ISG Provider Lens™

Cyber Security - Solutions & Services

Germany 2020

A research report comparing provider strengths, challenges and competitive differentiators

Quadrant Report

Customized report courtesy of:

T··Systems·

August 2020

About this Report

Information Services Group Inc. assumes responsibility for the content of this report. Unless otherwise noted, all content included in this report, including illustrations, research, conclusions, statements and positions, has been developed by Information Services Group Inc. and is the sole property of Information Services Group Inc.

The market research and analysis data presented in this report includes research information from the ISG Provider Lens™ program and from ongoing ISG research programs, discussions with ISG advisors, briefings with service providers and analysis of publicly available market information from various sources. The data compiled in this report is based on information last updated on 27th February 2020 - 30th April 2020. Interim mergers and acquisitions and the related changes are not included in this report

The main author of this report is Frank Heuer. The editor is Heiko Henkes

The Business Context Analyst and Global Vision Analyst is Ron Exler. The Research Analyst is Monica K and the Data Analyst is Kankaiah Yasareni.

ISG Provider Lens™

ISG Provider Lens™

ISG Provider Lens™ delivers leading-edge and actionable research studies, reports and consulting services focused on technology and service providers' strengths and weaknesses and how they are positioned relative to their peers in the market. These reports provide influential insights accessed by our large pool of advisors who are actively advising outsourcing deals as well as large numbers of ISG enterprise clients who are potential outsourcers.

For more information about our studies, please email ISGLens@isg-one.com, call +49 (0) 561-50697537, or visit ISG Provider Lens™ under ISG Provider Lens™.

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.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +49 (0) 561-50697537 or visit research.isg-one.com.

EXECUTIVE SUMMARY

General Trends

Within the scope of digitization and the industrial Internet of Things (IoT), business processes are increasingly being shifted to IT. With the growing need to ensure the protection of IT and communication systems in companies, IT security has been transformed into company security.

Data and IT infrastructures are constantly exposed to criminal threats. Hazards emerging from negligence in user companies are not uncommon. In addition to self-protection, legal regulations such as the basic Data Protection Regulation (DSGVO) in the EU force companies to implement stronger security measures to prevent cyber-attacks. The current COVID-19 crisis also poses a challenge for IT security, as the increased use of the home office and the resulting external connections of employees make IT systems more vulnerable.

IT security has thus emerged as an important topic. However, IT managers often struggle with the task of legitimizing investments in IT security vis-à-vis company stakeholders, especially the CFO. Unlike other IT projects, it is not always possible to prove the return on investment in this case, nor is it easy to quantify threat risks. Therefore, security measures often remain on low priority and are not always sufficient to counter advanced threats.

On the other hand, the problem is often not solely on the technical side; several attacks, such as Trojan and phishing attacks, can be attributed to careless behavior by users. In addition to modern IT security equipment, consultation and user training continues to play an important role in this regard.

Identity and access management (IAM)

After a period of average demand development, identity and access management (IAM) has been revived as an important security topic and will continue to play a major role in the future. The main reason is that the increasing digitalization of all areas drive the need to protect not only users and their identities, but also machines and certain areas of the company (keyword: Industry 4.0).

The software market as a whole is also witnessing a shift from on-premise operations to the cloud with respect to IAM solutions. Most providers have adapted to this transformation and offer both on-premise and cloud operation (identity as a service). Cloud-native companies are also emerging rapidly, while bundling and integration are playing a more important role.

In the course of this supplier investigation, 22 companies have been identified as relevant manufacturers in the IAM market in Germany, of which 5 were positioned as Leaders.

Data leakage/loss prevention, data security

Interest in data loss prevention (DLP) solutions has increased significantly in recent years. Various factors contribute to this, affecting the security of data in a company. The increased business use of private end devices poses a challenge in defending against undesired data outflows. In addition to the mobility and variety of functions for end devices, IT trends of big data, social business and cloud computing make it difficult to control data movements and place high demand on DLP solutions.

In the course of this supplier investigation, 25 companies have been identified as relevant manufacturers in the DLP market in Germany and 10 of them were able to position themselves as Leaders.

Strategic security services

Companies are facing various challenges concerning IT security and data protection. The increase in cyber risks, coupled with the lack of resources, drives the need for orientation around these topics. In addition, regulatory requirements on data security and data protection are increasingly enforced.

Owing to their complex IT (security) landscapes and projects, large companies are still among the main customers for strategic security services. However, even mid-tier companies are increasingly using these services owing to the lack of specialist staff and the need to keep pace with modern security systems.

In the course of this supplier investigation, 27 companies were identified as relevant service providers of strategic security services in Germany and 10 of them were able to position themselves as Leaders.

Technical security services

Companies are relying more on external service providers to keep their IT security systems up to date. Careless behavior on behalf of users is also taken advantage of by cyber criminals, for e.g., in the case of Trojan and phishing attacks. In addition to modern security equipment, training for users continues to play an important role.

IT security projects are often demanding and diverse. This is why service providers that offer a wide range of technical security services from a single source and address numerous IT security solutions have an advantage. Those that cooperate with renowned technology providers and have employees with numerous high-quality certifications can also set themselves apart.

In order to be successful in the demanding technical security services market for large customers, providers should demonstrate extensive and international experience in this market segment with a broad range of solutions. Teams that are strong and internationally represented should be available to provide support. Mid-tier companies often appreciate the local presence of service providers for their proximity and reliable support.

Owing to their complex IT (security) landscapes and projects, large companies are still among the most important customers for Technical Security Services. However, even mid-tier companies are making increasing use of these services and are, therefore, a target group with above-average market growth.

In this study, 22 companies have been identified as relevant service providers of technical security services in Germany and 11 of them were able to position themselves as Leaders.

Managed security services

Scarce qualified resources, high frequency of security incidents and their growing sophistication, as well as the necessary up-to-date specialist knowledge contribute to the rise in demand for managed security services.

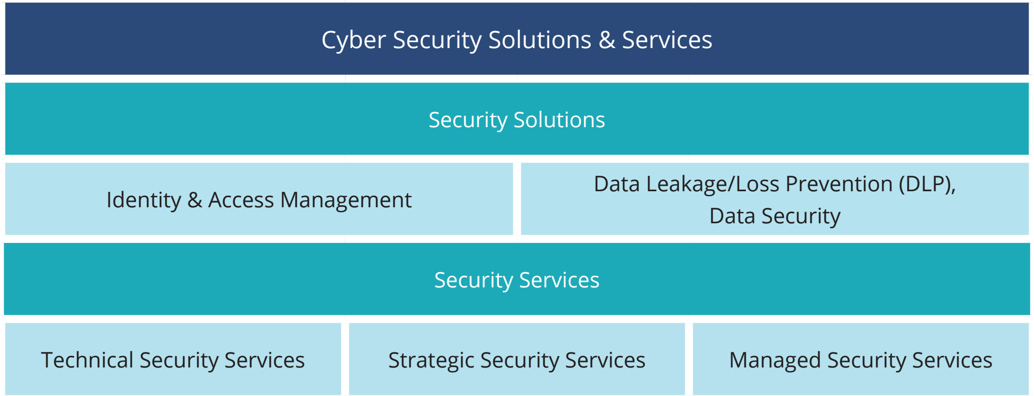
Large and mid-tier customers are turning towards security operations centers (SOCs) based in Germany due to the growing need for data protection. Moreover, it is important for both target groups to ensure the reliability of managed security services and a high level of innovation in order to stay a step ahead of cyber-criminals. This includes the expansion of SOCs towards Cyber Defense Centers.

For large companies, globally distributed SOCs play a special role due to their growing international presence. Owing to their complex IT security systems, large companies also give importance to a broad range of security topics that are covered by managed security services providers. German-speaking contacts play an important role in SOCs, especially for mid-tier customers.

In this report, 25 companies were identified as relevant manufacturers in the managed security services market in Germany. Ten of them were able to position themselves as Leaders.

Introduction

Simplified Illustration



Cyber Security Solutions & Services

Security Solutions

Identity & Access Management

Data Leakage/Loss Prevention (DLP), Data Security

Security Services

Technical Security Services

Strategic Security Services

Managed Security Services

Source: ISG 2020

Definition

This study examines five subject areas in the cyber security market in Germany. It is focused on creating a distinction between security solutions and security services. In this study, security solutions cover software and cloud services, based on proprietary software, from product providers.
The topics considered are identity & access management (IAM) and data leakage/loss prevention (DLP). Security services for security solutions include strategic security services, technical security services and managed security services.

Definition (cont.)

Scope of the Report

The ISG Provider Lens™ Cyber Security - Solutions & Services 2020 study aims to support IT decision makers in making the best use of their limited IT security budgets.

The ISG Provider Lens™ study offers the following to IT decision-makers:

- Transparency about the strengths and weaknesses of the providers
- Differentiating positioning of providers according to market segments
- Focus on local markets (in this case on the German market; further studies in the current wave deal with the U.S., Brazil, Great Britain, France, Switzerland and Australia)

This study serves as an important basis for decision making on positioning, building key relationships and go-to-market planning. ISG consultants and corporate customers also use the information from ISG Provider Lens™ report to assess their current supplier relationships and the potential to build new relationships.

The five security topics examined in this study are defined as follows:

Identity & Access Management (IAM): IAM products are used to capture, record and manage user identities and the associated access authorizations. These products ensure that access rights are granted in accordance with defined guidelines. In order to deal with existing and new requirements of applications, security providers are increasingly required to incorporate mechanisms, frameworks and automation (for e.g., risk assessment) into their management suites, enabling them to carry out real-time user profiling and attack profiling. The influence of social media and mobile users imposes additional requirements to cover the security needs of customers, which was previously the case with web-related and context-related authorization management. This category also includes cloud services from product providers.

Data leakage prevention/Loss Prevention (DLP), Data Security: DLP products are used for the identification and monitoring of sensitive data, ensuring that it is only accessible to authorized users and that there are no data leaks. These products are becoming increasingly important as the control of data movement and transfer is becoming more difficult for companies. The number

Definition (cont.)

of (mobile) end devices in companies on which data can be stored is growing. These end devices usually have their own connection to the Internet, allowing data to be sent and received without using the central Internet gateway. In addition, the end devices have a variety of interfaces (such as USB, Bluetooth, WLAN, NFC) through which data can also be exchanged. This category also includes cloud services from product providers.

Strategic Security Services: This quadrant primarily covers consultation for IT security solutions. It examines service providers that have no exclusive focus on in-house products or solutions.

Technical Security Services: These services mainly cover integration, maintenance and support of IT security solutions. This quadrant examines service providers that do not have an exclusive focus on their respective in-house products and are able to implement and integrate dealer solutions.

Managed Security Services: Managed security services include the operation and management of IT security infrastructures for one or more customers through a security operations center (SOC). Typical services include security monitoring, behavior analysis, recording of unauthorized access, advice on preventive measures, penetration tests, firewall operation, anti-virus operation, IAM operation, DLP operation and other (operational) services in order to guarantee constant protection in real time without loss of performance. This category considers service providers that are not exclusively focused on in-house products but can manage best-of-breed security tools. They can handle the entire life cycle of a security incident, from identification to resolution.

Provider Classifications

The ISG Provider Lens™ quadrants were created using an evaluation matrix containing four segments, where the providers are positioned accordingly.

Leader

The Leaders among the vendors/providers have a highly attractive product and service offering and a very strong market and competitive position; they fulfill all requirements for successful market cultivation. They can be regarded as opinion leaders, providing strategic impulses to the market. They also ensure innovative strength and stability.

Product Challenger

The Product Challengers offer a product and service portfolio that provides an above-average coverage of corporate requirements, but are not able to provide the same resources and strengths as the Leaders regarding the individual market cultivation categories. Often, this is due to the respective vendor's size or their weak footprint within the respective target segment.

Market Challenger

Market Challengers are also very competitive, but there is still significant portfolio potential and they clearly lag behind the Leaders. Often, the Market Challengers are established vendors that are somewhat slow to address new trends, due to their size and company structure, and therefore have some potential to optimize their portfolio and increase their attractiveness.

Contender

Contenders are still lacking mature products and services or sufficient depth and breadth of their offering, while also showing some strengths and improvement potentials in their market cultivation efforts. These vendors are often generalists or niche players.

Provider Classifications (cont.)

Each ISG Provider Lens™ quadrant may include a service provider(s) who ISG believes has a strong potential to move into the leader's quadrant.

Rising Star

Rising Stars are usually Product Challengers with high future potential. Companies that receive the Rising Star award have a promising portfolio, including the required roadmap and an adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market. This award is only given to vendors or service providers that have made extreme progress towards their goals within the last 12 months and are on a good way to reach the leader quadrant within the next 12 to 24 months, due to their above-average impact and innovative strength.

Not In

This service provider or vendor was not included in this quadrant as ISG could not obtain enough information to position them. This omission does not imply that the service provider or vendor does not provide this service. In dependence of the market ISG positions providers according to their business sweet spot, which can be the related midmarket or large accounts quadrant.

Cyber Security - Solutions & Services - Quadrant Provider Listing 1 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	● Not In	● Contender	● Not In	● Not In	● Not In
Accenture	● Not In	● Not In	● Leader	● Leader	● Leader
All for One	● Not In	● Not In	● Not In	● Market Challenger	● Not In
All for One Group	● Not In	● Not In	● Market Challenger	● Not In	● Not In
Atos	● Leader	● Not In	● Leader	● Leader	● Leader
Axians	● Not In	● Not In	● Leader	● Product Challenger	● Leader
Bechtle	● Not In	● Not In	● Leader	● Market Challenger	● Leader
Beta Systems	● Product Challenger	● Not In	● Not In	● Not In	● Not In
Brainloop	● Not In	● Product Challenger	● Not In	● Not In	● Not In
Broadcom	● Not In	● Leader	● Not In	● Not In	● Not In
Broadcom	● Product Challenger	● Not In	● Not In	● Not In	● Not In
BT	● Not In	● Not In	● Not In	● Not In	● Not In
CANCOM	● Not In	● Not In	● Leader	● Market Challenger	● Leader
Capgemini	● Not In	● Not In	● Leader	● Leader	● Leader
CenturyLink	● Not In	● Not In	● Not In	● Not In	● Product Challenger

Cyber Security - Solutions & Services - Quadrant Provider Listing 2 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
CGI	● Not In	● Not In	● Product Challenger	● Product Challenger	● Contender
Clearswift	● Not In	● Market Challenger	● Not In	● Not In	● Not In
Cognizant	● Not In	● Not In	● Contender	● Product Challenger	● Contender
Computacenter	● Not In	● Not In	● Leader	● Leader	● Product Challenger
Controlware	● Not In	● Not In	● Leader	● Market Challenger	● Product Challenger
CoSoSys	● Not In	● Market Challenger	● Not In	● Not In	● Not In
DELL/RSA	● Leader	● Not In	● Not In	● Not In	● Not In
Deloitte	● Not In	● Not In	● Product Challenger	● Leader	● Product Challenger
Deutsche Telekom	● Not In	● Not In	● Leader	● Not In	● Leader
DeviceLock	● Not In	● Product Challenger	● Not In	● Not In	● Not In
Digital Guardian	● Not In	● Product Challenger	● Not In	● Not In	● Not In
DriveLock	● Not In	● Leader	● Not In	● Not In	● Not In
DXC	● Not In	● Not In	● Leader	● Leader	● Product Challenger
econet	● Product Challenger	● Not In	● Not In	● Not In	● Not In
EY	● Not In	● Not In	● Not In	● Leader	● Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 3 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Fidelis Cybersecurity	● Not In	● Contender	● Not In	● Not In	● Not In
Forcepoint	● Not In	● Leader	● Not In	● Not In	● Not In
ForgeRock	● Product Challenger	● Not In	● Not In	● Not In	● Not In
Fortinet	● Contender	● Not In	● Not In	● Not In	● Not In
GBS	● Not In	● Leader	● Not In	● Not In	● Not In
HCL	● Not In	● Not In	● Product Challenger	● Product Challenger	● Product Challenger
IBM	● Leader	● Leader	● Leader	● Leader	● Leader
Infosys	● Not In	● Not In	● Contender	● Contender	● Not In
itWatch	● Not In	● Product Challenger	● Not In	● Not In	● Not In
KPMG	● Not In	● Not In	● Not In	● Leader	● Not In
Matrix42	● Not In	● Leader	● Not In	● Not In	● Not In
McAfee	● Not In	● Leader	● Not In	● Not In	● Not In
Micro Focus	● Product Challenger	● Not In	● Not In	● Not In	● Not In
Microsoft	● Leader	● Leader	● Not In	● Not In	● Not In
MobileIron	● Not In	● Leader	● Not In	● Not In	● Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 4 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Netskope	Not In	Product Challenger	Not In	Not In	Not In
NEVIS	Product Challenger	Not In	Not In	Not In	Not In
Nexus	Product Challenger	Not In	Not In	Not In	Not In
NTT	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Okta	Leader	Not In	Not In	Not In	Not In
One Identity	Contender	Not In	Not In	Not In	Not In
OneLogin	Product Challenger	Not In	Not In	Not In	Not In
OpenText	Not In	Product Challenger	Not In	Not In	Not In
Oracle	Market Challenger	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Market Challenger	Market Challenger	Leader
Ping Identity	Product Challenger	Not In	Not In	Not In	Not In
Proofpoint	Not In	Market Challenger	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Leader	Not In
SailPoint	Product Challenger	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 5 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Saviynt	● Product Challenger	● Not In	● Not In	● Not In	● Not In
Secureworks	● Not In	● Not In	● Not In	● Product Challenger	● Product Challenger
Solarwinds	● Contender	● Not In	● Not In	● Not In	● Not In
Sopra Steria	● Not In	● Not In	● Not In	● Market Challenger	● Leader
TCS	● Not In	● Not In	● Product Challenger	● Product Challenger	● Product Challenger
Thales/Gemalto	● Product Challenger	● Not In	● Not In	● Not In	● Not In
Trend Micro	● Not In	● Leader	● Not In	● Not In	● Not In
Trustwave	● Not In	● Product Challenger	● Not In	● Not In	● Product Challenger
Unisys	● Not In	● Not In	● Market Challenger	● Market Challenger	● Market Challenger
Varonis	● Not In	● Product Challenger	● Not In	● Not In	● Not In
Verizon	● Not In	● Not In	● Not In	● Product Challenger	● Product Challenger
WatchGuard	● Not In	● Product Challenger	● Not In	● Not In	● Not In
Wipro	● Not In	● Not In	● Product Challenger	● Product Challenger	● Product Challenger
Zscaler	● Not In	● Contender	● Not In	● Not In	● Not In

Cyber Security - Solutions & Services Quadrants

ENTERPRISE CONTEXT

Identity & Access Management

This report is relevant to enterprises across all industries in Germany for evaluating providers of legacy and cloud-native identity and access management (IAM) tools.

In this quadrant report, ISG lays out the current market positioning of IAM providers in Germany, and how they address the key challenges enterprises face in the region. In the past few years, some providers have augmented their product strategy to go beyond legacy IAM solutions to cloud-native solutions. At the same time, some leading providers only offer cloud-native solutions. ISG observes a market separation of the approaches so that they sometimes compete for the same enterprise business. Meanwhile, enterprise requirements for IAM expand with an increasing number of devices being connected to enterprise networks with the Internet of Things (IoT) and other digital transformation initiatives.

Manufacturing is a critical industry in Germany, so security is important but with a unique set of access points. Germany is a maturing security market compared to other regions and IAM is growing as securing identifications continues to be important. The addition of new non-personal identities needing access emerge via robotic process automation (RPA) and the IoT. With the COVID-19 pandemic, and the shift to working from anywhere, has changed the way enterprise employees and contractors access corporate systems for collaboration and file access.

IT and technology leaders should read this report to understand the relative positioning and capabilities of IAM solutions. The report also shows how service providers' technical capabilities compare with the rest in the market.

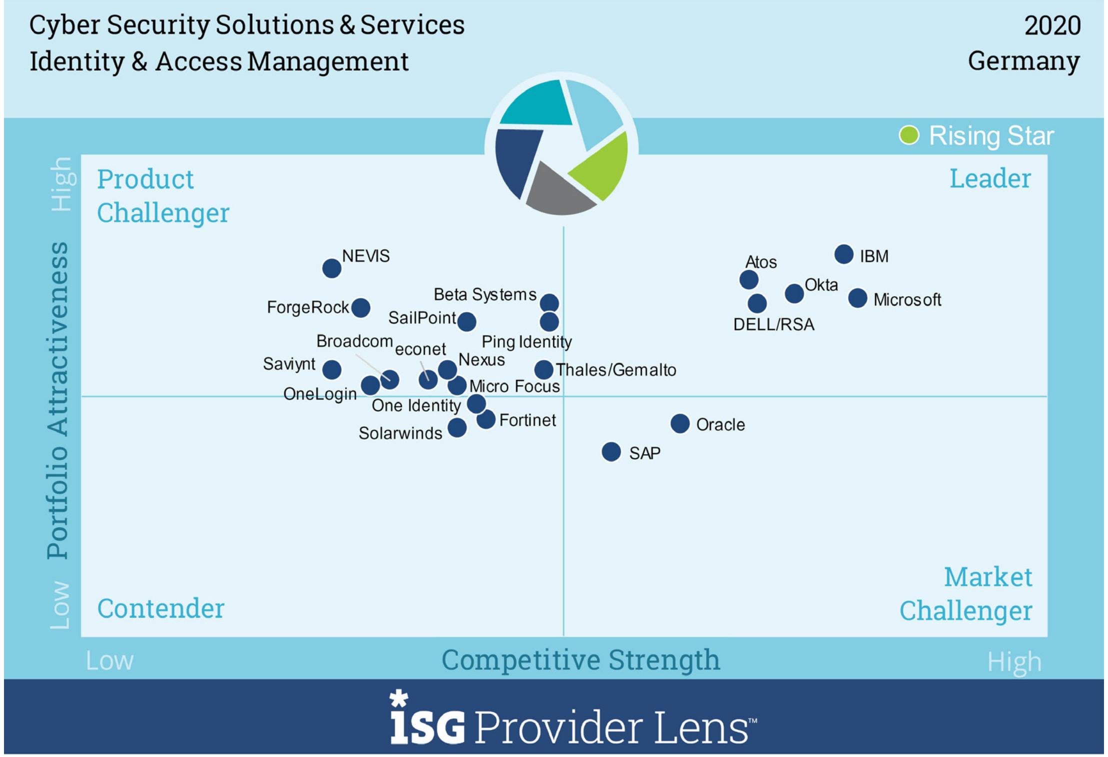
Security and data professionals should read this report to identify the providers that provide a wide range of IAM features and how they can be compared with each other.

Business executives and board members should read this report to understand the landscape of IAM as it directly affects how a business avoids cyberattacks and protects its reputation.

IDENTITY & ACCESS MANAGEMENT

Definition

IAM products are used to capture, record and manage user identities and the associated access authorizations. These products ensure that access rights are granted in accordance with defined guidelines. In order to deal with existing and new requirements of applications, security providers are increasingly required to incorporate mechanisms, frameworks and automation (for e.g., risk assessment) into their management suites, enabling them to carry out real-time user profiling and attack profiling. The influence of social media and mobile users imposes additional requirements to cover the security needs of customers, which was previously the case with web-related and context-related authorization management. This category also includes cloud services from product providers.



Source: ISG Research 2020

IDENTITY & ACCESS MANAGEMENT

Eligibility Criteria

- Relevance (Sales, number of customers) as an IAM product provider in Germany
- Offering must be based on in-house software, not third-party software

Observations

After a period of average demand development, IAM has been revived as an important security topic and will continue to play a major role in the future. The main reason is that the increasing digitalization of all areas drive the need to protect not only users and their identities, but also machines and certain areas of the company (keyword: Industry 4.0). In the future, securing identity will be crucial for securing digital systems and their networks. In addition, the number of users, devices and services is constantly increasing along with the number of digital identities to be managed. With the increase in permanent data loss arising from cyberattacks, it is more important to ensure effective and efficient control of identity management. Digital identities are the key to data, devices and services, making it critical to ensure they are specially secured.

As in case of the software market as a whole, there is also a shift from on-premise operation to the cloud with respect to IAM solutions. Most providers have adapted to this transformation and offer both on-premise and cloud operation (identity as a service). Companies that are purely cloud providers are

IDENTITY & ACCESS MANAGEMENT

Observations (cont.)

also becoming increasingly common; a special mention would be Okta. The growing success of this U.S.-based provider in Germany shows that customers are increasingly valuing the convenient operation of cloud-based security solutions. A key factor in this case is opening up new target groups; using IAM has become possible without any challenges owing to its cloud-based operations, even for small and mid-tier companies that would otherwise be unable to cope with their own operations.

Bundling and integration also play a critical role. Microsoft has successfully implemented this action plan in the IAM market for several years and has now significantly expanded its market position.

In the course of this supplier investigation, 22 companies have been identified as relevant manufacturers in the IAM market in Germany. Five of them were able to position themselves as Leaders.

- **Atos** has further developed its Evidian IAM portfolio over the year. The company has also been able to score with its modular offering.
- With its subsidiary (via the integrated EMC) RSA, **Dell** is characterized by the high performance of its offering.
- **IBM** benefits from the performance and extensive range of functions of its IAM solution, as well as its ability to integrate into IT landscapes.
- **Microsoft** was able to improve its position in the IAM market compared to last year's study. It has strengthened its competitiveness in this segment through cost-effective bundling. The company was able to gain significant market share for its complete and intelligent Microsoft 365 solution. It also scores with its technical features.
- **Okta** has observed an improvement in its position. It can further expand its position in the German IAM market through continued engagements and its cloud approach, which is particularly attractive for small and mid-tier companies.
- Last year's Product Challenger, **CA Technologies**, was acquired by Broadcom. As a result, in this study, Broadcom has been evaluated instead.

ENTERPRISE CONTEXT

Data Loss / Leakage Prevention

This report is relevant to enterprises across industries in Germany for evaluating providers of data leakage/loss prevention (DLP) products, including cloud services, that identify and monitor sensitive data, provide access for only authorized users and prevent data leakage.

In this quadrant report, ISG highlights the current market positioning of providers of DLP and data security solutions in Germany and the way they address the key challenges faced by enterprises in the region. ISG notes that enterprises face the challenge of controlling data movements/transfers as connectivity has become ubiquitous. In the meanwhile, enterprise need for DLP solutions has expanded with an increasing number of devices being connected to enterprise networks with the Internet of Things (IoT) and other digital transformation initiatives.

Germany's cyber security market is mature and competitive, with the presence of both global providers and local players. The need for DLP solutions and services is growing because of the requirement to comply with the data protection guideline in the European Union (EU), the General Data Protection Regulation (GDPR).

IT and technology leaders should read this report to understand the relative positioning and capabilities of providers of DLP solutions.

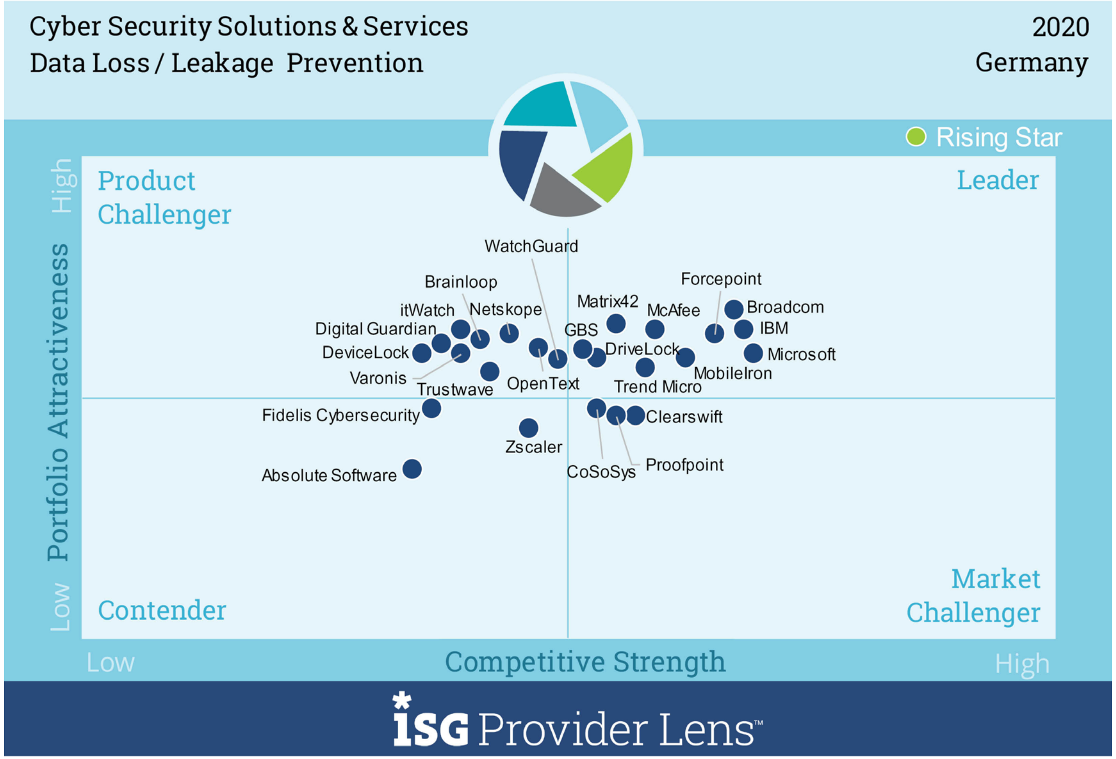
Security and data professionals should read this report to understand how providers and their tools help comply with the security and data protection laws in Germany, such as the GDPR, by providing DLP security solutions, and how they can be compared to each another.

Compliance and governance leaders should read this report to understand the landscape of DLP as it directly affects compliance with the GDPR.

DATA LOSS / LEAKAGE PREVENTION

Definition

This quadrant covers products for the identification and monitoring of sensitive data, ensuring that it is only accessible to authorized users and that there are no data leaks. DLP products are becoming increasingly important as the control of data movements and transfers is becoming more difficult for companies. The number of (mobile) end devices in companies on which data can be stored is growing. These end devices usually have their own connection to the Internet, allowing data to be sent and received without using the central Internet gateway. In addition, the end devices have a variety of interfaces (such as USB, Bluetooth, WLAN, NFC) through which data can also be exchanged. This category also includes cloud services from product providers.



Source: ISG Research 2020

DATA LOSS / LEAKAGE PREVENTION

Eligibility Criteria

- Relevance (sales, number of customers) as a DLP product provider in Germany
- DLP offering to be based on in-house software, not third-party software

Observations

DLP solutions have gained significant interest in recent years owing to various factors that affect the security of data in an enterprise. The growing business use of private end devices poses a challenge in terms of protection against undesired data outflows. Enterprises often evade configuration and control by operational administration and may not be monitored extensively for legal reasons such as data protection requirements. DLP solution providers should take these restrictions into account to ensure control without allowing operational security gaps. With the sanctions of the General Data Protection Regulation (GDPR), enforced since the end of May 2018, the importance of data protection as well as DLP solutions has risen further among enterprises.

In addition to the mobility and variety of functions for end devices, IT trends of big data, social business and cloud computing make it difficult to control data movements and place high demand on DLP solutions. With the growing volumes of data, powerful DLP solutions are required to quickly locate, classify and protect it against unauthorized actions such as copying or moving based on protection needs. Cloud

DATA LOSS / LEAKAGE PREVENTION

Observations (cont.)

storage solutions and cloud apps can cause data to leave the company network unintentionally during processing. There is also a risk that operational data will be transferred to private cloud storage services. Social networks and other social media platforms open up new communication channels such as email through which data can flow.

In the course of this supplier investigation, 25 companies have been identified as relevant manufacturers in the DLP market in Germany. Ten of them were able to position themselves as Leaders.

- Semiconductor manufacturer Broadcom acquired the enterprise product business of Symantec in late 2019. Accordingly, Broadcom was rated instead of Symantec and has taken over its Leader position.
- With the motto "Made in Germany", DriveLock has set itself apart from most of the international providers.
- Forcepoint has set itself apart from the competition owing to its data fingerprinting process.
- **GBS** is an expert on email security with a strong focus on social collaboration, a topic that is growing in relevance.
- With Guardium, **IBM** offers a universally applicable DLP solution.
- **Matrix42's** DLP offering not only assures a wide range of security functions but also ensures a high level of user acceptance.
- **McAfee** has established itself as a leader following the acquisition of DLP specialist Skyhigh in 2018. Its position is further strengthened by its large market presence, vast range of service offerings and innovative technology in Germany's DLP market.
- With its proven bundling principle, **Microsoft** has succeeded in further strengthening its position in the DLP market.
- **MobileIron** is highly specialized in mobile security. However, the company is still often perceived as a provider of mobile device management (MDM) and enterprise mobility management (EMM) solutions and services.
- With its easy-to-use DLP solution, **Trend Micro** has been able to strengthen its market position.

ENTERPRISE CONTEXT

Strategic Security Services

This report is relevant to enterprises across industries in Germany for evaluating providers of strategic security services that comprise consultations for cyber security solutions.

In this quadrant report, ISG highlights the current market positioning of providers of strategic security services in Germany and the way they address the key challenges faced by enterprises in the region.

Germany, like other markets, understands the increasing importance of cyber security, and is concurrently witnessing an expansion of strategic security services. The demand for strategic security services is growing because of the risks faced by enterprises due to the increase in number and types of attacks on their online assets. Also, enterprises need to comply with the European Union's General Data Protection Regulation (GDPR). In ISG's experience, companies in Germany discern providers based on their ability to provide experienced security professionals locally as part of a service engagement.

IT and technology leaders should read this report to understand the relative positioning and capabilities of strategic security services providers. The report also compares the consulting capabilities of the various service providers in the market.

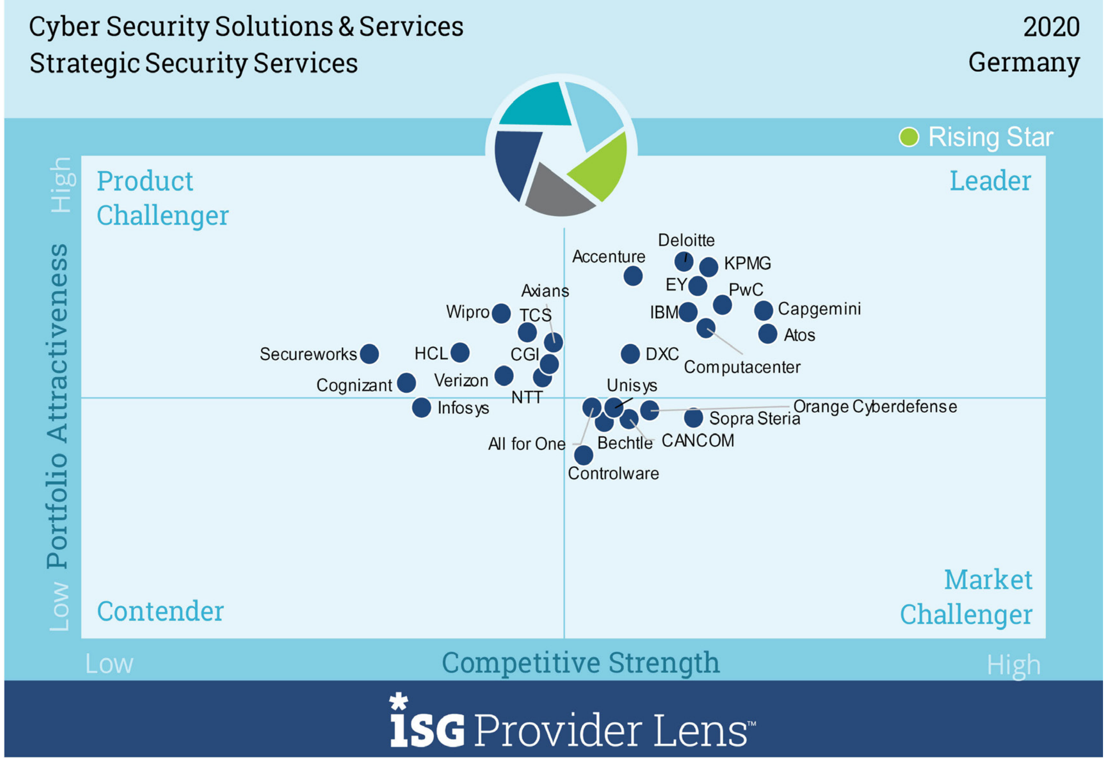
Security and data professionals should read this report to understand identify how strategic security services providers can be compared with each another in terms of their competence in offering security.

Business executives, including C-suite and board members, should read this report to understand the landscape of strategic security services as it determines how a business avoids cyberattacks and retains its credibility.

STRATEGIC SECURITY SERVICES

Definition

Strategic security services primarily cover consultation for IT security solutions. This quadrant examines service providers that have no exclusive focus on in-house products or solutions.



Source: ISG Research 2020

STRATEGIC SECURITY SERVICES

Eligibility Criteria

- Proven experience in IT security consulting for companies in Germany
- No exclusive focus on in-house products or solutions

Observations

Companies are facing various challenges concerning IT security and data protection. The increase in cyber risks, coupled with lack of resources, drives the need for orientation around these important topics.

The increase in sophisticated cyberattacks makes it difficult for companies, from large to small-tier enterprises, to protect their IT systems. The lack of IT specialists further complicates the situation. Mid-size companies in particular are suffering from the intense shortage of skilled IT security professionals. They often lag behind the larger companies that usually provide better conditions in this respect.

In addition, regulatory requirements for data security and protection are increasing. An important example is the Basic Data Protection Regulation (DSGVO), which is many small and mid-tier enterprises find it difficult to comply with even after it came into force more than two years ago.

Due to these factors, many companies require external support. This often starts with consultation on strategies, solutions and technology providers to meet the security and data protection requirements. In addition, the COVID-19 crisis has stirred a need for additional consultation services as IT systems are now

STRATEGIC SECURITY SERVICES

Observations (cont.)

more vulnerable owing to the increased practice of remote working and the resulting need for stronger external connections among employees.

Owing to their complex IT (security) landscapes and projects, large companies are still among the most important customers for strategic security services. Mid-tier companies are also increasingly using these services and have thus become another target group with above-average market growth.

Service providers in this market segment fall into two groups: (i) IT security service providers whose portfolios also cover security consultation and (ii) consultation firms whereby the "Big Four" auditors comprising Deloitte, EY, KPMG and PwC play a prominent role.

In the course of this provider investigation, 27 companies have been identified as relevant service providers of strategic security services in Germany. Ten of them were able to position themselves as Leaders.

- **Accenture's** success is attributed to a deep understanding of technology and access to the highest levels of management of clients.
- **Atos** is a BSI-certified IT security service provider and has a convincing holistic security approach.
- **Capgemini** offers a wide range of consultation services combined with a special approach to customer care.
- **Computacenter's** comprehensive consultation services are an important part of its holistic approach to security services.
- **Deloitte** benefits from its deep business expertise in the IT security consultation domain.
- **DXC's** broad thematic competence enables it to implement integrated IT and cyber security solutions.
- **EY** has been expanding it client base through its competence and customer-orientation approach.
- **IBM's** customers benefit from the firm's integrated service portfolio and deep technical knowledge.
- **KPMG** has strategic competence coupled with strong business and technical understanding.
- In addition to its large global presence, **PwC** is able to distinguish itself by leveraging its various competencies.

ENTERPRISE CONTEXT

Technical Security Services

This report is relevant to enterprises across industries in Germany for evaluating providers of technical security services.

In this quadrant report, ISG highlights the current market positioning of providers of technical security services in Germany and the way they address the key challenges faced by enterprises in the region. With the growing number of vendors of tools and shortage of skills, providers of technical security services are becoming increasingly relevant to streamline implementation.

Germany is a mature security market, where large companies typically require extensive technical security services because of their complex architectures and requirement for a wider variety of tools. In ISG's experience, companies in Germany discern providers based on their ability to provide specialized and highly skilled resources locally as part of a service engagement.

IT and technology leaders should read this report to understand the relative positioning and capabilities of technical security services providers. The report also compares the technical capabilities of the various service providers in the market.

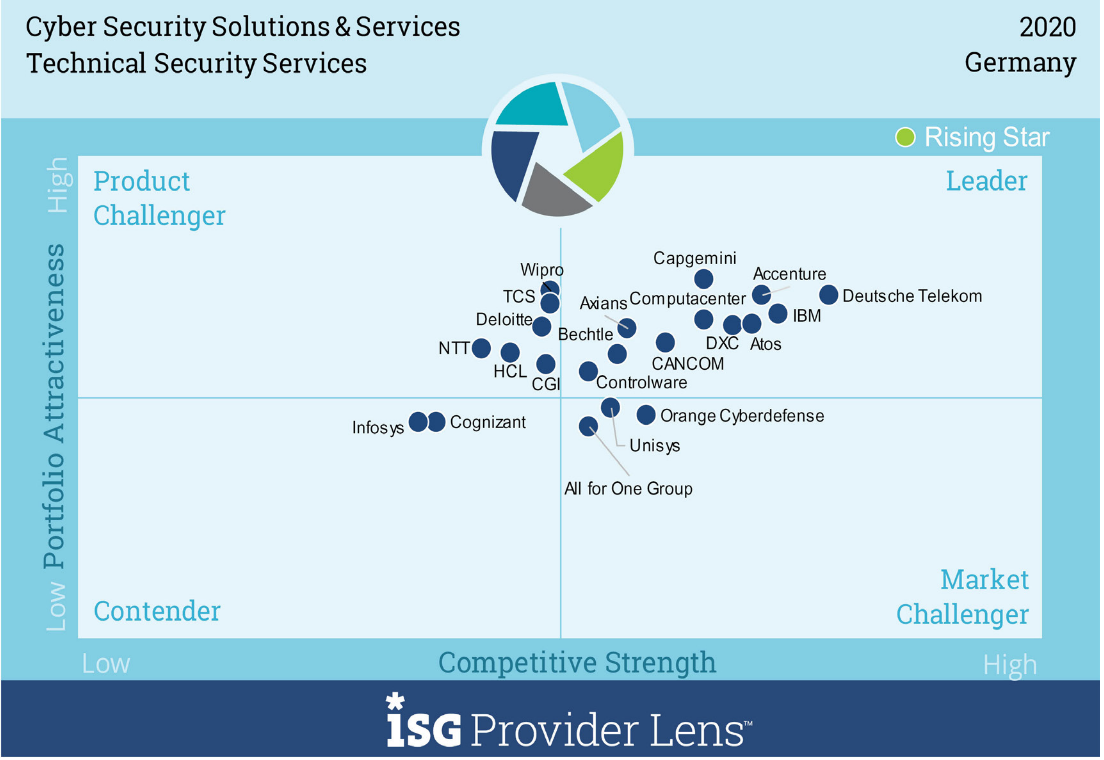
Security and data professionals should read this report to understand how technical security services providers can be compared to each other.

Business executives, including C-suite and board members, should read this report to understand the landscape of technical security services as it directly affects how a business avoids cyberattacks and retains its credibility.

TECHNICAL SECURITY SERVICES

Definition

Technical Security Services cover services such as integration, maintenance and support of IT security solutions. This quadrant examines service providers that do not focus exclusively on proprietary products and are able to implement and integrate dealer solutions.



Source: ISG Research 2020

TECHNICAL SECURITY SERVICES

Eligibility Criteria

- Proven experience in implementing security solutions for companies in Germany
- Authorization from IT security product manufacturers to sell and support their security solutions
- Certified Experts
- Participation in IT security associations/organizations (desired, not required)

Observations

The increasingly intensity, complexity, innovativeness of cyberattacks makes it a challenge for companies to protect their IT systems from damage. The lack of IT specialists complicates this situation. Therefore, companies are increasingly relying on external service providers to keep their IT security systems updated. Cyber criminals are also taking advantage of user negligence in the form of Trojan and Phishing attacks. In addition, for modern security equipment, training for users plays an important role.

Small and mid-tier companies have to catch up on modernizing their IT security systems; these companies often suffer particularly owing to lack of IT specialists, lack of awareness or excessive demands on insufficient capital. However, the ever-increasing, more complex security threats and the need to comply with data security guidelines are compelling these companies to take action which, in many cases, requires external support. Mid-tier companies also, often, appreciate the local presence of service providers for uncomplicated, quick support.

In addition, the COVID-19 pandemic has created external support requirements to secure IT landscapes, since the increased use of home offices and personal connections of employees make IT systems more vulnerable.

IT security projects are often demanding and diverse. Therefore, service providers that offer a wide range of technical security services from a single source and address as many IT security challenges as possible are at an advantage, as are service providers that have partnerships with renowned technology providers and have employees have numerous certifications.

TECHNICAL SECURITY SERVICES

Observations (cont.)

In order to be successful in the demanding market of Technical Security Services for large customers, providers must be able to present extensive as well as global experience in this market segment with a broad range of solutions. Powerful, often internationally represented teams must be available for support.

Due to their complex IT (security) landscapes and projects, large companies continue to be among the most important customers for technical security services. For the reasons described above, mid-tier companies are also increasingly using these services and are, therefore, a target group with above-average market growth.

In this study, 22 companies have been identified as particularly relevant providers of Technical Security Services in Germany. Of these, 11 were able to position themselves as leaders.

- **Accenture** offers a wide range of services from a single source for the IT security transformation of its clients.
- **Atos** is a BSI-certified IT security service provider and has a holistic security approach.
- **Axians** offers an extensive security services portfolio and its offerings are not limited to mid-tier German companies.
- **Bechtle** scores with extensive Technical Security Services and local presence.
- **CANCOM** offers customized security solutions and not only for mid-tier companies.
- **Capgemini** combines an extensive cybersecurity service portfolio with commitment to customer care.
- **Computacenter** attracts customers with its holistic approach to security services.
- **Controlware** scores with its modular security services portfolio.
- **Deutsche Telekom,** with Telekom Security, has the largest team for providing IT security services in Germany.
- **DXC** convinces customers with its integrated solutions for cybersecurity and IT systems.
- **IBM** can offer its customers a comprehensive, integrated service portfolio, in addition to its deep technical knowledge.

DEUTSCHE TELEKOM

Overview

In the area of Telekom Security, the Telekom Group bundles its extensive IT security competencies under T-Systems. The Telekom Security portfolio is marketed under the Magenta Security label.

Strengths

Portfolio covers a broad spectrum: With Magenta Security, T-Systems offers a comprehensive portfolio of security services, covering all security technologies.

Expanded offerings: Deutsche Telekom has recently expanded its portfolio of security services. So now a complex/advanced solution like drone defense can also be addressed.

Large team of experts: The Telekom Security division employs around 1,300 security specialists, which is the largest team in Germany.

Advantage of local origin: With Security made in Germany, Deutsche Telekom scores well, particularly with mid-tier customers.

Caution

The portfolio is difficult to manage: The extensive security portfolio of Deutsche Telekom, with the large number of partners, is difficult to manage.

2020 ISG Provider Lens™ Leader

With Telekom Security, Deutsche Telekom has the largest team of IT security services in Germany.

ENTERPRISE CONTEXT

Managed Security Services

This report is relevant to enterprises across industries in Germany for evaluating providers of managed security services (MSS).

In this quadrant report, ISG highlights the current market positioning of providers of MSS in Germany and the way they address the key challenges faced by enterprises in the region. In the past few years, some providers have expanded their portfolios, from running security operations centers (SOCs) to offering complex, artificial intelligence (AI)-powered cyber security solutions.

In Germany, the demand for MSS primarily arises from the Manufacturing industry with its critical operations requiring security. Germany is a mature security market for large companies, with potential for growth in the midmarket. The demand for MSS is growing in the latter because of a shortage of experts with the needed cyber security skills. At the same time, the large companies typically require more extensive security services. In ISG's experience, companies in Germany discern providers based on their ability to provide specialized and highly skilled resources locally as part of a service engagement.

IT and technology leaders should read this report to understand the relative positioning and capabilities of MSS providers. The report also compares the technical capabilities of the various service providers in the market.

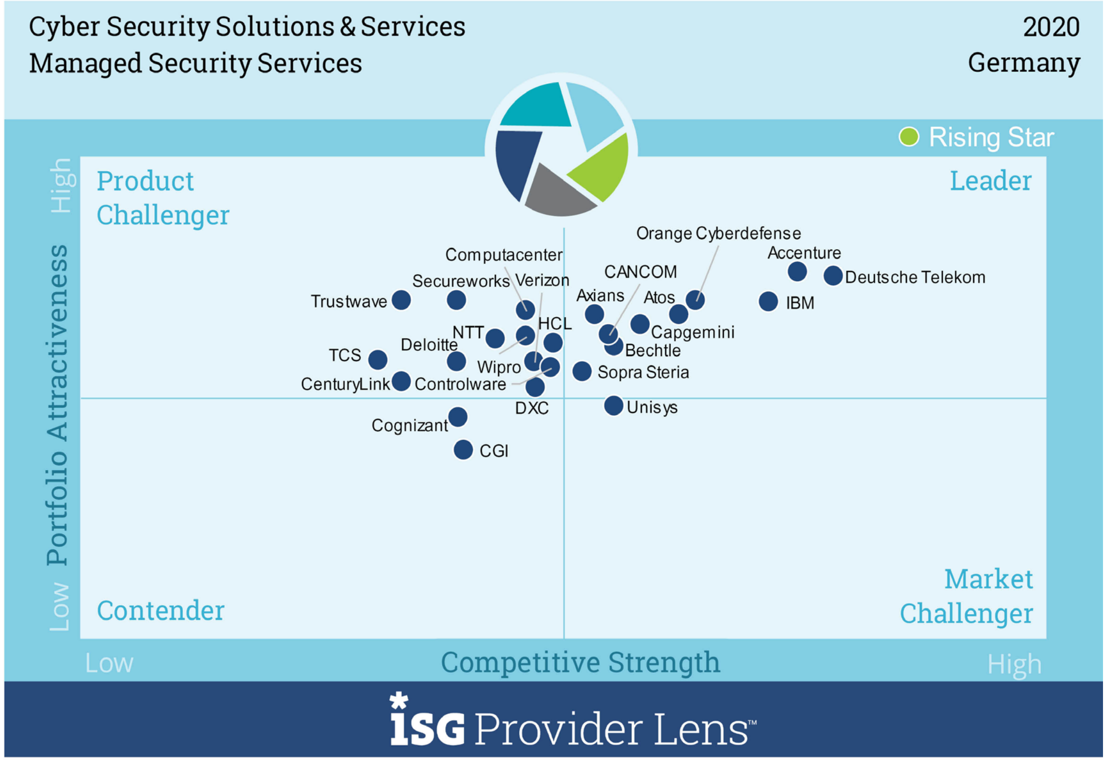
Security and data professionals should read this report to understand how MSS providers can be compared with each other.

Business executives, including C-suite and board members, should read this report to understand the landscape of MSS as it directly affects how a business avoids cyberattacks and retains its credibility.

MANAGED SECURITY SERVICES

Definition

Managed Security Services include the operation and management of IT security infrastructures for one or more customers through a security operations center (SOC). Typical services include security monitoring, behavior analysis, recording of unauthorized access, consultation regarding preventive measures, penetration tests, firewall operation, anti-virus operation, IAM operation, DLP operation and other (operational) services to ensure constant protection, in real time, without loss of performance. This quadrant considers service providers that are not exclusively focused on proprietary products, but can manage best-of-breed security tools. They can handle the entire lifecycle of a security incident — from identification to resolution.



Source: ISG Research 2020

MANAGED SECURITY SERVICES

Eligibility Criteria

- Offering security services such as detection and prevention, security information and event management (SIEM), support through security consultation and security audits, both remotely or at a customer's location.
- Authorizations from providers of IT security products
- Ideally, SOCs should be owned and managed by the provider and not primarily by partners
- Certified personnel, for example, with regard to CISSP, CISM, GIAC etc.

Observations

With the increasing intensity and complexity of cyberattacks aimed at large, established companies, Managed Security Services are increasingly coming into focus. Paucity of qualified resources, increasing frequency of incidents and the need for up-to-date information are triggering the demand for these services. Due to the frequently global presence of large companies, SOCs that are distributed worldwide play a special role in this segment. SOCs located in Germany are preferred by large companies because of the increasing need for data protection. Due to their complex IT security systems, large companies often place high value on a wide range of security solutions that are covered by the Managed Security Service providers.

At the same time, mid-tier companies are increasingly depending on the support of external service providers to deal with increasing security challenges; small and mid-tier businesses are becoming increasingly interested in Managed Security Services for handling security systems. In this context, SOCs based in Germany are an advantage for mid-tier companies, since this clientele prefers operations in Germany; German-speaking contacts also play an important role for this customer group.

MANAGED SECURITY SERVICES

Observations (cont.)

Regardless of the size of the company, ensuring the reliability of Managed Security Services is important to customers, which means that the services to ensure availability and confidentiality — physical protection of SOCs, redundant systems, high-class SLAs and a highly available hotline — must be optimal. In addition, customers expect Managed Security Service providers to be highly innovative so that they can always stay ahead of cyber criminals. This includes the expansion of SOCs toward cyber defense centers, by countering increasingly complex threats with advanced technology, including AI.

In this study, 25 companies were identified as particularly relevant for the Managed Security Services market in Germany. Of these, 10 were able to position themselves as leaders.

- **Accenture** has expanded its position in the Managed Security Services market with the acquisition of Broadcom's Symantec Cyber Security Services business.
- **Atos** impresses with its extensive managed security services and operations in Germany.
- **Axians** offers extensive managed security services in Germany.
- **Bechtel's** comprehensive managed security services and SOC in Germany are appreciated by mid-tier and other customer segments.
- **CANCOM** develop its extensive portfolio of Managed Security Services dynamically.
- **Capgemini** combines extensive managed security services with a large global presence.
- **Deutsche Telekom** scores with its motto, Security made in Germany.
- **IBM's** managed security services are based on powerful proprietary technology.
- **Orange Cyberdefense** has established SOCs worldwide.
- **Sopra Steria** offers extensive managed security services from its base in Germany.

DEUTSCHE TELEKOM

Overview

In the area of Telekom Security, the Telekom Group bundles its extensive IT security competencies in one unit, under T-System. The Telekom Security portfolio is marketed under the label, Magenta Security. Deutsche Telekom operates SOCs in several continents, especially in Europe.

Strengths

Extensive services: Telekom Deutschland's portfolio of managed security services covers a wide range of technologies and services.

Expanding its offerings: Deutsche Telekom has opened a new SOC in Singapore, and the concept of SOC services for connected cars is also very interesting. The company is also planning further additions to its portfolio.

Local operations: Deutsche Telekom operates Managed Security Services in Germany, which is appreciated by many mid-tier customers.

Security Made in Germany: With this motto, Deutsche Telekom can score especially in the context of data protection, and particularly with the target group of mid-tier companies.

Caution

The portion of mid-tier customers could be expanded: In contrast to most of its competitors, Deutsche Telekom has its own mid-tier unit; however, the focus of its managed security services is still on large customers even though the demands in the mid-tier segment are growing above average.

2020 ISG Provider Lens™ Leader

Deutsche Telekom scores with Security Made in Germany.

Methodology

METHODOLOGY

The research study “2020 ISG Provider Lens™ Cyber Security - Solutions & Services” analyzes the relevant software vendors/service providers in the German market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

The study was divided into the following steps:

1. Definition of 2020 ISG Provider Lens™ Cyber Security - Solutions & Services, German 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. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
6. Use of the following key evaluation criteria:
   - Strategy & vision
   - Innovation
   - Brand awareness and presence in the market
   - Sales and partner landscape
   - Breadth and depth of portfolio of services offered
   - Technology advancements

Authors and Editors

Frank Heuer, Author

Senior Advisor

Frank Heuer is Manager, ISG Research at ISG Germany. His focus rests on topics including Cyber Security, Digital Workspace, Communication, Social Business & Collaboration and Cloud Computing, especially Workspace/Unified Communications & Collaboration as a Service. His areas of responsibility include consultation ICT providers on strategic and operational marketing and sales. Mr. Heuer is active as a speaker at conferences and Webcasts on his main topics and is a member of the IDG network of experts.

Ron Exler, Enterprise Context and Global Overview Analyst

Principal Analys

Ron Exler is a Principal Analyst with ISG Research, with a cross-industry focus on the disruptive and progressive influences on businesses – and the experiences of their customers - of the Digital Workplace, Internet of Things (IoT), location intelligence, and other digital innovations. Ron has led product management at enterprise software companies, run enterprise research advisory services, and advised, built and deployed innovative technology inside large enterprises. Ron holds a Master of Science degree in Cartography from the University of Wisconsin as well as a Bachelor of Science degree from Oregon State University. Ron also holds the ISG Digital Xpert certification.

Authors and Editors

Heiko Henkes, Author

Director Advisor

Heiko Henkes is a Director and Principal Analyst at ISG; in his role as Global IPL Content Lead, he is responsible for strategic business management and acts as thought leader of ISG's team of research analysts. His core competencies are in the areas of defining derivations for all types of companies within their IT-based business model transformation. He builds the bridge between IT trend topics and acts as keynote speaker on current and future IT trends. Heiko has over 12 years' experience in IT consulting, primary and secondary market research and provider GTM strategies.

His research Focus: Digital Business Transformation, Cloud and Edge Computing, Mobile Business, Change Management and Mixed Reality

ISG Provider Lens™ | Quadrant Report
August 2020

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of 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 1,300 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 www.isg-one.com.