ISG Provider Lens™

Cyber Security - Solutions & Services

Germany 2020

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

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

ISG Provider Lens™

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.

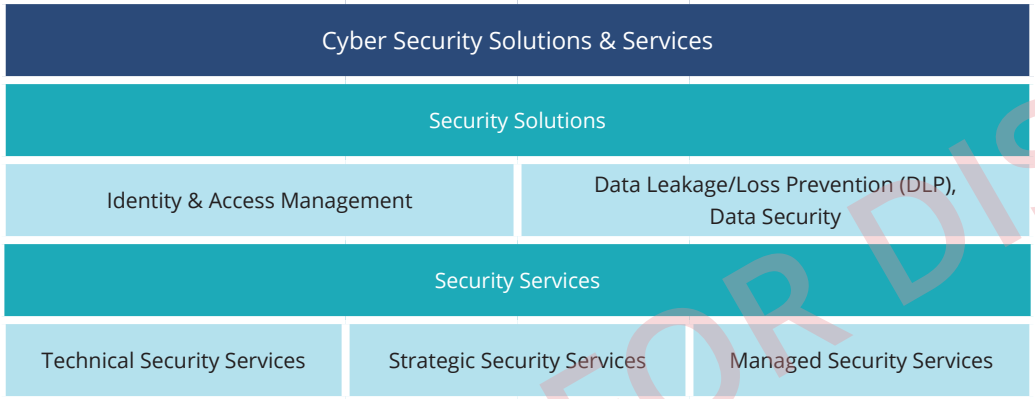
Large and mid-tier customers are turning towards security operations centers (SOCs) based in Germany due to the growing need for data protection. Moreover, it is important for both target groups to ensure the reliability of managed security services and a high level of innovation in order to stay a step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



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.

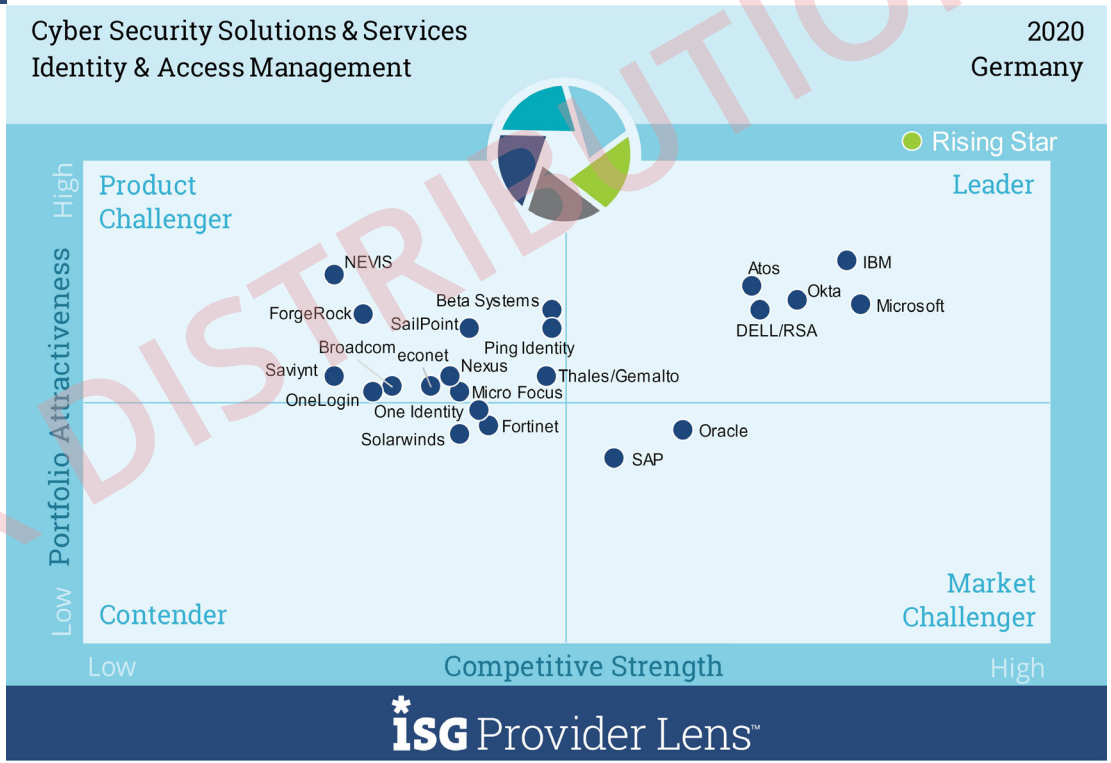
Security and data professionals should read this report to identify the providers that provide a wide range of IAM features and how they can be compared with each other.

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.

ATOS

Overview

Evidian is part of French IT service provider Atos. With the Evidian IAM portfolio, Atos is not only an IT security service provider but also a specialist for IAM products. The Evidian IAM suite includes Evidian Enterprise SSO, Evidian Authentication Manager, Evidian Web Access Manager, Evidian Identity Governance and Administration (IGA) and Evidian Analytics and Intelligence.

Strengths

Vast range of functions: With its IAM portfolio, Atos covers a vast range of security requirements. The solution has a modular architecture with well-coordinated elements, enabling it to be well adapted to customer needs.

Highly flexible solution: In addition to on-premise products, Atos also offers IAM as a cloud service from globally represented data centers.

Local operation: The solution is also delivered in Germany apart from other global data centers. This makes the offering interesting for global customers as well as companies that have high requirements for inland data storage.

High-performance solution: Among other features, the Evidian IAM suite also offers the powerful user management function.

Strong focus on innovation: The specialization of the Evidian IAM portfolio underlines Atos' innovative strength and comprehensive roadmap.

Caution

Atos could still expand its service portfolio based on the direct Evidian offering. It is advisable to consider supplementing the portfolio with services such as supply chain integration, developer/administrator support or a standard field service.

2020 ISG Provider Lens™ Leader

With its Evidian IAM portfolio, Atos offers an innovative and extensive offering.

DELL/RSA

Overview

With the integration of EMC in 2016, Dell is well represented in the IAM market with its subsidiary RSA. Dell/RSA offers the IAM portfolio under the RSA SecurID Suite.

Caution

DELL/RSA should provide more clarity on its portfolio . The extensive offering and unclear structure sometimes make it difficult for customers to obtain an overview.

Strengths

High-performing solution: The RSA SecurID Suite is one of the IAM solutions with the highest performance.

Easy to manage solution: DELL/RSA customers also benefit from the simple management of the RSA SecurID Suite.

High level of recognition; wide market distribution: DELL/RSA caters to a wide customer spectrum, ranging from small and mid-tier companies to large corporations.

Professional support for implementation: DELL/RSA supports the implementation of its IAM solution with numerous best practices and blueprints. New customers thus benefit from the experience gained from numerous customer projects.

2020 ISG Provider Lens™ Leader

DELL/RSA attributes its widespread presence in the IAM market to the high performance of its RSA SecurID Suite.

IBM

Overview

IBM is well positioned in the IAM market with its Security Access Manager and IBM Cloud Identity, of which the latter is an identity-as-a-service (IDaaS) offering.

Strengths

Covers wide range of functions: With its IAM portfolio, IBM can cover an extensive range of functions.

High level of integration: IBM's IAM solution can be optimally integrated into the existing IT landscape. The company currently offers the option of integrating its solution into mobile devices.

High performance: The Security Access Manager solution offers powerful authentication.

Strong market presence: IBM has an extensive customer base and a large worldwide partner network.

Wide range of use cases: IBM's wide range of use cases enables it to support a variety of customers.

Caution

IBM has relatively fewer publicly available references. Given its strong market position, the company could focus on expanding this.

IBM's market perception has potential for optimization. While existing customers, in particular, benefit from ability of the IAM solution to integrate into the IT systems, many potential customers do not even consider the company as an IAM provider. This is mainly due to IBM's reputation of offering complex and expensive products. IBM's leading position in the future could thus be jeopardized as it may lag behind competitors in terms of new gaining new customers in this fast-growing market. The company should focus on booting its external image such as by advertising the IBM Cloud® Identity offering more extensively.

2020 ISG Provider Lens™ Leader

IBM not only convinces regular customers with its high-integration capability, but also with a wide range of functions and efficient performance.

MICROSOFT

Overview

Microsoft's IAM offering is Azure Active Directory.

Caution

Despite Microsoft's transparency campaigns on data protection and dealing with compliance requirements, there are still widespread concerns among many users.

Strengths

High integration into existing Microsoft world: The integration capability of the IAM solution with existing cloud solutions makes it particularly appealing for Microsoft Azure customers. Azure Active Directory can also provide IAM for third-party (non-Microsoft) cloud solutions in the same way as for Microsoft's solutions and applications.

Improvements through constant innovation: Microsoft has been able to distinguish itself through technical features such as fingerprint scanning or face recognition instead of passwords.

Proven action plan: Microsoft's success in penetrating the IAM market is attributed to the implementation of cost-effective bundling. With Microsoft 365, it was able to gain significant market share in the IAM market.

Large market presence: The company benefits from the widespread use of its solutions and an unrivaled network of partners.

2020 ISG Provider Lens™ Leader

Microsoft knows how to expand its market position in the IAM market with proven action plans.

OKTA

Overview

Okta is a California-based company that specializes in IAM solutions from the cloud. The company had set up an office in Munich in early 2019.

Strengths

Quick implementation: Okta's IAM solution is characterized by quick implementation and reliability.

Tailored to customer requirements: Okta has integrated the Lightweight Directory Access Protocol (LDAP) to serve customers whose applications require this type of authentication.

Wide market presence: Okta's focus on investing heavily in marketing and sales in Europe has strengthened its market position. The company also has a website in German.

Cloud-based approach: The company has enabled market access to enterprise clients that had refrained from using an IAM solution due to the capital expenditure involved. These are mainly small and mid-tier companies that promise above-average potential.

Caution

Despite having a network of well-known partners in Germany, Okta could still look into expansion to strengthen its position.

2020 ISG Provider Lens™ Leader

Okta can further expand its market presence in Germany's IAM market through continued engagements.

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.

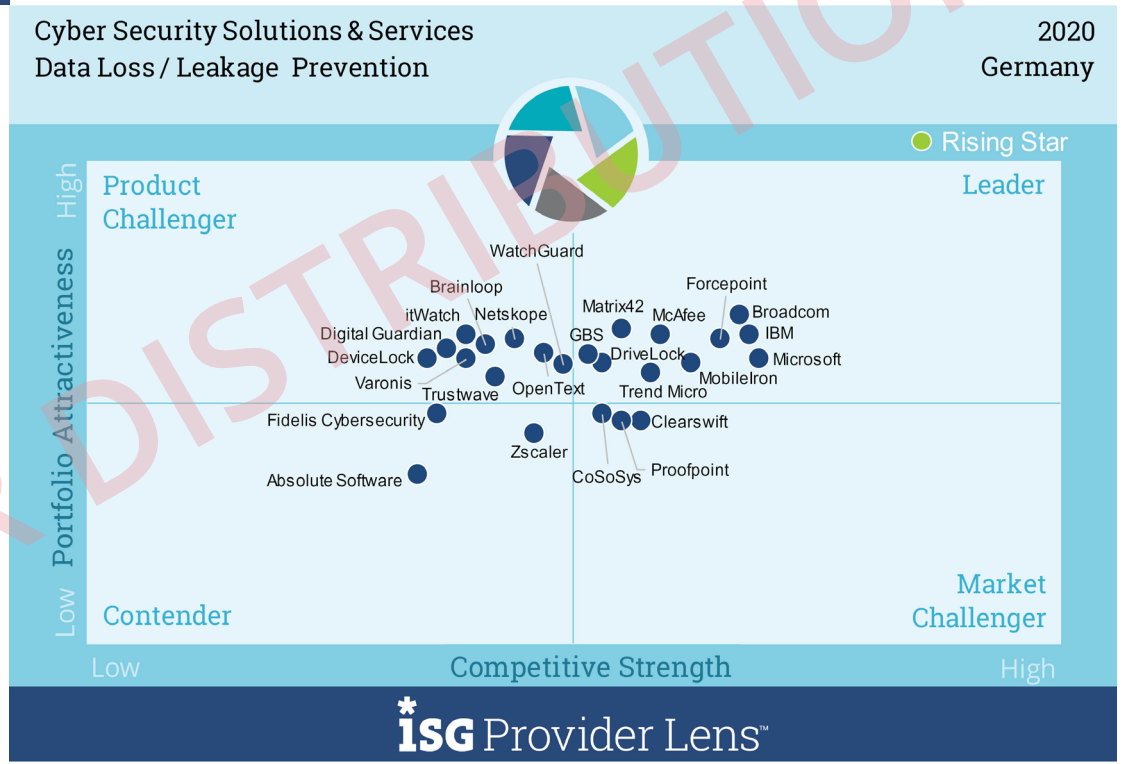
Security and data professionals should read this report to understand how providers and their tools help comply with the security and data protection laws in Germany, such as the GDPR, by providing DLP security solutions, and how they can be compared to each another.

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.

BROADCOM

Overview

Semiconductor manufacturer Broadcom acquired the enterprise product business of Symantec in late 2019. Symantec was one of the most comprehensive and successful product/service providers in the cyber security market. With the takeover of Symantec, Broadcom is one of the strongest providers in the market for DLP with its Symantec Data Loss Prevention and is accordingly positioned in the Leader quadrant.

Strengths

Symantec acquisition: With this move, Broadcom has set the benchmark for providers in the DLP market. It offers the most comprehensive range of services and uses Symantec Data Loss Prevention to cover numerous data loss scenarios. These include advanced functions such as image analysis and handwriting recognition.

Centralization and unification: The Broadcom solution provides a centralized console and unified policy management across all channels, namely cloud, end devices, storage, email and web.

Support through artificial intelligence (AI): Vector machine learning (ML) identifies intellectual property and other unstructured data, such as financial documents and source code, which are difficult to analyze.

Hybrid deployment model: Broadcom enables its customers to have a modern hybrid deployment model.

High flexibility over administration: The company can easily adapt to the DLP requirements of customers.

Partner network: With its close-meshed network of partners, Broadcom has a wide reach in the market.

Caution

The installation for Broadcom's DLP solution is quite complex. The company should simplify the process in order to reach out to a larger group of customers.

The transition from Symantec to Broadcom has not been a smooth one. Broadcom as a brand name does not yet have the same reputation in the security market as Symantec. Customers also report issues in purchase and renewal of licenses for Symantec's security software. These factors adversely affect Broadcom's market position.

2020 ISG Provider Lens™ Leader

With the takeover of Symantec, Broadcom has positioned itself as frontrunner in the DLP market.

DRIVELOCK

Overview

With the DriveLock Zero Trust Platform, Munich-based company DriveLock offers a DLP solution that can be operated in the enterprise as well as in the form of a managed security service from the cloud.

Strengths

Reliance on AI: DriveLock consistently makes use of ML algorithms.

Solution addresses a promising field of applications: DriveLock leverages its DLP solution to address a wide range of requirements of an IoT environment.

High level of trust among users: With the motto "Made in Germany", DriveLock can set itself apart from its competitors, most of whom are multinationals. With its “no-backdoor” guarantee (i. e., there is no secret access to the program, which enables bypassing normal access security), the company meets the needs of many user enterprises. Official approvals in Germany underline its trustworthiness.

Caution

DriveLock is not well known among large, globally active providers and should thus focus on strengthening its image.

Though its services cover a fairly wide range of requirements, they lack important features compared to the competition. DriveLock could consider adding test automation and supply chain integration to the offering.

2020 ISG Provider Lens™ Leader

With its "Made in Germany" motto, DriveLock plays a special role in the DLP market.

FORCEPOINT

Overview

U.S.-based company Forcepoint was established through the merger of DLP specialist Websense with Raytheon Cyber Products. With its Forcepoint DLP solution, the company has been able to position itself as a leader in the DLP space.

Strengths

Quick resolution to DLP incidents: With defined processes for investigating and eliminating the effects of security incidents, Forcepoint enables the rapid resolution of DLP incidents.

Data fingerprinting: This feature is a particular strength of Forcepoint's DLP solution. It allows data to be tracked with automatically applied control functions, even if the end devices are not in the network.

High degree of automation: Forcepoint's Incident Risk Ranking is based on ML mechanisms and offers a high degree of automation. This relieves the burden on security officers in enterprises.

Ready-to-use policy templates: These templates comply with the rules of the basic EU data protection regulation.

Caution

Raytheon, the parent company of Forcepoint, is an American defense company with close ties to the U.S. government. This may cause apprehension and reservation among customers that are critical of providers based in the region.

2020 ISG Provider Lens™ Leader

Forcepoint can stand out from the competition, particularly with its data fingerprinting process.

GBS

Overview

GBS, based in Karlsruhe, has been part of the Bulgarian BULPROS group of companies since January 2017. With its iQ.Suite DLP Advanced and iQ.Suite 360, the company has been able to position itself as a Leader in the DLP segment.

Strengths

Sophisticated DLP solution: With iQ. Suite DLP Advanced, GBS offers a solution that can detect sensitive content in email texts and attachments.

Secure dual-control principle: With email communication continuing to be the most important means of collaboration in companies, GBS has specialized in controlling information outflows via this communication channel. iQ.Suite DLP offers an interesting feature — emails identified in advance go through a dual-control check and can be released by a predefined individual such as the respective supervisor or the data protection officer.

Protection coverage includes social collaboration: With collaboration in companies undergoing a transformation, GBS has expanded its skills beyond email security and, as part of the BULPROS group, is an expert in securing collaboration environments and applications.

Several clients are managed centrally at low cost: The iQ.Suite Multi-Client Edition can support groups with affiliated subsidiaries and companies. It has a large distributed mail infrastructure that allows for cost-effective central administration of multiple clients.

iQ.Suite DLP Advanced — quick implementation and on customer-specific basis: Owing to the granular functionalities and regulations, customer-specific DLP scenarios can be implemented quickly, flexibly and tailored to customer needs.

Compliance with the GDPR/DSGVO: GBS takes the requirements of GDPR into account by providing detailed notifications of security incidents to ensure timely reporting of data protection violations.

Caution

GBS DLP solution still does not provide an inventory of data storage locations. It would also be advantageous to provide users with role-specific and user-specific releases for interfaces and devices.

The addition of innovation management, field service and supply chain integration to the service portfolio could help GBS strengthen its market position.

2020 ISG Provider Lens™ Leader

With its extensive expertise in email security, GBS has emerged as a strong leader in the DLP segment.

IBM

Overview

With its Guardium portfolio for DLP, IBM has positioned itself in the Leader quadrant in this space.

Strengths

Universal spectrum of applications: IBM Guardium secures data in on-premise as well as hybrid cloud and multi-cloud environments.

Strong AI capabilities: The IBM solution is suitable for protection of structured as well as unstructured data.

High level of integration: For existing customers, the DLP solution can be optimally integrated into their IT landscape.

Large market presence: IBM has one of the most extensive partner networks in the DLP space.

Caution

While existing IBM customers, in particular, benefit from the ability of the DLP solution to integrate into their IT systems, many potential customers do not consider IBM as a DLP provider. This is mainly due to IBM's reputation of offering complex and expensive products. IBM's leading position in the future could thus be jeopardized as it may lag behind competitors in terms of new gaining new customers in this fast-growing market.

2020 ISG Provider Lens™ Leader

With the Guardium portfolio, IBM offers a universally applicable DLP solution.

MATRIX42

Overview

Matrix42, a digital workspace management provider based in Frankfurt took over its technology partner, endpoint specialist EgoSecure. Matrix42 is positioned in the leader quadrant for DLP with EgoSecure Data Protection and Endpoint Detection & Remediation.

Strengths

Wide range of functions: Matrix42 offers a comprehensive range of functions in its DLP portfolio and is continuously developing the offering.

Professional service and support: The DLP portfolio offers an accompanying range of services to address various security requirements. In addition to round-the-clock on-call duty, Matrix42 also offers support in German which is particularly advantageous for the growing mid-tier segment.

Large local and international presence: Matrix42 has cloud data centers in numerous countries, including Germany. This is beneficial for enterprises clients that are interested in both local and global operations.

High acceptance among users: All safety functions take place fully automatically in the background. This allows the user to continue working as he prefers and is used to. This promotes acceptance among users.

Caution

Matrix42 is continuing to expand its indirect sales channel in order to rapidly expand its reach in the market, especially in the mid-tier, which is a relevant segment for the company. However, there is still potential that can be tapped in this case.

2020 ISG Provider Lens™ Leader

Matrix42 not only offers a wide range of DLP functions, but also ensures a high level of acceptance among users.

MCAFEE

Overview

In 2018, McAfee acquired the competitor and DLP specialist Skyhigh. The company is represented in the DLP market with the Total Protection for DLP product suite.

Caution

Given McAfee's strong presence and extensive experience in the DLP market, its references in Germany have potential for expansion.

Strengths

Wide range of offerings: McAfee's range of DLP services cater to a wide range of requirements. The McAfee Prevent solution enables proactive policy enforcement for many data types where a wide range of content types can be classified. It can also determine the location of an end device and tailor a response such as whether or not the end device is on the network.

Strong local and international presence: McAfee has cloud data centers in numerous countries, including Germany. This is beneficial for customers that are interested in both local and international operations.

Dense distribution network: McAfee has a close-knit network of sales partners in Germany.

2020 ISG Provider Lens™ Leader

McAfee combines a wide range of services with a strong presence in the DLP market.

MICROSOFT

Overview

Microsoft's DLP offering is Azure Information Protection. With its strong portfolio, the company has positioned itself in the leader quadrant for DLP.

Strengths

Full control over all data: Microsoft enables overall control even if it is passed on to individuals outside the organization.

Compliance with legal requirements: Microsoft provides predefined templates that make it easier to cater to the requirements of GDPR.

Proven action plan: Microsoft's success in penetrating the DLP market is attributed to cost-effective plans such as bundling (for e.g., with Microsoft 365) The company was able to gain significant market share in the DLP market.

Large market presence: In the market, Microsoft offers solutions services from its unrivaled network of partners.

Caution

Microsoft could provide greater clarity for its DLP portfolio to increase preference for the solutions.

Despite Microsoft's transparency campaigns on data protection and dealing with compliance requirements, there are still widespread concerns among many users.

2020 ISG Provider Lens™ Leader

Microsoft succeeds by further expanding its position in the DLP market.

MOBILEIRON

Overview

MobileIron is an expert in mobile device management and enterprise mobility management solutions. Accordingly, the company specializes in the backup of mobile data, which is supported with Docs@Work.

Strengths

Comprehensive protection: MobileIron provides secure access and DLP controls across content for business email and SharePoint. The Docs@Work solution prevents data loss by ensuring that email attachments and other documents in the secure content interface are not accessed through untrusted apps.

Specialization in mobile data usage: Data usage increasingly implies mobile data usage due to the growing importance of mobile end devices. Thus, MobileIron, with its approach, is positioned to be a pioneer.

Extensive sales partner network: MobileIron's dense partner network in Germany contributes to its competitiveness. Deutsche Telekom's is its most important long-term sales partner.

Caution

MobileIron could consider increasing its marketing communication toward mid-tier companies to drive greater market success for its DLP solutions. The company MobileIron has mainly been catering to customers from the upper mid-tier and larger companies segment, with less on the broader layer below. However, there is a growing need for DLP in mobile use, especially among mid-tier companies.

Despite MobileIron's now strong position in the DLP market and its future-oriented approach, the company is still commonly perceived as a provider of mobile device management (MDM) and enterprise mobility management (EMM) with less market awareness of its DLP solutions. Increased marketing communication towards DLP to complement its MDM and EMM solutions could be helpful.

2020 ISG Provider Lens™ Leader

With a specialization in mobile security, MobileIron is well positioned in the DLP market in Germany.

TREND MICRO

Overview

Security expert Trend Micro offers a wide range of leading security solutions. The company DLP offering is called Integrated DLP (iDLP).

Strengths

Easy to implement: Trend Micro iDLP is easy to deploy and inexpensive as it integrates DLP functionality into existing Trend Micro solutions and management consoles via a plug-in, making it appealing to many users.

Ease in compliance: Trend Micro's DLP solution helps user organizations meet compliance regulations through ready-to-use compliance templates.

Improved visibility and control: Trend Micro provides greater visibility and control with a fully integrated, centrally managed solution.

Focus on data security for users: iDLP trains employees to handle company data according to the guidelines, for e.g., through warnings and blocking.

Numerous sales partners: Trend Micro's close-knit partner network allows for a wide reach in the DLP market in Germany.

Caution

Trend Micro's range of services is less extensive compared to those of other leading providers and is mainly offered through partners. With a more comprehensive service offering, the company could strengthen its client base.

2020 ISG Provider Lens™ Leader

The simple introduction and application of the DLP solution helps to strengthen Trend Micro's 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.

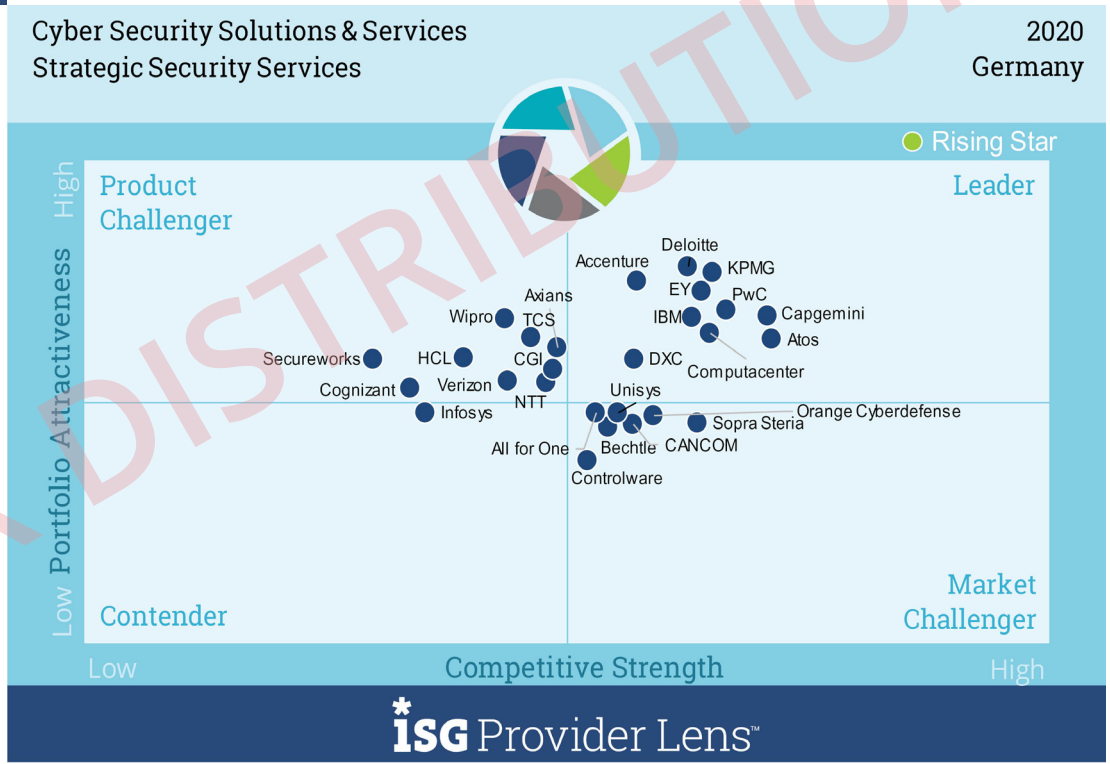
Security and data professionals should read this report to understand identify how strategic security services providers can be compared with each another in terms of their competence in offering security.

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.

ACCENTURE

Overview

Accenture, one of the world's largest management consulting, technology and outsourcing service providers, offers a strong portfolio of strategic security services. The company is well positioned in this segment with its 'Strategy & Risk' offering. It has several innovation centers in Germany.

Strengths

Wide range of offerings: Accenture scores well with the depth of its offering that covers a wide range of topics and services.

Extensive expertise and experience: Apart from the IT services market, Accenture is strongly positioned in the strategic security services space with its vast expertise and experience in consultation as well as a deep understanding of technology.

Access to board level: As a highly reputed technology consultant, Accenture has access to board levels in customer companies. This target group is important for the sustainable implementation of security strategies.

Systematic approach for portfolio development: Accenture leverages its innovation centers to ensure that the company itself and its clients are well positioned for the future.

Caution

Accenture does not exploit the full potential of the market despite having a base of exclusive clientele. The company is not particularly focused on mid-tier companies, which often much to catch up with in the cyber security space.

2020 ISG Provider Lens™ Leader

A combination of deep understanding of technology and access to the highest management levels contributes to Accenture's success in this space.

ATOS

Overview

French IT service provider Atos offers consultation and technology services, system integration and outsourcing services. The company's strength lies in its cyber security consulting offering for the strategic security services market.

Strengths

Vast portfolio: Atos provides an extensive range of services for customers in Germany and across the world.

Holistic approach: Atos understands how to address the needs of its enterprise customers with a holistic approach that emphasizes the business relevance of security services.

Numerous certifications: Atos is an IT security service provider certified by the Federal Office for Information Security (BSI). It also has numerous other certifications.

Large security team: Atos has a global Security Services team comprising several thousand specialists.

Caution

Atos is primarily geared to the needs of large companies with demanding requirements. Mid-tier companies, which need to keep pace in terms of their cyber security strategies present a large market potential.

Atos' wide range of services does not include unified threat management. The company should consider including this technology-related offering to boost the attractiveness of the portfolio for many customers, especially small and mid-tier companies.

2020 ISG Provider Lens™ Leader

Atos is a BSI-certified IT security service provider and has a convincing holistic security approach.

CAPGEMINI

Overview

Capgemini is a French consultation and IT service company and one of the largest European management consultancies. The company offers cyber security consulting services for IT security.

Strengths

Wide range of services: Capgemini's has a vast portfolio of consultation services and the security topics covered are extensive.

High-level customer care approach: All of Capgemini's customers are looked after by a manager who is also responsible for delivery.

Large security team: Capgemini has a global Security Services team with several thousand specialists.

Caution

Capgemini is primarily geared to the needs of large companies with higher requirements. Mid-tier companies, which particularly need to keep pace in terms of their cyber security strategies, present a large market potential.

2020 ISG Provider Lens™ Leader

Capgemini offers a wide range of consultation combined with a special approach to customer care.

COMPUTACENTER

Overview

Computacenter is a British IT service provider. It offers a portfolio for IT security services under its Digital Trust proposition.

Strengths

Wide range of services: Computacenter's range of consultation services and the security topics covered are extensive.

Holistic approach: Computacenter has positioned itself as a strategic partner with a holistic security approach and a strong understanding of the infrastructure and business requirements of its customers. Security, in general, is an integral part of most projects and services at Computacenter, but can also be obtained as a separate service.

Large security team: Computacenter employs a Security Services team in Germany with numerous specialists.

Caution

Computacenter's business focus lies more on large companies with 5,000 or more employees. It should pay more attention to the mid-tier client segment, which is showing above-average growth in this space.

2020 ISG Provider Lens™ Leader

Computacenter's comprehensive consultation services are an integral part of its holistic approach to security services.

DELOITTE

Overview

Deloitte offers services in the areas of auditing, tax consultation and consulting for companies and institutions. Its global network includes member companies in more than 150 countries; The company has more than 9,000 employees in Germany.

Caution

Deloitte is primarily geared to the needs of large companies with high requirements. Mid-tier companies, which particularly need to keep pace in terms of their cyber security strategies, present a large market potential.

Strengths

Significant expansion in offering: Deloitte has invested heavily in its digitalization security offering.

Deep understanding of customer needs: The company has a high level of understanding of the business requirements of its customers.

Strong global presence: Its large global presence enabled the company to offer one-stop support for global projects.

2020 ISG Provider Lens™ Leader

Deloitte benefits from its deep business expertise in the IT security consultation domain.

DXC

Overview

DXC Technology (DXC) was established with the merger of HPE's service division and CSC 2017, presenting a strong combination of their security service competencies and other capabilities. DXC offers consultation, implementation and managed Services in this segment. Its security unit provides services to customers and also ensures security for its own operations. The company has around 138,000 employees in over 70 countries.

Strengths

Integrated solutions: As a thematically broad IT service provider, DXC is able to offer integrated solutions and security for IT systems.

Extensive services: DXC has a wide portfolio of cyber security consultation offerings.

Focus on agility: Despite its extensive manpower, DXC is working on various other domains in this space such as blueprints to achieve greater agility.

Caution

Customer relationship could be less complex: The projects indicate that DXC is a large organization, where many managers are involved in projects, resulting in many contact persons and complex relationship with customers.

2020 ISG Provider Lens™ Leader

DXC's broad thematic competence enables it to implement integrated IT and cyber security solutions.

EY

Overview

Ernst & Young (EY) is a network of legally independent and autonomous companies operating globally in fields such as auditing, tax consultation and management consultation. The organization employs over 284,000 people at 700 locations in 150 countries.

Caution

EY is primarily geared to the needs of large companies with higher requirements. Mid-tier companies need to keep pace in terms of their cyber security strategies and thus present a large market potential. However, this client segment also finds EY's consulting costs to be on the higher side.

Strengths

Strong advisory skills: EY's strong base of consultants have a wide and deep spectrum of qualifications, allowing it to differentiate itself in this space.

Customer-orientation approach: EY maintains a strong focus on its customers.

Ensuring trust: EY's relationship with its customers is characterized by a particularly high degree of transparency.

2020 ISG Provider Lens™ Leader

EY is expanding its client base through its strong competencies and customer-orientation approach.

IBM

Overview

IBM is one of the world's largest IT product and service providers. In the cyber security space, the firm offers a wide range of products under the Cybersecurity Services' label, specializing in various services for major customers.

Strengths

Comprehensive and integrated portfolio: IBM has one of the broadest portfolios for IT security services comprising various interconnected elements that range from consultation to managed security services and cloud services. This enables the firm to provide strong customer support following consultation.

Global delivery: IBM's large, globally present and experienced Security Service team is focused on global delivery, which is an important aspect for customers around the world.

Deep technical insights: As a technology provider, IBM has a deep understanding of security solutions, offering relevant consulting services in this space.

Caution

IBM is not the first choice for customers that are cost sensitive.

Provider independence cannot be advocated as convincingly as done by its many competitors: IBM is not only a major security consultant, but also a provider of security products. As a result, in terms of consultation, IBM cannot convince customers (particularly potential) that it is as independent as others providers that do not have product portfolios.

2020 ISG Provider Lens™ Leader

IBM customers benefit from its integrated service portfolio and deep technical knowledge.

KPMG

Overview

KPMG International (commonly referred to as KPMG) is a global network of legally independent and independent companies with a focus on auditing, tax consultation and business consultation. The company has its headquarters in Switzerland and operational headquarters in the Netherlands. It has more than 219,000 employees in 147 countries.

Strengths

Strong business and technical understanding: KPMG has a strong focus on addressing the IT security challenges of business operations.

Collaboration: KPMG's consultants are considered to be highly goal-oriented and cooperative.

Strategic competence: The consulting teams convince many customers about the company's strategic competence.

Caution

KPMG is not the first choice for customers that are cost sensitive.

2020 ISG Provider Lens™ Leader

KPMG is well positioned with its strategic competence and a combination of business and technical understanding.

PWC

Overview

PricewaterhouseCoopers International (hereinafter PwC) is a global network of legally autonomous and independent companies in domains such as auditing, tax consultation and business consultation. The global PwC network is present in 157 countries with more than 250,000 employees. The company has more than 11,800 employees in Germany.

Strengths

Skillful uses of competencies: PwC knows how to successfully bundle its competencies in various subject areas for IT security consultation.

Consultants impress with their range of skills: PwC consultants are characterized by great thematic competence and entrepreneurial flair.

Global delivery: PwC's large international presence enables global delivery, which is an important aspect for customers across the world.

Caution

PwC is not the first choice for customers that are essentially cost-sensitive.

2020 ISG Provider Lens™ Leader

PwC has a large global presence and is able to distinguish itself by demonstrating 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.

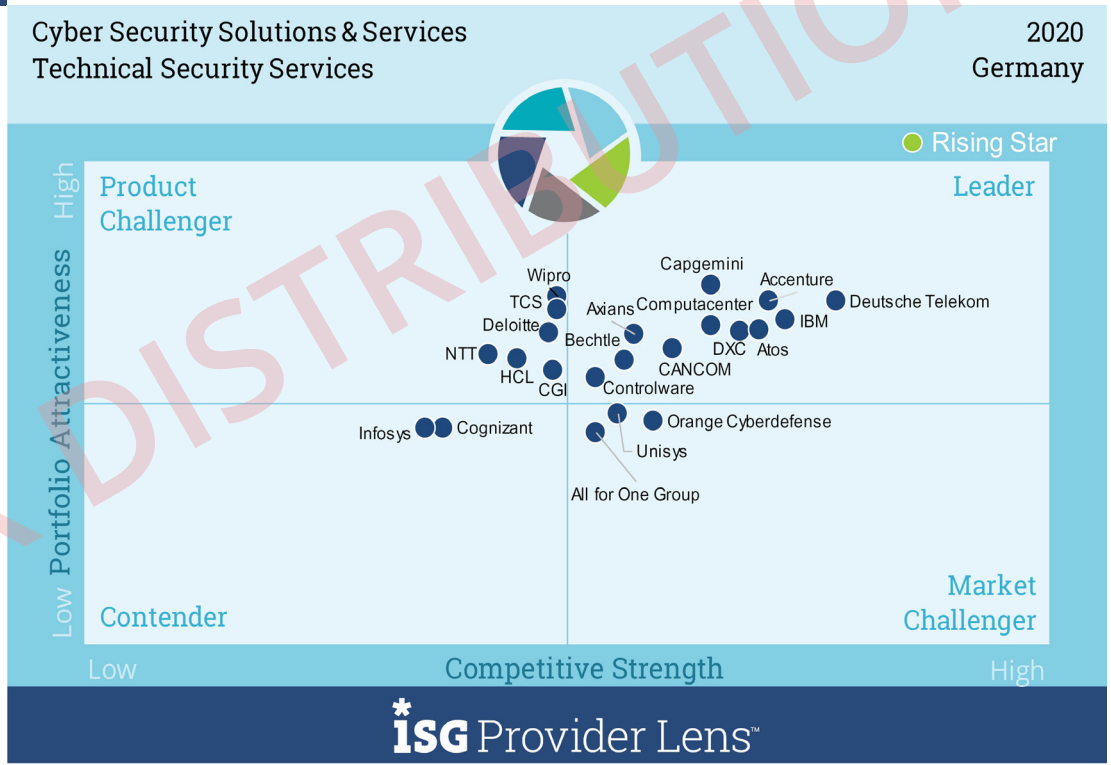
Security and data professionals should read this report to understand how technical security services providers can be compared to each other.

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.

ACCENTURE

Overview

As one of the largest management consulting, technology and outsourcing service providers in the world, Accenture also has a portfolio for Technical Security Services. It operates in the market for Technical Security Services with its Cyber Defense offering. The company has several innovation centers in Germany.

Strengths

Great expertise and experience: As in the IT services market as a whole, Accenture also scores in the Technical Security Services market with its great expertise and experience in transformation through a deep understanding of technology.

Wide range of offers: Accenture covers a wide range of areas and services in the implementation of IT security projects.

Strong partner ecosystem: Accenture works with numerous well-known providers of IT security products.

Systematically developing portfolio: Through its Innovation Centers, Accenture ensures that it, along with its customers, is well-prepared for the future.

Caution

Does not harness the full potential of the market: The clientele of Accenture is quite exclusive. So far, the company has not specialized in mid-tier companies that need to catch up on their cybersecurity measures.

2020 ISG Provider Lens™ Leader

Accenture offers a wide range of services from a single source for the IT security transformation of its clients.

ATOS

Overview

The France-based IT service provider, Atos, offers consultation and technology services, and system integration and outsourcing services. In the Technical Security Services market, Atos offers its services under the name, Cybersecurity.

Strengths

Numerous certifications: Atos is an IT security service provider certified by the Federal Office for Information Security (BSI) and also has numerous other certifications such as ISO 27001.

Holistic approach: Atos is attuned to the needs of its enterprise customers and takes a holistic IT security approach that also emphasizes the business relevance of security services.

Strong partner ecosystem: Atos works with numerous renowned providers of IT security products.

Large Security Team: Atos has a security services team with thousands of specialists worldwide and is, therefore, able to implement large-scale security projects.

Caution

It is advisable to expand the range of topics and services covered: Atos covers a wide range of topics, but does not include Unified Threat Management, especially DLP. Regarding services, it could consider training for users, administrators and field service personnel.

Atos hardly addresses the mid-tier: Atos is primarily geared to address the needs of large companies, less so for mid-tier companies that need to update their security landscape and, therefore, represent a large market potential.

2020 ISG Provider Lens™ Leader

Atos impresses with its status as a BSI-certified IT security service provider and with its holistic approach to security.

AXIANS

Overview

Axians IT Security (Axians) is the IT security business division of the Axians group of companies, which is part of the France-based Vinci Group. Axians offers managed security services, security-as-a-service, as well as technical and organizational security services.

Strengths

Comprehensive portfolio: Axians has a comprehensive portfolio of security services, covering a wide range of security technologies.

Strong technology partnerships: Axians maintains partnerships with numerous renowned security technology providers.

Focuses on the mid-tier: Axians is focused on mid-tier companies in terms of IT security projects. This segment needs to update its cybersecurity landscape and, therefore, has significant growth potential.

Renowned references: Axians not only addresses the security demands of small and mid-tier companies, but can also name well-known large companies as its customers for IT security services.

Caution

Expansion of global presence is advisable: Axians is represented in 23 countries, but needs to expand its global presence both in terms of tapping potential customers that operate globally and competing with players that have presence worldwide; hence, it is advisable to consider other countries.

2020 ISG Provider Lens™ Leader

Axians offers an extensive security services portfolio that is not limited to mid-tier German companies.

BECHTLE

Overview

Bechtle is one of the largest IT system houses in Germany. The company provides its Technical Security Services under the name, Bechtle Security - the 360-degree solution for maximum security, from the competence center Bechtle Internet Security & Services (BISS), which was founded in 2000 .

Strengths

Wide range of offerings: Bechtle covers a wide range of areas and services in the implementation of IT security projects.

Focus on mid-tier companies: With regard to IT security projects, Bechtle is focused on mid-tier companies. These have an above-average backlog with regard to adopting/integrating cybersecurity solutions and are, therefore, the target group with particular growth potential.

Benefits from local presence: The company has presence in numerous locations in Germany. The decentralized structure of Bechtle is advantageous for addressing its target group of mid-tier customers.

Large security team: Bechtle has one of the largest IT security teams in Germany.

Caution

Greater global presence is worth considering: The local presence is a strong competitive factor, but global customers may miss the company's presence/support in other regions of the world.

Regional quality differences are possible: The decentralized structure of Bechtle has a positive effect on local needs, but can cause regional quality differences. However, Bechtle has now begun to standardize its services.

2020 ISG Provider Lens™ Leader

Bechtle scores with an extensive range of technical security services and a local presence.

CANCOM

Overview

CANCOM is one of the leading IT system houses in Germany. In the Technical Security Services segment, CANCOM offers its services under the CANCOM Security Solutions label'.

Strengths

Tailor-made security concepts for mid-tier to large companies: CANCOM offers a comprehensive Portfolio — from planning and implementation to managed services and cloud services.

Wide range of offerings: CANCOM covers a wide range of areas and services in the implementation of IT security projects. The company has expanded its services extensively over the past 12 months.

Focus on mid-tier companies: CANCOM is focused on mid-tier companies with regard to IT security projects. Overall, this segment has an above-average backlog in the integration of cybersecurity measures and are, therefore, a target group with particular growth potential. The large local presence of CANCOM is particularly advantageous for this segment.

Caution

More global expansion would be worth considering: Local presence is a strong competitive factor, and CANCOM is not only represented in Germany, but also in the U.S. and in some countries in Europe, but customers with a global presence may miss the company's presence/support in other regions.

2020 ISG Provider Lens™ Leader

CANCOM offers customized security concepts; its offerings are not limited to mid-tier companies.

CAPGEMINI

Overview

Capgemini is a France-based consultation and IT services company and one of the largest management consultancies in Europe. The company employs over 4,500 IT security experts worldwide.

Strengths

Wide range of services and topics: Capgemini's offering of Technical Security Services and the security topics covered therein is extensive.

Dynamic growth: Capgemini has considerably expanded its IT security services portfolio in the past 12 months, and is planning further extensive innovations.

High-level customer care approach: All customers are looked after by a manager, who is also responsible for delivery.

Large security team: Capgemini has a global security services team with thousands of specialists; in proportion to the number of customers, the team of IT security experts in Germany is large.

Caution

Capgemini hardly addresses the mid-tier: Capgemini is primarily attuned to the demands of large companies, and less so to mid-tier companies; this segment needs to particularly gear up in terms of cybersecurity initiatives and, therefore, represents a large market potential.

2020 ISG Provider Lens™ Leader

Capgemini combines an extensive cybersecurity service portfolio with commitment to customer care.

COMPUTACENTER

Overview

Computacenter is an U.K.-based IT service provider. The company's portfolio for IT security services is offered under the Digital Trust label.

Strengths

Holistic approach: Computacenter is able to position itself as a strategic partner with a holistic security approach and understanding of the infrastructure and business requirements of its customers. Security is an integral part of most projects and services of Computacenter, but can also be obtained as a separate service.

Extensive service portfolio developed dynamically: Computacenter's range of services with regard to Technical Security Services is broad. In addition, the roadmap indicates numerous measures for expansion.

Extensive partner ecosystem: Computacenter has a large number of renowned technology partners; for many of these players, Computacenter is a top partner.

Caution

The focus is more on large companies: Computacenter's business focus rests on large companies, with 5,000 or more employees, than on the mid-tier segment which is growing above average.

Extension of the technology spectrum is advisable: The company does not cover Unified Threat Management In its technology spectrum, which is otherwise very extensive. Covering this area could make Computacenter more attractive for mid-tier customers.

2020 ISG Provider Lens™ Leader

The holistic approach to security services contributes to the attractiveness of Computacenter.

CONTROLWARE

Overview

Controlware is a Germany-based IT service provider headquartered in Dietzenbach in Hesse. Controlware employs around 840 people and maintains a sales and service network comprising 16 locations in Germany, Austria and Switzerland.

Strengths

Modular Portfolio: In order to optimally cover the needs of its customers, Controlware's security services offering is modularly structured.

Balanced customer structure: Large as well as mid-tier customers are equally important for Controlware. Thus, the company can benefit from the large budgets of large customers and the above-average growth potential of the mid-tier segment.

Local presence: Mid-tier customers, in particular, trust local service providers.

Caution

Expansion of the portfolio is advisable: Controlware's technical security services have, so far, not covered the areas of Data Leakage/Loss Prevention and Identity & Access Management.

2020 ISG Provider Lens™ Leader

Controlware scores with a modular security services portfolio.

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.

DXC

Overview

In the company DXC Technology (DXC), the HPE service division and CSC 2017 combined, among others, their security service competencies. DXC offers consultation, implementation and managed services in this segment. The security unit at DXC provides its services to customers and also secures its own operations. DXC employs approximately 138,000 people in over 70 countries.

Strengths

Extensive services: DXC covers a wide range of security services; it DXC has a broad base dedicated to cloud security. Furthermore, DXC is also focused on providing solutions for IAM.

Integrated solutions: As an IT service provider that covers a number of areas, DXC has the ability to offer integrated solutions from IT systems and corresponding security.

Extensive resources: DXC has several thousand employees worldwide in the Security division.

Focus on automation: Despite the extensive manpower, DXC continues to work on the topics of Automation and Blueprints in order to achieve greater agility.

Caution

The customer relationship could be less complex: DXC's projects reflect that it is a very large organization; many managers are involved in projects.

2020 ISG Provider Lens™ Leader

DXC convinces with its integrated solutions for cybersecurity and IT systems.

IBM

Overview

IBM is one of the largest IT product and service providers in the world. In the Cybersecurity market, IBM offers a wide range of products under the label, Cybersecurity Services, and specializes in services for major customers.

Strengths

Comprehensive, integrated Portfolio: IBM is represented in the market with one of the broadest portfolios for IT Security Services, which include technical security services.

One-stop-shop for solutions: Due to IBM's competence in the IT market, it can offer IT solutions and the corresponding security from a single source.

Deep technical knowledge: As a technology provider, IBM has a deep understanding of security solutions, including the ones offered under IBM Technical Security Services.

Global delivery: IBM's large, globally present, experienced security service team enables global delivery, which is important for customers around the world.

IBM emphasizes support: An interesting offer from IBM is a truck with 20 workstations, in which customers and interested parties can simulate stress situations with regard to IT security. Furthermore, IBM stimulates a collaborative exchange of its numerous customers so that they can mutually benefit from their experience.

Caution

The costs are relatively high: IBM is not the first choice for customers that are essentially cost-sensitive.

2020 ISG Provider Lens™ Leader

In addition to deep technical knowledge, IBM can also offer its customers a comprehensive, integrated service portfolio.

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.

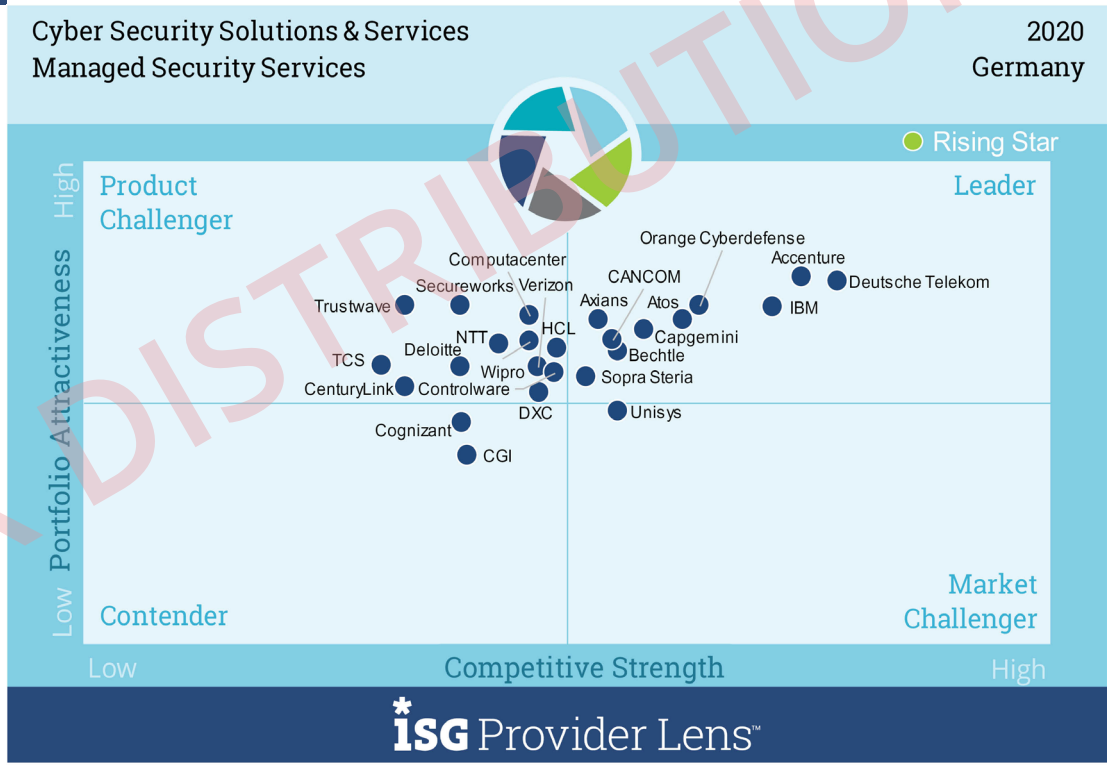
Security and data professionals should read this report to understand how MSS providers can be compared with each other.

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.

ACCENTURE

Overview

As one of the largest management consulting, technology and outsourcing service providers in the world, Accenture also offers Managed Security Services under the name, Managed Security Services. In January 2020, Accenture announced the acquisition of Broadcom's Symantec Cyber Security Services business, which has helped Accenture strengthen its position in the Managed Security Services market.

Strengths

Extensive managed security services: Accenture offers a wide range of managed security services that are becoming increasingly relevant in the market.

Reliability of services: The managed security services offered by the company are characterized by availability and confidentiality.

Global presence: Accenture operates globally distributed SOCs that make the company particularly attractive for companies with a global presence.

Caution

The local presence can be expanded: An SOC in Germany could make Accenture more attractive for interested parties.

Accenture does not exploit the full potential of the market: The clientele of Accenture is quite exclusive. So far, the company does not specialize in mid-tier companies that need to catch up on managed security services.

2020 ISG Provider Lens™ Leader

With the acquisition of Broadcom's Symantec Cyber Security Services business, Accenture has been able to establish its market position.

ATOS

Overview

The France-based IT service provider, Atos, offers consultation and technology services, and system integration and outsourcing services. Atos operates 14 SOCs worldwide.

Strengths

Operations worldwide: Germany is one of the locations for Atos' SOC. A local SOC is preferred by many large companies. Atos is represented worldwide with numerous SOCs on different continents and is, therefore, attractive for companies that have a global presence.

Extensive managed security services: Atos offers a wide range of managed security services that are becoming increasingly relevant in the market.

Reliability of services: The managed security services offered by the company are characterized by availability and confidentiality.

Dynamic growth: Atos has made numerous additions to/innovations in its managed security services roadmap.

Caution

Atos hardly addresses the mid-tier: Atos is attuned to the demands of large companies, and less so to mid-tier companies that need to update their security landscapes and are plagued with lack of IT specialists; this segment represents a large market potential.

2020 ISG Provider Lens™ Leader

Atos impresses with its extensive managed security services and operations in Germany.

AXIANS

Overview

Axians IT Security (Axians) is the IT security business division of the Axians group of companies, which is part of the France-based Vinci Group. Axians offers managed security services and security-as-a-service, as well as technical and organizational security SOLUTIONS.

Strengths

Customer-oriented portfolio: Among other areas, managed security services is central to the security portfolio of Axians.

Extensive services: Within the framework of managed security services, Axians covers a wide range of areas.

Reliability of services: The managed security services by Axians are characterized by availability and confidentiality.

Local operations: Axians has SOCs in Germany , which makes it an attractive for many mid-tier companies.

Balanced customer structure: For Axians, large as well as mid-tier customers are equally importance with regard to managed security services; Axians can benefit from large budgets of large customers and the above-average growth of the mid-tier segment.

Caution

Awareness in the German market has potential for expansion: Axians has now established a leading position in the Managed Security Services market in Germany. However, companies do not often shortlist Axians when it comes to managed security service needs.

2020 ISG Provider Lens™ Leader

Axians offers extensive managed security services in Germany.

BECHTLE

Overview

Bechtle is one of the largest IT system houses in Germany. The company provides its managed security services under the name, Bechtle Security - the 360-degree solution for maximum security, from an SOC in Germany.

Strengths

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

Adaptable services: Bechtle offers its Managed Security Services in a modular way - depending on a customer's needs and in accordance with their core business.

Support in local language: Bechtle operates an SOC, as a part of the Global Network Operations Center (GNOC), with German-speaking support.

Focus on mid-tier companies: Bechtle's managed security services are focused on mid-tier companies. This segment has above-average need to catch up with cybersecurity solutions, and is particularly affected by lack of IT security skills and, therefore, represents particular growth potential.

Caution

Greater global reach is worth considering: A local SOC is a strong competitive factor, but customers with a global presence may miss its presence/support in other regions.

2020 ISG Provider Lens™ Leader

Not only mid-tier customers appreciate Bechtel's comprehensive managed security services and SOC in Germany.

CANCOM

Overview

CANCOM is one of the leading IT system houses in Germany. In the managed security services segment, CANCOM offers its services under the label, CANCOM Managed and Security as a Service.

Strengths

Extensive services: CANCOM's Portfolio for Managed Security Services covers a wide range of technologies and services.

Dynamically developing its services: CANCOM has made numerous additions to/innovations in its managed security services roadmap.

Focus on mid-tier companies: CANCOM focuses on mid-tier companies in its offerings for managed security services. These companies have an above-average need to catch up with cybersecurity solutions and are particularly affected by lack of IT security skills; therefore, this target group has particular growth potential.

Local operations: CANCOM operates an SOC in Germany, which enables it to meet the expectations of many mid-tier customers.

Caution

Greater global reach is worth considering: The local SOC is a strong competitive factor, but customers with a global presence may miss the company's presence/ support in other regions.

2020 ISG Provider Lens™ Leader

CANCOM continues to develop its extensive managed security services dynamically.

CAPGEMINI

Overview

Capgemini is a France-based consultation and IT services company and one of the largest management consultancies in Europe. Capgemini operates 15 SOCs worldwide.

Strengths

Extensive services: Within the framework of its Managed Security Services, Capgemini covers a wide range of areas.

Reliability of managed security services: The accompanying services to ensure availability and confidentiality leave nothing to be desired.

Capgemini shows great dynamism: Capgemini has developed its managed security services portfolio significantly in the past 12 months and is planning more extensive innovations.

Global presence: Capgemini is represented in several continents its SOCs.

Caution

Capgemini hardly addresses the mid-tier: Capgemini is primarily geared to the needs of the demanding large companies, and less so to the mid-tier companies that particularly need to tap the benefits of managed security services and, therefore, represent a large market potential.

The local presence can be expanded: An SOC in Germany could increase traction among many interested parties, especially the mid-tier segment.

2020 ISG Provider Lens™ Leader

Capgemini combines its extensive managed security services with a large global presence.

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.

IBM

Overview

IBM is one of the largest IT product and service providers in the world. IBM operates a global network of Security Operations Center. The company's managed security services are based on its QRadar technology.

Strengths

Comprehensive, integrated Portfolio: IBM is present in the market with one of the broadest portfolios for IT Security Services, which include managed security services.

Powerful technology base: The managed security services offered by IBM are based on the efficient, in-house QRadar technology.

Enjoys large-scale awareness: IBM is one of the best-known providers of managed security services in the world.

Global operations: IBM's global SOC network enables global operations, which is important for its customers distributed worldwide.

Caution

IBM hardly addresses the mid-tier: IBM is primarily attuned to the demands of large companies, and less so to the needs of mid-tier companies that need to yet realize the benefits of managed security services and, therefore, represent a large market potential.

2020 ISG Provider Lens™ Leader

The managed security services from IBM are based on powerful proprietary technology.

ORANGE CYBERDEFENSE

Overview

Orange Cyberdefense is the IT Enterprise Security business of Orange, the largest France-based telecommunications company. The company operates sOCs in several continents.

Strengths

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

Continuous expansion of offerings: Orange Cyberdefense has considerably expanded its managed security services in the last 12 months. The company is planning further additions to its portfolio.

Global operations: Orange Cyberdefense's globally distributed SOCs enable global operations, which is important for its globally distributed customers.

Local presence: Orange Cyberdefense operates a CyberSOC/SOC in Germany.

Caution

The technology topics addressed could be expanded: With its managed security services, Orange Cyberdefense covers numerous areas of security, and the inclusion of Workplace Security in its portfolio could increase customer interest.

2020 ISG Provider Lens™ Leader

Orange Cyberdefense has global presence and local operations in terms of SOCs.

SOPRA STERIA

Overview

Sopra Steria is a France-based consultation company and IT service provider. In 2005, Steria Mummert Consulting was established with the takeover of Mummert Consulting AG by the France-based Steria Group. Through the merger of Sopra and Steria, in September 2014, it became Sopra Steria GmbH.

Strengths

Extensive services: Sopra Steria covers a wide range of areas within the framework of its managed security services.

Reliability of services: The managed security services offered by Sopra Steria are characterized by availability and confidentiality.

Local operations: Sopra Steria operates an SOC in Germany.

Caution

Awareness in the German market still offers potential for expansion: Sopra Steria has now established a leading position in the Managed Security Services market in Germany. However, user companies do not often shortlist Sopra Steria when looking for Managed Security Services.

2020 ISG Provider Lens™ Leader

Sopra Steria offers extensive managed security services in Germany.

Methodology

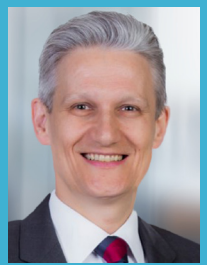
METHODOLOGY

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.