



**\*ISG** Provider Lens™

2019/2020

Cyber Security  
Solutions & Services

imagine your future®

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 75 of the top 100 enterprises in the world, 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](http://www.isg-one.com)



## Table of Contents

Definition .....	4
Quadrant Research.....	5
Schedule.....	8

© 2019 Information Services Group, Inc. All rights reserved. Reproduction of this publication in any form without prior permission is strictly prohibited. Information contained in this report is based on the best available and reliable resources. Opinions expressed in this report reflect ISG’s judgment at the time of this report and are subject to change without notice. ISG has no liability for omissions, errors or completeness of information in this report. ISG Research™ and ISG Provider Lens™ are trademarks of Information Services Group, Inc.

# Definition

Within the scope of digitalization and the (industrial) internet of things, business processes more and more shift into the IT. In order to protect the company itself, it becomes increasingly important to protect its IT- and communication systems. Finally, IT security turns into company security.

Data and IT infrastructures are permanently exposed to criminal threats. Additionally, there are threats causing from carelessness in the companies. Beside the demand for self-protection, laws (e.g. in Europe: General Data Protection Regulation) more and more force companies to protect themselves from cyberattacks.

So, ICT security is a topic which must not be ignored. However, IT executives often struggle to justify security investments to the business management, particularly the CFO, to whom many of them report directly. Unlike other IT projects, it is not always possible to prove the ROI of such security investments. It is not easy to quantify threat-related risks, and therefore, security measures are often rather low-level and not sufficient to address novel kinds of threats. On the other hand, it is not (always) the lack of suitable technology that leads to security vulnerabilities; many attacks such as Trojan and phishing attacks, are caused by users' thoughtless behavior. Therefore, consulting and user trainings continue to play a key role, together with up-to-date ICT equipment.

The new benchmark "ISG Provider Lens –Cyber Security Solutions & Services 2019/2020 Germany" addresses both areas to support ICT decision-makers to help them make the best use of their (tight) security budgets.

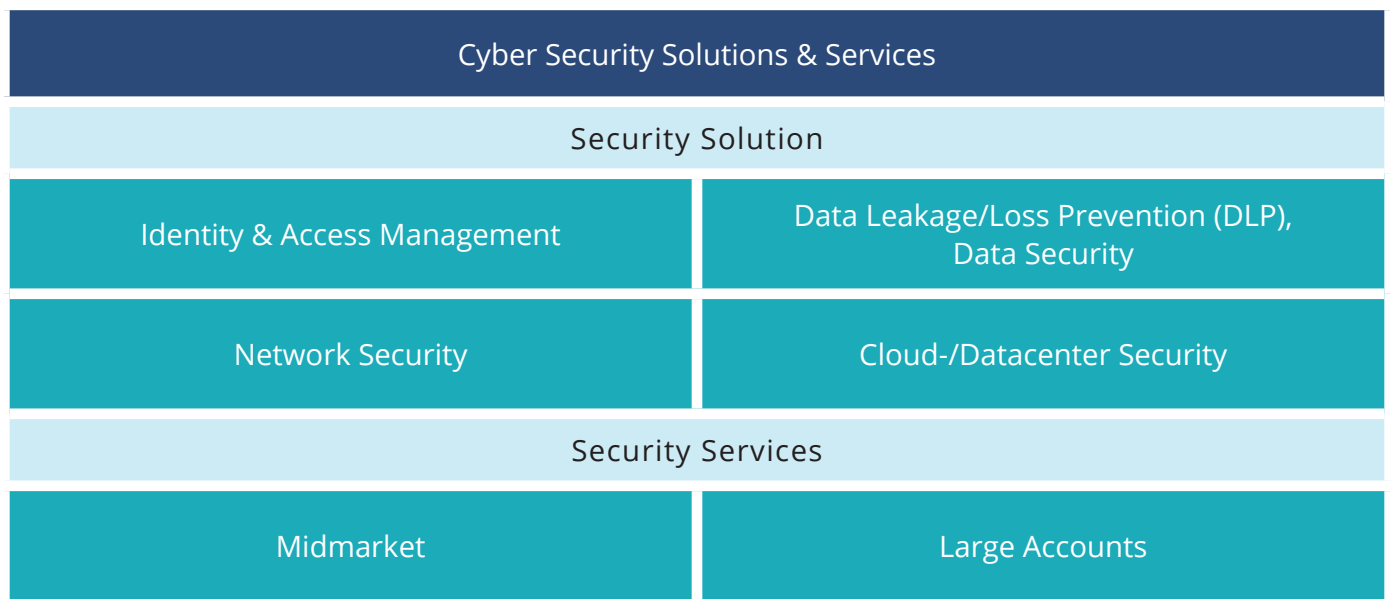
The ISG Provider Lens™ study offers IT-decision makers:

- Transparency of strengths and weaknesses of relevant providers;
- A differentiated positioning of providers by market segments;
- Focus on the German market.

This study serves as an important decision-making basis for positioning, key relationships, and go-to-market considerations. ISG advisors and enterprise clients also leverage information from these reports while evaluating their current vendor relationships and potential new engagements.

# Quadrant Research

As part of the ISG Provider Lens™ quadrant study, we are introducing the following six quadrants on Cyber Security.



## Identity & Access Management

Identity & access management (IAM) products are used to collect, record and administrate user identities and related access rights. They ensure that access rights are granted, based on defined policies. To handle existing and new application requirements, security providers are increasingly challenged to embed mechanisms, frameworks and automation, e.g., risk analyses, into their management suites to provide real-time user and attack profiling functionality. Additional requirements are related to social media and mobile users to address clients' security needs that go beyond traditional web- and context-related rights management. Includes cloud services by product providers.

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

Data leakage/loss prevention (DLP) refers to products for the identification and monitoring of sensitive data to ensure that they can only be accessed by authorized users and to prevent data leakage. DLP products are gaining importance, since it becomes increasingly difficult for companies to control data movements and data transfers. The number of (mobile) devices within companies that can be used to store data is increasing; these devices are mostly equipped with their own Internet connection and can send and receive data without using the central Internet gateway. Devices also are supplied with a multitude of interfaces (e.g., USB, Bluetooth, WLAN, NFC), which can also be used to share data. Includes cloud services by product providers.

## Network Security

Enterprise networks are exposed to all kinds of attacks, from unauthorized access to computers by external parties to attacks attempting to interrupt the company's services (DoS/DDoS) and risks related to carelessness of the company's own employees. If a company is "worth" the trouble, attackers are increasingly investing great efforts and use highly sophisticated means to intrude deeply into the network infrastructure and use such cyber attacks (advanced persistent threats) to spy out sensitive data over a longer period of time without being detected.

Network security products have been designed to address these risks. Within the context of this study, network security is defined as measures to protect physical network infrastructures, including wireless LANs. Includes cloud services by product providers.

## Cloud-/Datacenter Security

The cloud / datacenter security category comprises products to defend against IT infrastructure attacks or threats – independent of whether they are installed in the cloud (private, public, hybrid or multi-cloud) or on-premise. Includes cloud services by product providers.

## Security Services

Security services cover services for security solutions. Services include consulting, training, integration, maintenance, support or management security services. Managed security services comprise the operations and management of an IT security infrastructure for one or several customers by a security operations center. The midmarket target group comprises companies with at least 50 up to 4,999 employees. The large accounts target group comprises companies with at least 5,000 employees. This analysis examines services that do not have an exclusive focus on the respective provider's own proprietary products. Includes cloud services by providers that are not product providers.

A large, light blue geometric graphic consisting of several overlapping shapes, including a large triangle and a smaller square, positioned on the right side of the page.

### **Research production disclaimer:**

ISG collects data for the purposes of writing research and creating provider/vendor profiles. The profiles and supporting data are used by ISG advisors to make recommendations and inform their clients of the experience and qualifications of any applicable provider/vendor for outsourcing work identified by the clients.

This data is collected as part of the ISG FutureSource process and the Candidate Provider Qualification (CPQ) process. ISG may choose to only utilize this collected data pertaining to certain countries or regions for the education and purposes of its advisors and not to produce ISG Provider Lens reports.

These decisions will be made based on the level and completeness of information received directly from providers/vendors and the availability of experienced analysts for those countries or regions. Submitted information may also be used for individual research projects or for briefing notes that will be written by the lead analysts.

# Schedule

The research phase falls in the period between **March** and **May 2019** during which survey, evaluation, analysis, and validation will take place. The results will be presented to the media in **July 2019**.

<b>Milestones</b>	<b>Beginning</b>	<b>End</b>
Launch	February 2019	
Survey Phase	March 11, 2019	April 05, 2019
Sneak previews	June 04, 2019	
Content provisioning	June 28, 2019	
Press release	July 01, 2019	

Please refer to the link below to view/download the Provider Lens™ 2019 Research Agenda :

[https://isg-one.com/docs/default-source/default-document-library/isg-provider-lens-annual-plan-2019.pdf?sfvrsn=c323cc31\\_0](https://isg-one.com/docs/default-source/default-document-library/isg-provider-lens-annual-plan-2019.pdf?sfvrsn=c323cc31_0)



## Contact



Frank Heuer  
Lead Author



Jan-Niklas Hombach  
Global Project Manager

Do you need any further information?

If you have any questions, please do not hesitate to contact us at [isglens@isg-one.com](mailto:isglens@isg-one.com).