represented in the quadrant in the future.

Of the 71 providers evaluated in this study specifically for the German market, 31 qualified for this quadrant. Twelve of them achieved a position as a Leader.

accenture

Through automation and a broad service portfolio, **Accenture** enables cost-effective end-to-end security and positions itself as a leading provider of technical security services in Germany.

Atos

A large, qualified team and a broad service portfolio make **Atos** a high-performing, leading provider of technical security services in Germany.

axians

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

BECHTLE

Bechtle stands out with a strong local market presence and extensive resources, positioning itself as a leading provider of technical security services in Germany, particularly in the dynamically growing small and midsize enterprises market segment.

CANCOM

CANCOM impresses its customers with tailored solutions based on a comprehensive range of topics and services. CANCOM offers high-performance technical cybersecurity services for small and midsize enterprises and for demanding KRITIS sectors.

Capgemini

Capgemini distinguishes itself as an innovative provider of technical security services and boasts a large international team.

Computacenter combines its strong partner network with comprehensive services and extensive in-house expertise, positioning itself as a leader in the German market for technical security services.

Controlware is successful in the fast-growing SME segment.

With its targeted and modular technical cybersecurity services and German roots,

With a large, highly qualified team and an end-to-end service offering made in Germany, **Deutsche Telekom**, through its subsidiary Deutsche Telekom Security, is a leader in technical security services in Germany.

DXC Technology's customers benefit from integrated IT/security solutions as well as the capabilities of a large, internationally active team.

With international experience, a broad portfolio, and strong technology partnerships, **HCLTech** positions itself as a leading provider of technical security services in Germany.

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

Leader

"Thanks to a large, highly qualified team and end-to-end services made in Germany, Deutsche Telekom, together with its subsidiary Deutsche Telekom Security, is a leading provider of technical security services in Germany."

Frank Heuer

Deutsche Telekom

Overview

Headquartered in Bonn, Germany, Deutsche Telekom employs more than 198,000 people in 50 countries. In FY25, the company generated €119.1 billion in revenue. In 2020, Telekom Security was transformed into a separate legal entity, Deutsche Telekom Security GmbH, within the Deutsche Telekom Group. Deutsche Telekom / T-Systems (hereinafter "Deutsche Telekom") employs more than 2,600 people in the security sector worldwide. In addition to managed security services and Strategic Security Services, the company also offers Technical Security Services.

Strengths

Services from Germany: With Security made in Germany, Deutsche Telekom scores particularly well with midmarket customers. Customer proximity and the local delivery of TSS are major advantages, not just for midmarket customers.

Very large, qualified team: The large workforce enables close customer relationships—Deutsche Telekom employs the largest team of cybersecurity specialists in Germany. In addition, the company enhances its specialists' expertise through extensive training and certification programs, resulting in more than 2,000 employee certifications. Last but not least, the experts can draw on their extensive experience from providing cybersecurity services to the Deutsche Telekom Group.

End-to-end cybersecurity solutions: Deutsche Telekom offers comprehensive TSS that cover a wide range of areas to enable zero-trust-based solutions for customers. In addition to TSS, the company also offers consulting and managed security services from a single source, ensuring that the entire lifecycle of a security project is covered. Furthermore, it enables IT solutions with associated cybersecurity. Another advantage is the company's specialized expertise in combining IT and telecommunications security.

Caution

Deutsche Telekom is now represented on three continents; however, compared to other leading providers at Deutsche Telekom's performance level, its international presence still has room for expansion.

Next-Gen SOC/MDR Services

Who Should Read This Section

This report is valuable for providers offering **next-gen SOC/MDR services in Germany** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence.

Cybersecurity professionals

Should read this report to gain a clear understanding of emerging threat patterns, evolving attack vectors and near-term risks shaping the security landscape. The insights support informed security planning, enable rapid control prioritization and help teams strengthen defenses while improving operational efficiency and reducing overall security complexity.

Technology professionals

Should read this report to understand key cybersecurity trends and how integrated, platform-based security approaches align with broader IT and digital transformation goals. The report offers insights into modern security architectures and strategic objectives, helping technology leaders design resilient environments that keep pace with rapidly changing security demands.

Business professionals

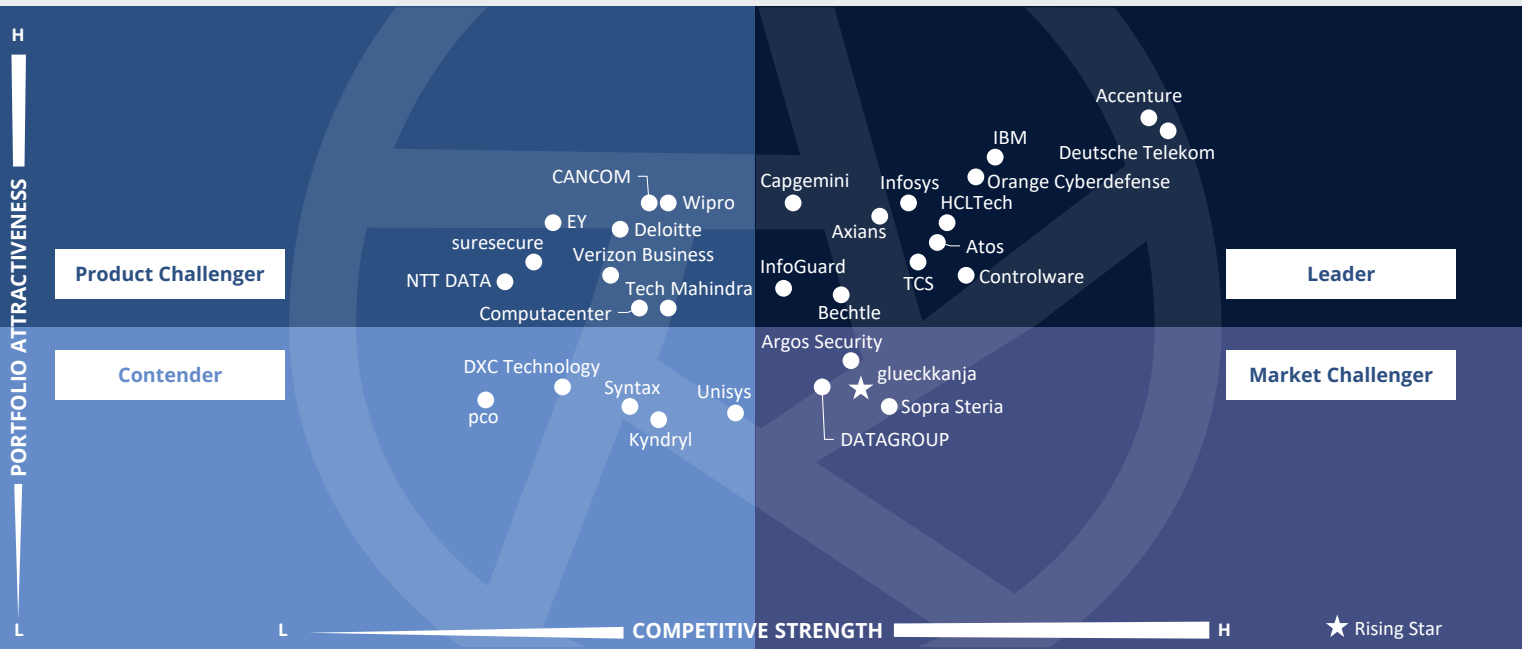
Business professionals must read this report to gain practical insights into simplifying security operations while balancing risk, cost and efficiency. It highlights actionable approaches and solutions that reduce operational complexity, support better decision-making and enable organizations to strengthen security outcomes without slowing business performance or innovation.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC/MDR Services

Germany 2026



This quadrant focuses on the **most relevant** providers of **next-gen SOC/MDR services** in the German market, excluding service providers that limit their offerings to their own products. The threat landscape and a shortage of skilled workers **are driving** the market.

Frank Heuer

Definition

This quadrant evaluates service providers that deliver continuous monitoring and MDR services through SOCs. Their offerings span the entire incident lifecycle, including detection, triage, investigation, containment and coordinated remediation. Providers integrate and operate modern security technologies, apply threat intelligence and advanced analytics, and deliver human-led and automated threat hunting to strengthen enterprise resilience. Next-gen SOC/MDR services combine managed security operations with innovative AI-driven analytics, autonomous triage and security orchestration, automation and response (SOAR)-based orchestration to reduce response times and improve threat visibility across IT and OT environments. They support co-managed models and do not focus on strategic advisory or technology implementation, which fall within the scope of SSS and TSS, respectively.

In the following, "Managed Services" is used synonymously with "Next-Gen SOC/MDR Services."

Eligibility Criteria

1. **24/7 monitoring, detection, and response services** via **proprietary SOCs** covering IT and/or OT environments
2. **MDR-specific capabilities**, including behavioral analysis, integration of threat data based on a Large Language Model (LLM), human-driven and automated threat hunting, and advanced detection engineering
3. **Operation and management** of Security Information & Event Management (SIEM), SOAR, Endpoint Detection & Response (EDR), Network Detection & Response (NDR), and other relevant security technologies, supported by OEM accreditations
4. Demonstration of a structured **approach to incident response,** including triage, investigation, containment, coordination of remediation efforts, and post-incident improvement
5. Use of **AI-driven** analytics, autonomous triage agents, and SOAR workflows for faster detection and shorter mean time to response (MTTR)
6. **Co-managed service models** that enable shared visibility, collaboration with analysts, and joint response processes
7. **Reference** cases demonstrating measurable improvements in detection coverage, response efficiency, or operational resilience in the target region
8. **No exclusive focus** on proprietary products, but rather management and operational services for best-of-breed security tools

Observations

Demand for MDR services and SOC services is driven by increasingly sophisticated, frequent, complex and adaptable cyberattacks. For 2026, ISG forecasts more than 15 percent growth in the German market for managed security services, of which SOC and MDR services are key components, following 16.5 percent growth in 2025.

The need for constantly up-to-date specialist knowledge and the simultaneous shortage of qualified professionals are increasingly bringing these managed services into the spotlight for German companies.

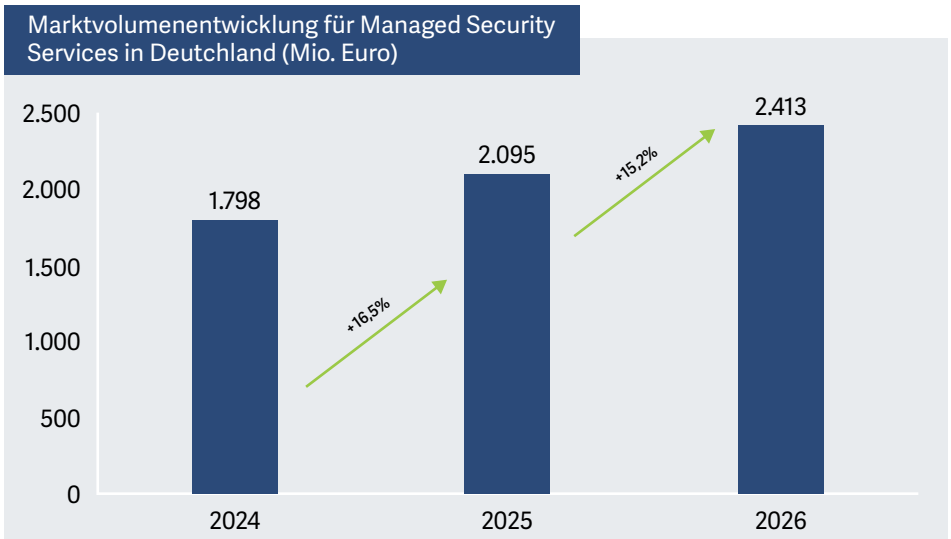
For large enterprises, globally distributed SOCs play a special role due to their often international presence. However, large enterprises also value EU and German SOC locations because of the increased importance of data protection.

SMEs are also showing increased interest in SOC and MDR services to help them overcome growing challenges amid a severe shortage of skilled workers. For this target group, SOCs in Germany and German-speaking contacts are key advantages.

In general, providers are also expected to demonstrate a high degree of innovation. This includes, among other things, increasing efficiency through automation, such as agentic AI. For industrial customers, the integration of OT security to safeguard networked manufacturing facilities is of interest.

InfoGuard has moved from Rising Star to Leader this year. The new Rising Star is glueckkanja. Argos Security emerged from the merger of the German providers indevis and Data-Sec and is now represented in the quadrant in place of indevis. EY has also made a successful entry.

Ein stark wachsender Markt



Quelle: ISG Research DACH

Of the 71 vendors evaluated in this study specifically for the German market, 31 qualified for this quadrant. Of these, 13 achieved a Leader position. One vendor was identified as a Rising Star.

accenture

Comprehensive services, a broad spectrum of supported technologies, a global presence and expansion into new target groups form the basis for **Accenture's** strong success in the German market for next-gen SOC/MDR services.

Atos

With innovative approaches and the global reach of its next-gen SOC/MDR services, **Atos** ranks among the leading providers in the German market.

axians

With comprehensive, customer-focused services, **Axians IT Security** is successful in the German market for next-gen SOC/MDR services.

BECHTLE

Bechtle impresses its customers with comprehensive, certified, and modularly adaptable next-gen SOC/MDR services, positioning itself as a leader in Germany.

Capgemini

Capgemini's success in the German market for next-gen SOC/MDR services is based on comprehensive services, strong resources, and an international presence.

controlware

Modular, customizable SOC services made in Germany contribute to **Controlware's** success in the German market for next-gen SOC/MDR services.

T

With its comprehensive, advanced next-gen SOC/MDR services, large, qualified team and operations in Germany, **Deutsche Telekom** stands out as a leading provider.

HCLTech

Thanks to powerful, continuously enhanced services and a strong commitment to the German market, **HCLTech** continues to expand its leading position in next-gen SOC/MDR services.

IBM

IBM combines powerful technology with comprehensive, globally available next-gen SOC/MDR services for large, internationally active customers.

InfoGuard
SWISS CYBER SECURITY

Through its high technological dynamism and growing success, **InfoGuard** has risen from Rising Star to a leading provider of next-gen SOC/MDR services in Germany.

Infosys

Infosys has extensive resources and continuously develops its next-gen SOC/MDR services to benefit large enterprise customers, thereby positioning itself as a leader in these services.

orange Cyberdefense

Orange Cyberdefense stands out with its European roots, global and local presence and continuously optimized next-gen SOC/MDR services.

tcs TATA CONSULTANCY SERVICES

A global presence and extensive technology coverage, including OT security, make **TCS** a leader in the German market for next-gen SOC/MDR services.

glueckkanja

glueckkanja is strategically tapping into growth segments, recording strong growth and has thus emerged as the new **Rising Star** in the market for next-gen SOC/MDR services in Germany.

Leader

"With its comprehensive, innovative next-gen SOC/MDR services Made in Germany and its large, qualified team, Deutsche Telekom stands out as a leading provider in Germany."

Frank Heuer

Deutsche Telekom

Overview

Headquartered in Bonn, Germany, Deutsche Telekom employs more than 198,000 people in 50 countries. In FY25, the company generated €119.1 billion in revenue. In 2020, Telekom Security was transformed into a separate legal entity, Deutsche Telekom Security GmbH, within the Deutsche Telekom Group. Deutsche Telekom / T-Systems (hereinafter "Deutsche Telekom") employs more than 2,600 people in the security sector worldwide. The SOC combines machine learning-based artificial intelligence, behavioral analysis and threat hunting. Magenta Security Shield and Magenta Security MDR Pro offer differentiated services.

Strengths

Numerous qualified specialists: In Germany, Deutsche Telekom maintains a large, highly qualified team of experts for its managed security services and offers its customers the same technologies and services that the company uses to protect Deutsche Telekom AG worldwide. As a result, Deutsche Telekom's experts understand the complexities of protecting a global enterprise customer and possess the necessary experience and knowledge to protect customers to the same high standard.

SOC operations in Germany: Deutsche Telekom operates its managed *security services in Germany*, among other locations, and offers Security made in Germany, which is viewed as an advantage in the context of the data protection debate. Deutsche Telekom operates state-of-the-art cyber defense and security operations centers and, as a global carrier, generates extensive threat intelligence. The Telekom Threat Library, a comprehensive database of malware, APT attacks, zero-day exploits and attack patterns, is continuously updated.

Expanding offering: Deutsche Telekom is continuously developing its already comprehensive offering to ensure it can continue to provide a robust portfolio in the future and plans extensive additions; the roadmap lists numerous projects.

Caution

Deutsche Telekom is already highly successful in the managed security services market. By offering a co-managed SOC/MDR service, the company could tap into additional customer groups for whom such a service would be particularly well-suited.

Next-Gen SOC/MDR Services – Midmarket

Who Should Read This Section

This report is valuable for providers offering **next-gen SOC/MDR services (midmarket) in Germany** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence.

Business professionals

Must read this report to gain practical insights into simplifying security operations while maintaining effective risk management. It highlights real-world approaches and solution models that help reduce operational complexity, improve efficiency and enable better alignment between security investments, business priorities and overall organizational performance.

Cybersecurity professionals

Should read this report to understand emerging trends, evolving threat scenarios and near-term risks affecting modern SOC and MDR environments. The insights support strategic security decision-making, help teams prioritize detection and response capabilities and enable improved productivity while reducing operational and architectural security complexity.

Technology professionals

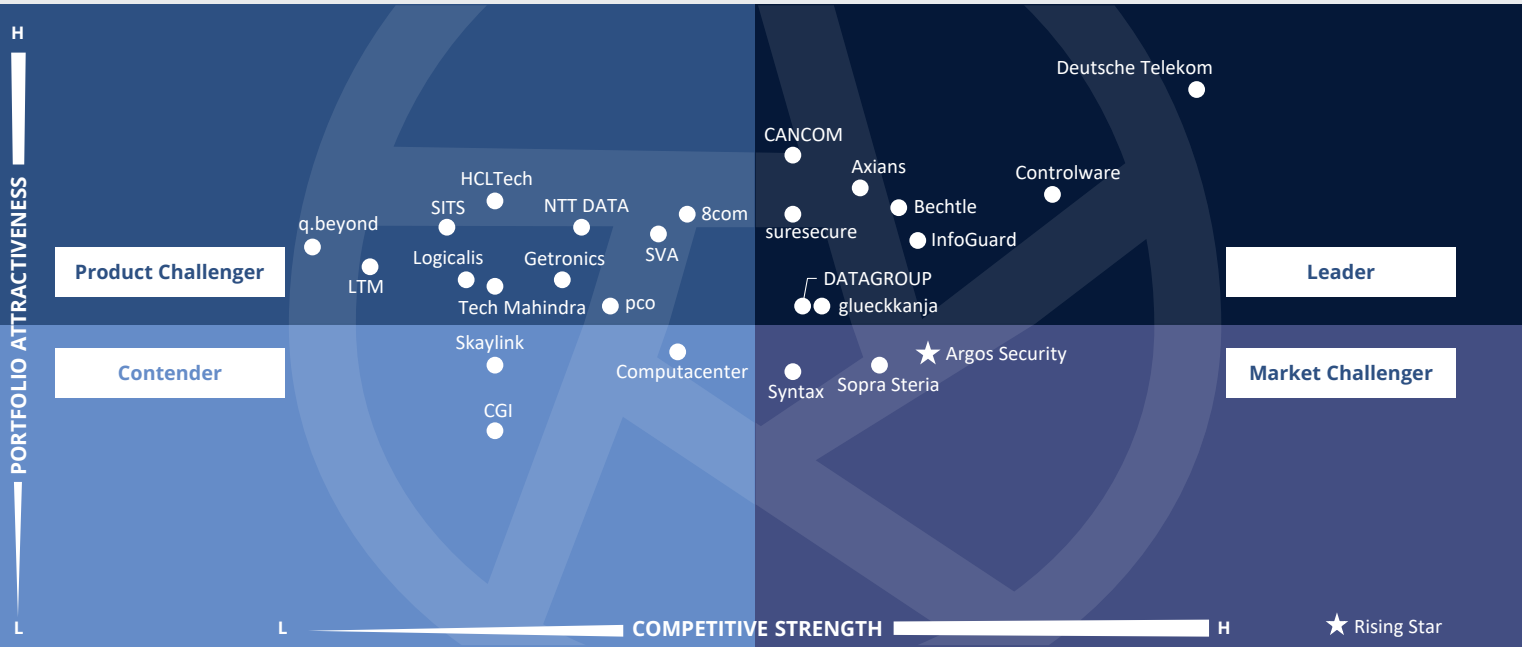
Technology professionals should read this report to gain insights into emerging security trends, next-generation SOC/MDR platforms and the strategic objectives driving their adoption. It helps technology leaders understand how tailored security architectures can integrate with existing IT environments and support scalable, resilient defenses in a rapidly changing security landscape.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC/MDR Services – Midmarket

Germany 2026



This quadrant focuses on the **most relevant** providers of **next-gen SOC/MDR services** for German **SMEs**, excluding providers that only support their own products. Increasing cyberattacks and a shortage of skilled workers are driving **rising demand.**

Frank Heuer

Definition

This quadrant evaluates service providers that deliver continuous monitoring and MDR services through SOCs. Their offerings span the entire incident lifecycle, including detection, triage, investigation, containment and coordinated remediation. Providers integrate and operate modern security technologies, apply threat intelligence and advanced analytics, and deliver human-led and automated threat hunting to strengthen enterprise resilience. Next-gen SOC/MDR services combine managed security operations with innovative AI-driven analytics, autonomous triage and security orchestration, automation and response (SOAR)-based orchestration to reduce response times and improve threat visibility across IT and OT environments. They support co-managed models and do not focus on strategic advisory or technology implementation, which fall within the scope of SSS and TSS, respectively.

In the following, "Managed Services" is used synonymously with "Next-Gen SOC/MDR Services."

Eligibility Criteria

1. **24/7 monitoring, detection, and response services** via proprietary SOCs covering IT and/or OT environments
2. **MDR-specific capabilities,** including behavioral analysis, integration of threat intelligence based on a Large Language Model (LLM), human-led and automated threat hunting, and advanced detection engineering
3. **Operation and management** of Security Information & Event Management (SIEM), SOAR, Endpoint Detection & Response (EDR), Network Detection & Response (NDR), and other relevant security technologies, supported by OEM accreditations
4. Demonstration of a structured **approach to incident response**, including triage, investigation, containment, coordination of remediation efforts, and post-incident improvement
5. Use of **AI-driven** analytics, autonomous triage agents, and SOAR workflows for faster detection and shorter mean time to response (MTTR)
6. **Co-managed service models** that enable shared visibility, collaboration with analysts, and joint response processes
7. **Reference** cases demonstrating measurable improvements in detection coverage, response efficiency, or operational resilience in the target region
8. **No exclusive focus** on proprietary products, but rather management and operational services for best-of-breed security tools

Observations

Demand for next-gen SOC/MDR services is growing even faster in the midmarket segment than in the overall market. Two main factors are driving this trend: Midsize companies in Germany are affected by the cybersecurity skills shortage even more than large enterprises. At the same time, they are also facing an increasing number of increasingly complex security challenges and are now more frequently targeted by cybercriminals who view this demographic as easy prey. Additionally, the NIS 2 Directive has imposed heightened security requirements on many SMEs. As a result, midsize companies are increasingly reliant on external SOC/MDR services.

For the SME segment in Germany, SOCs are a plus due to trust and data protection considerations. German-speaking contacts also play an important role. Many SMEs want their SOC service providers to offer straightforward, rapid onboarding.

SMEs also expect SOC service providers to demonstrate a high level of innovation to stay one step ahead of cybercriminals. This includes, among other things, the use of automation, such as agentic AI, to efficiently manage even more complex threats. For industrial customers, integrating OT security to protect networked manufacturing facilities is becoming increasingly attractive.

glueckkanja has risen to the Leader position this year. The new Rising Star is Argos Security, formed by the merger of the German providers indevis and Data-Sec, and has now taken the place of indevis. 8com, q.beyond, SITS and Skaylink have successfully entered this quadrant.

Of the 71 vendors evaluated in this study specifically for the German market, 26 qualified for this quadrant. Nine of them achieved a Leader position. One vendor was identified as a Rising Star.

axians

With comprehensive and tailored next-gen SOC/MDR services, **Axians IT Security** is able to win over its midmarket customers. This makes the provider one of the leading SOC service providers in Germany.

BECHTLE

With its comprehensive and adaptable services, as well as delivery from Germany, **Bechtle** is a leader in next-gen SOC/MDR services for German SMEs.

CANCOM

CANCOM precisely addresses the needs of small and midsize businesses in the German market for next-gen SOC/MDR services, including with regard to data sovereignty.

controlware

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

DATAGROUP

DATAGROUP stands out in the market for SOC services for German SMEs with high-quality, integrated services.

With a large team and a comprehensive range of *made-in-Germany* offerings, **Deutsche Telekom** is the leading provider of next-gen SOC/MDR services for German SMEs.

glueckkanja

glueckkanja is experiencing strong growth and is thus establishing itself as one of the leading providers of next-gen SOC/MDR services in the German SME segment.

InfoGuard
SWISS CYBER SECURITY

Following the acquisition of Com-Sys, **InfoGuard** has significantly strengthened and expanded its position in the market for next-gen SOC/MDR services in the SME segment in Germany.

sure[secure]

suresecure has successfully established itself as an innovative and leading provider of SOC services in the German SME market.

Argos Security

Argos Security, through the merger of indevis and Data-Sec, is the new **Rising Star** in the market for next-gen SOC/MDR services for German SMEs.

Leader

"With Security made in Germany and an innovative offering delivered by highly qualified staff, Deutsche Telekom positions itself as a leading provider of SOC/MDR services for German SMEs."

Frank Heuer

Deutsche Telekom

Overview

Headquartered in Bonn, Germany, Deutsche Telekom employs more than 198,000 people in 50 countries. In FY25, the company generated €119.1 billion in revenue. In 2020, Telekom Security was transformed into a separate legal entity, Deutsche Telekom Security GmbH, within the Deutsche Telekom Group. Deutsche Telekom / T-Systems (hereinafter "Deutsche Telekom") employs more than 2,600 people in the security sector worldwide. The SOC combines machine learning-based artificial intelligence, behavioral analysis and threat hunting.

Strengths

Services from Germany: Deutsche Telekom offers Security made in Germany and provides its managed security services in Germany, among other locations, a fact particularly appreciated by many SMB customers. The provider operates state-of-the-art cyber defense and security operations centers. With Security made in Germany, Deutsche Telekom scores points, especially in light of the data protection debate and particularly among the SMB target group. In the fall of 2024, Deutsche Telekom opened its new SOC in Bonn.

Large, highly qualified team: Deutsche Telekom maintains a very large, highly qualified team of experts in Germany for its managed security services and offers its customers the same services and technologies that the company uses to protect Deutsche Telekom AG worldwide. Deutsche Telekom's experts therefore understand the challenges involved in protecting corporate customers and have the necessary knowledge and experience to protect customers to the same high standard.

Extensive, growing portfolio: To ensure it can continue offering a robust portfolio in the future, Deutsche Telekom is continuously expanding its already very comprehensive range of services and plans further extensive additions to the portfolio; the roadmap lists numerous projects.

Caution

Overall, Deutsche Telekom is very successful in the SME segment. Its primary focus is on upper-midmarket customers. By placing a stronger emphasis on the segment below this, Deutsche Telekom could be even more successful due to the above-average growth in demand there.

Post-Quantum Encryption Consulting

Who Should Read This Section

This report is valuable for providers offering **post-quantum encryption consulting in Germany** to understand their market position and for enterprises evaluating these providers. In this quadrant, ISG highlights the current market positioning of these firms based on the depth of their cryptography-focused capabilities, their readiness for post-quantum cryptography (PQC) adoption and their overall market presence.

Business professionals

Should read this report to gain insights into the strategic importance of transitioning to post-quantum-ready encryption. It helps them understand the implications of PQC on risk mitigation, long-term data protection and compliance, while offering clarity on how consulting partners can simplify the shift and support secure digital transformation.

Cybersecurity professionals

Should read this report to understand emerging trends, risks and mitigation strategies associated with post-quantum threats. It supports informed decision-making on cryptographic modernization, highlights provider strengths and enables teams to enhance resilience, streamline complex security operations and prepare for a quantum-safe future.

Technology professionals

Should read this report to learn about evolving encryption standards, PQC migration frameworks and the tooling required to support quantum-safe architectures. It provides clarity on vendor capabilities, integration approaches and best practices that can help teams align modernization priorities with the fast-changing security landscape.

IT and digital transformation leaders

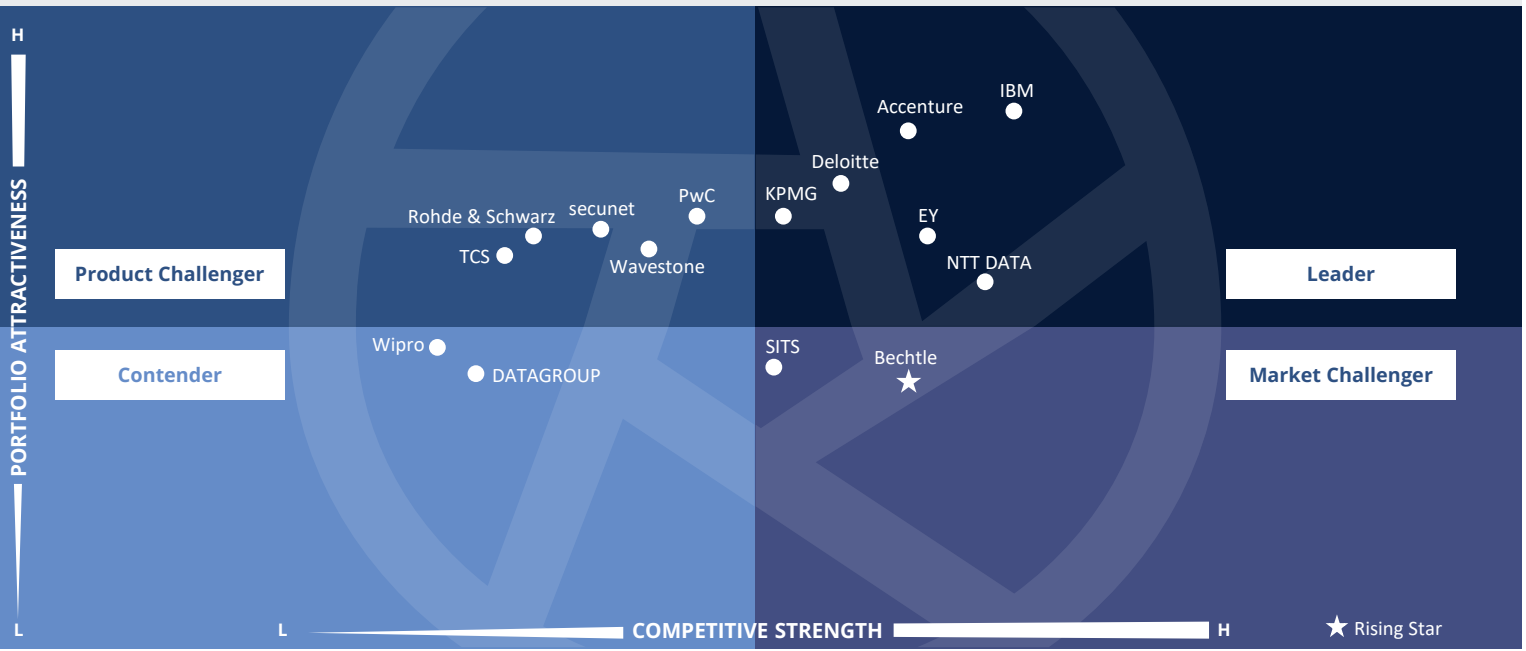
Should read this report to understand how post-quantum encryption consulting services can support long-term security planning. The analysis helps them evaluate providers' expertise in assessment, roadmap development and implementation, enabling more informed decisions as they prepare infrastructure and applications for a quantum-resilient environment.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Post-Quantum Encryption Consulting

Germany 2026



This quadrant focuses on the **most relevant** providers of post-quantum encryption consulting in Germany who offer services **beyond their own products**. Harvest Now, Decrypt Later makes this an **urgent** issue.

Frank Heuer

Post-Quantum Encryption Consulting

Definition

This quadrant evaluates consulting-led service providers that assist enterprises in preparing for and executing the cryptographic transition required to mitigate risks associated with quantum computing. These providers assess cryptographic dependencies across the IT, OT, IoT and digital supply chain environments, including inventory management, identification of quantum-vulnerable algorithms and exposure to harvest now, decrypt later threats. They develop risk-based post-quantum cryptography (PQC) strategies, design migration and hybrid cryptographic roadmaps, and advise on the adoption of emerging post-quantum standards aligned with the National Institute of Standards and Technology (NIST), Federal Office for Information Security (BSI) and other regulatory bodies. PQC consulting addresses the impacts on key management, identity systems, communications, applications and infrastructure architectures, enabling organizations to plan for compliant, scalable and future-resilient cryptographic transformations.

Eligibility Criteria

1. Conducting **cryptographic and quantum risk assessments**, including the inventory of cryptographic assets, algorithms, and key usage in IT, OT, IoT, cloud, network, and application environments
2. Proven **consulting expertise in the development of PQC strategies**, including phased migration plans, hybrid cryptography planning, and dependency analyses
3. Availability of consulting services in accordance with **new standards and guidelines** such as NIST PQC, BSI TR-02102, the European Telecommunications Standards Institute (ETSI), and relevant ISO/IEC requirements
4. Assessment of **the impact on key management**, Public Key Infrastructure (PKI), identity and access systems, secure communication, and application architectures
5. Proven **PQC-related client engagements in Germany**, pilots, simulations, or proofs of concept addressing quantum-based risk mitigation
6. **Vendor-neutral consulting** services with proven expertise in relevant technology ecosystems and cryptographic implementations
7. **Support in complying** with government regulations and meeting the objectives of industry-specific or national cryptographic transition initiatives

Observations

With its groundbreaking capabilities, emerging quantum technology poses a significant threat to existing encryption of sensitive data. Quantum computers are expected to become commercially available toward the end of this decade or the beginning of the next.

However, the new strategies of cybercriminals often no longer allow for waiting until this Q-Day. With the Harvest Now, Decrypt Later approach, the threat has become immediate. This primarily affects companies whose existence depends heavily on data, such as banks and insurance companies. Consequently, these industries in particular are already seeking advice on the best defense strategies.

As Q-Day approaches, other industries and a wider range of companies will increasingly begin to address this issue. Consequently, even at this early stage of market development, the consulting market for post-quantum encryption is gradually beginning to differentiate itself across various target groups.

In this early market phase, the focus is primarily on consulting services for threat analysis, including consideration of regulatory requirements and the inventory of potentially compromised data. Soon, there will also be significantly greater demand for plans for concrete action and implementation services.

Of the 71 providers evaluated in this study specifically for the German market, 15 qualified for this quadrant. Six of these achieved a position as Leaders. One provider was identified as a Rising Star.

accenture

Accenture impresses at the C-level with comprehensive expertise and clear strategic recommendations on post-quantum encryption, positioning itself as a leading consultant in this field in Germany.

Deloitte.

In its post-quantum encryption consulting, **Deloitte** combines regulatory expertise with sound risk assessment, making it one of the leading providers in the German market.

EY

EY distinguishes itself in post-quantum encryption consulting through a risk-oriented, regulatory-aligned consulting model, making it one of the leading service providers in Germany.

IBM

IBM is a pioneer in quantum computer development and a trailblazer and leading consultant in the field of post-quantum encryption in Germany.

KPMG

KPMG positions itself as a leading provider of post-quantum encryption consulting in the German market through its combination of strategic, regulatory and transformation expertise.

NTT DATA

With a comprehensive, vendor-neutral portfolio, **NTT DATA** is already successfully established in Germany's post-quantum encryption consulting market and is positioned as a leading provider.

BECHTLE

Bechtle is experiencing strong growth, anticipates expansion in the future market of post-quantum encryption consulting, and thus qualifies as a **Rising Star** in Germany.

Data Leakage/Loss Prevention (DLP) and Data Security

Who Should Read This Section

This report is valuable for vendors offering **data leakage/loss prevention (DLP) and data security in Germany** to understand their market position and for enterprises looking to evaluate these vendors. In this quadrant, ISG highlights the current market positioning of these vendors based on the depth of their solution offerings and market presence.

IT security professionals

Should read this report to understand the current state of the DLP and data security market in Germany. It provides insights into vendor capabilities, service depth, and market positioning, along with emerging trends, innovative features, and best practices. The report helps practitioners benchmark solutions, identify strengths and gaps, and design effective data protection strategies aligned with evolving threat landscapes.

Chief Information Security Officers (CISOs)

Should read this report to gain a strategic view of the evolving DLP landscape in Germany. It supports informed decision-making by highlighting leading providers, solution maturity and market presence. CISOs can use these insights to prioritize investments, align DLP initiatives with business and risk objectives and strengthen organizational resilience against data leakage and regulatory exposure.

Compliance officers

Responsible for data protection and regulatory adherence should read this report to understand how DLP solutions support compliance with German and EU data protection requirements. The report explains how provider capabilities address data visibility, control and reporting needs, helping organizations reduce compliance risk, demonstrate accountability and maintain ongoing adherence to data privacy and security regulations.

ISG Provider Lens®

Source: ISG RESEARCH

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

Germany 2026

This section evaluates the **most relevant** DLP providers in Germany that offer or operate proprietary **software**. The intensified **discussion on data protection** and the safeguarding **of intellectual property** contribute to the market's significance.

Frank Heuer

Data Leakage/Loss Prevention (DLP) and Data Security

Definition

This quadrant evaluates independent software vendors (ISVs) that develop proprietary DLP and data security solutions delivered as on-premises software, cloud platforms or SaaS. These products enable the discovery, classification and monitoring of sensitive data across endpoints, networks, cloud services and storage systems and apply policy-based controls to prevent unauthorized access or exfiltration. Modern DLP technologies increasingly integrate device hardening, application control and behavioral analytics to prevent data misuse at the endpoints and enforce policies even in offline or unmanaged environments. They provide centralized governance, reporting and compliance support to protect structured and unstructured data throughout its lifecycle. In a distributed IT landscape with heightened risks of insider and data flow breaches, these solutions form the core safeguard for protecting critical information assets and ensuring consistent data handling practices.

Eligibility Criteria

1. Provision of a **proprietary DLP or data security product** (no embedded third-party DLP engines)
2. **Support for core architectures** such as endpoint, network, cloud, and storage environments
3. **Detection, classification, and protection** of structured and unstructured data at rest and in transit
4. **Centralized management capabilities**, including policy control, reporting, and configuration
5. Data **discovery**, real-time **monitoring**, and policy-based **enforcement**
6. **Proven** enterprise-level implementations and documented customer adoption

Observations

Numerous factors are contributing to the growing importance of DLP solutions. Data has become an increasingly important, and in some cases, existentially critical, corporate asset. The enormous growth in corporate data requires powerful DLP solutions that can quickly identify and classify data and protect it from unauthorized actions in accordance with its protection requirements. With the General Data Protection Regulation (GDPR) and the NIS 2 Directive, the importance of data protection in companies has further increased.

The diversity of data storage locations requires consistent data protection across all of them. The increasing business use of personal devices poses a particular challenge in terms of protection against unwanted data leaks, as these devices often elude configuration and control by corporate administration and, in some cases, cannot be comprehensively monitored by the company for legal reasons.

Cloud storage solutions and apps can result in data unintentionally leaving the corporate network during processing.

Social media and communication platforms open up communication channels through which data can leak; added to this are the risks associated with data transfers via email.

Data can leak not only unintentionally but also due to internal negligence; companies must also be able to protect themselves against dishonest behavior by internal stakeholders.

AI is increasingly helping to address these challenges. Data-centric security, that is, the direct protection of data during its use, sharing and storage, is growing in importance.

Last year's Rising Star, ManageEngine, has risen to the rank of Leader this year.

Of the 71 vendors evaluated in this study specifically for the German market, 23 qualified for this quadrant. Nine of them achieved a Leader position.

Broadcom

Broadcom combines performance with ease of management and great flexibility, positioning itself as a leading provider of DLP solutions in Germany.

DriveLock

The German DLP provider **DriveLock** builds trust through its commitment to *Made in Germany* and *No Backdoor* and efficiently supports its customers in compliance throughout the entire data lifecycle, including in the cloud.

Forcepoint

Forcepoint helps users simplify DLP through advanced solutions, rapid incident response and data protection compliance.

Fortra

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

GBS

The German DLP provider **GBS** ensures secure communication and collaboration through sophisticated technology and the dual-control principle while keeping business processes unaffected.

IBM

With Guardium, **IBM** offers a comprehensive, flexible DLP solution that is expertly and forward-looking, supported by AI and post-quantum encryption.

ManageEngine

Thanks to strong growth, **ManageEngine** has risen from a Rising Star to a Leader in the German DLP solutions market, driven by easier compliance, simplification through automation and unified analytics.

Microsoft

Through support for comprehensive data protection and strategic marketing, such as integration and bundling, **Microsoft** is expanding its leadership position in the German DLP market with Purview.

Trellix

A comprehensive solution for a wide variety of data types and a broad market reach in Germany make **Trellix** a leading provider of data loss/leakage prevention in Germany.

Appendix

Methodology & Team

The market research study "ISG Provider Lens® 2026 Cybersecurity — Services and Solutions" analyzes the relevant software vendors and service providers in the German market based on a multi-stage market research and analysis process and positions these providers using the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Author:
Frank Heuer

Editor:
Maria Müller-de Haen

Research Analyst:
Monica K

Data Analysts:
Rajesh Chillappagari and Laxmi Sahebrao

Consultant Advisor:
Marco Ezzy

Project Manager:
Smita S M

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.

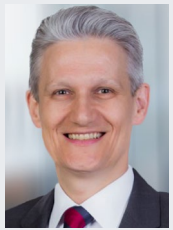
The research and analysis presented in this report includes research from the ISG Provider Lens® program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. The data collected for this report represent information that ISG believes to be current as of May 2026 for providers that actively participated and for providers that did not. ISG recognizes that many mergers and acquisitions may have occurred since then, but this report does not reflect these changes.

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

The study was conducted in the following steps:

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

Author



Frank Heuer
Principal Analyst

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

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

Enterprise Context and Global overview analyst

Monica K
Research Analyst

Monica K is a Manager and Lead Research Specialist at ISG, where she also serves as a digital expert. She co-authors Provider Lens® studies, the global summary report, and the enterprise perspective for the cybersecurity, ESG, and sustainability markets. Her responsibilities include managing comprehensive research projects and collaborating with internal stakeholders on diverse consulting initiatives.

With over a decade of experience in technology, business, and market research,Monica brings valuable expertise to ISG clients. Previously, she worked at a research firm specializing in IoT, product engineering, vendor profiling, and talent intelligence.

Study Sponsor

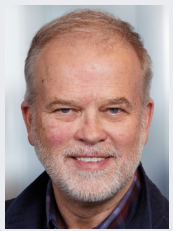
Heiko Henkes

Director & Principal Analyst, Global IPL Content Lead

Heiko Henkes serves as Managing Director and Principal Analyst at ISG, where he oversees the Global ISG Provider Lens® (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as strategic program manager and thought leader for IPL Lead Analysts. Additionally, Henkes heads the Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice.

His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation, IT competencies, sustainable business strategies, and change management in a Cloud-AI-driven business landscape. Henkes is renowned for his contributions as a keynote speaker on digital innovation, where he shares insights on leveraging technology for business growth and transformation.

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens®

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

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

ISG Provider Lens®

The ISG Provider Lens® Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners. 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 and cities) and higher education institutions. Visit: Public Sector.

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

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth.

The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.

For more information, visit isg-one.com.

ISG Provider Lens®

JUNE, 2026

REPORT: CYBERSECURITY — SERVICES AND SOLUTIONS