ISG Provider Lens™

Cyber Security Solutions and Services 2019

Definition

Facebook's data leakage affair attracted the public's attraction to data security again. This is a very striking example for an unwanted use of data, but not comparable to the permanent criminal threats data and IT infrastructure are exposed to. 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.

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.
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 – 2019 Cyber Security Solutions and Services" addresses both areas to support ICT decision-makers to help them make the best use of their (tight) security budgets.

This new study will examine traditional topics and providers of future-oriented security technologies as well as security service providers.

Again, this year's ISG Cyber Security Provider Lens provides a detailed and differentiated overview of key ICT security providers.

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

- Transparency of strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments
- Focus towards the US and German market

Our 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 in 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 8 quadrants on Cyber Security Solutions and Services.

Simplified presentation

Source: ISG 2018

Identity and Access Management (IAM)

Identity and 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 (software as a service) by product providers, based on own software.

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 (software as a service) by product providers, based on own software.

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 (software as a service) by product providers, based on own software.

Datacenter and Cloud Security

The datacenter and cloud 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 (software as a service) by product providers, based on own software.

Pervasive and Predictive Security

Pervasive and predictive security products deal with pervasive, comprehensive protection. Predictive security has its origins in the network security arena, and the combination of both disciplines has caused a change of paradigms towards comprehensive security products, consisting of an overall set of enterprise-wide security technologies, combined with the ability to secure identities and data across the whole range of products, make predictions on and assess the risks of new technologies and services and their delivery. Includes cloud services (software as a service) by product providers, based on own software.

Endpoint Security

Endpoint security products can be used to ensure the security of clients and their interfaces within the network. Mobile security as a part of endpoint security refers to the protection of mobile processes, applications and devices (such as smartphones, tablets, laptops) and connecting networks against threats and vulnerabilities. Includes cloud services (software as a service) by product providers, based on own software.

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 (software as a service) by providers that are not product providers.

Schedule

The research phase is between **April and July 2018** during which survey, evaluation, analysis and validation will take place. Selected results will be presented to the media in **September 2018**.

We will roll out the survey on an online platform called Qualtrics. The invites will be sent with links to fill in the responses and submit.

Milestones	Beginning	End
Launch	March, 2018	
Survey (questionnaire)	April 12, 2018	May 17, 2018
Sneak previews	August 13, 2018	
Content provisioning	September 20, 2018	
Press release	September 27, 2018	

Contact

Frank Heuer

Lead Author and Senior Advisor
Cyber Security Solutions and Services

Shachi Jain

Regional Author and Senior Analyst
Cyber Security Solutions and Services

Jan-Niklas Hombach

Global Project Manager
Cyber Security Solutions and Services

Do you need any information?

If you have any questions, please do not hesitate to contact us at isglens@isgone.com.

About ISG

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; technology 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 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.