ISG Provider Lens™

Cyber Security Solutions and Services

Security Services

U.S. 2019

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

October 2018

Customized report courtesy of:

LTI
Let's Solve

About this Report

Information Services Group, Inc. is solely responsible for the content of this report.

Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by and are the sole property of Information Services Group, Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that was current as of September 2018. ISG recognizes that many mergers and acquisitions have taken place since that time but those changes are not reflected in this report.

The lead author for this report is Shachi Jain. The editor is Jan Erik Aase.

ISG Provider Lens™

ISG Provider Lens™ delivers leading-edge and actionable research studies, reports and consulting services focused on technology and service providers' strength 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.

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.

EXECUTIVE SUMMARY

Many companies' focus on cybersecurity is increasing as they embrace digitalization and the Internet of Things (IoT). Organizations, irrespective of size and industry, are constantly under attack, and regulatory authorities are strengthening laws to protect data. As more and more behemoths like Facebook face data leakage incidents, companies, regulators and the public alike are paying more attention to data protection and privacy issues. As all this is happening, internal risks are also increasing because of factors including the rise of shadow IT, a lack of employee education about information security, and increasingly sophisticated attacks. Many successful breaches, especially Trojan and phishing attacks, are caused by users' thoughtless behavior.

Still, IT executives often struggle to justify security investments to management, and it is not always possible to prove the ROI of security investments. Consulting services and user training continue to play key roles in helping organizations protect their systems and data, especially when training and consulting are combined with up-to-date IT and communications equipment.

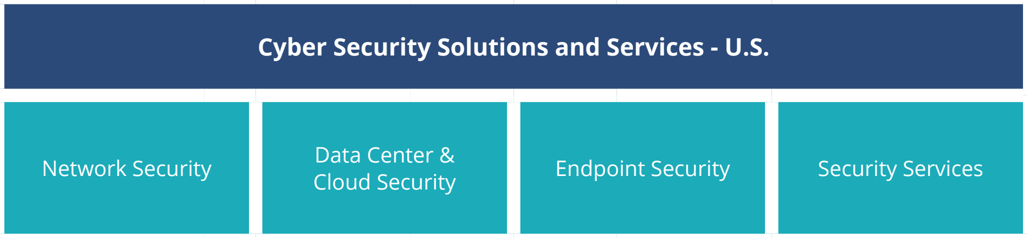
Some of the key trends ISG is observing in the U.S. cybersecurity market are summarized below.

- **Lack of qualified talent:** As hackers use more sophisticated methods and tools to launch attacks, organizations are facing a huge challenge in finding skilled employees to mitigate the threats. While finding the required talent is a major problem, companies are also facing challenges in retaining their skilled employees. Enterprises are increasingly looking toward service providers to act as business partners that will help them address the talent shortage by provisioning training modules and providing skilled labor.
- **Digital deception tools gaining prominence:** Digital deception continues making inroads among mainstream buyers as enterprise leaders re-evaluate the effectiveness of spending for on-premises security information and event management (SIEM), cloud security operations centers (SOC),threat hunting and threat intelligence services, and attempt to rationalize their cyber detection, analysis and response portfolios. Enterprises are increasingly investing in sophisticated detection tools that can help them learn about the potential impact of an attack while keeping their internal resources safe.
- **Cloud-based security services gain traction:** IT security spending is shifting toward cloud and related as-a-service managed and professional services. Workload virtualization has become mainstream and demand for virtualized security is accelerating to support cloud migrations, ranging from single application workload subscriptions to entirely outsourced data centers.

- **Machine learning (ML) and artificial intelligence (AI) applied to security:** Attacks need to be detected in real time, which requires comprehensive monitoring of physical and virtual infrastructure environments whether they are in the cloud or in an internal data center. Automated incident response has become the new normal in security operations centers as security automation and orchestration products account for significant security spending. The demand for real-time threat analytics and intelligence is increasing. Applying AI and ML in threat intelligence tools helps in identifying patterns to develop more robust and proactive security management systems.

Introduction

Simplified illustration


Cyber Security Solutions and Services - U.S.
Network Security
Data Center & Cloud Security
Endpoint Security
Security Services

Source: ISG 2018

Definition

This study examines traditional topics and providers of future-oriented security technologies plus security service providers. The ISG Provider LensTM study offers IT-decision makers:

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

Security solutions examined within this study include respective hardware, software and cloud services provided by product vendors. Security services are services provisioned for managing security solutions for the clients and include monitoring and management of intrusion detection systems and firewalls, patch management and upgrades, security assessments and security audits, and emergency response in case of cyber-attacks. That category also includes cloud services by providers that are not product providers.

Definition (cont.)

Scope of the Report

Network Security

Enterprise networks are exposed to all kinds of attacks, from attempted unauthorized access to computers by external parties to attempts to interrupt the company's services (DoS/DDoS), and they are also exposed to risks related to the carelessness of the company's own employees. Attackers are increasingly investing great effort and using highly sophisticated methods to intrude deeply into network infrastructure and use such cyberattacks (advanced persistent threats, or APTs) to spy on sensitive data over a long period of time without being detected.

Network security products have been designed to address these risks and challenges. Within the context of this study, network security is defined as measures to protect physical network infrastructures, including wireless LANs.

Networks are exposed to multiple kinds of threats, which must be fought with the best available tools. Within this analysis, a broad scope of network security functionality has been examined accordingly, including protection against advanced persistent threats (APTs), protection against denial of service (DoS) and distributed denial of service (DDoS) attacks, intrusion detection systems (IDS) and intrusion prevention systems (IPS) to protect against network attacks and encrypted network connectivity (VPN). Functionality is not related to specific individual products. Rather, there are solutions for unified threat management that combine multiple functionalities within a single appliance and are especially suited for midmarket requirements. Next-generation firewalls also integrate additional functionality such as IPS. This category also includes cloud services by product vendors.

Definition (cont.)

Data Center & Cloud Security

The Data Center & Cloud Security category comprises products to defend against attacks and other threats to IT infrastructure – independent of whether the infrastructure is in the cloud (private, public, hybrid or multi-cloud) or on-premise. This category also includes cloud services provided by product vendors.

Endpoint Security

Endpoint security products can be used to ensure the security of client devices and their interfaces within the network. Mobile security refers to the protection of mobile processes, IoT devices, applications and devices such as smartphones, tablets and laptops, and their connecting networks against threats and vulnerabilities. This category also includes cloud services offered by product vendors, based on their own software.

Security Services

The Security Services category covers services provisioned for security solutions. These services include consulting, training, integration, maintenance, support and managed security services. Managed security services comprise the IT security infrastructure operations and management for one or multiple customers by a security operations center. This analysis examines services that do not have an exclusive focus on the respective provider's own proprietary products (instead the focus is on independent security services). This category also includes cloud services by providers that are not product vendors.

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 have therefore still 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 mostly product challengers with high future potential. When receiving the "Rising Star" award, such companies have a promising portfolio, including the required roadmap and an adequate focus on key market trends and customer requirements. Also, the "Rising Star" has an 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 12-24 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.

Cyber Security Solutions and Services - Quadrant Provider Listing 1 of 4

	Network Security	Datacenter and Cloud Security	Endpoint Security	Security Services
Accenture	● Not In	● Not In	● Not In	● Leader
Atos	● Not In	● Not In	● Not In	● Product Challenger
Attivo Networks	● Rising Star	● Not In	● Not In	● Not In
AVG	● Not In	● Not In	● Market Challenger	● Not In
Barracuda Networks	● Leader	● Leader	● Not In	● Not In
CA	● Not In	● Market Challenger	● Not In	● Not In
Capgemini	● Not In	● Not In	● Not In	● Product Challenger
Check Point	● Leader	● Product Challenger	● Not In	● Not In
Cisco	● Leader	● Leader	● Market Challenger	● Not In
Cognizant	● Not In	● Not In	● Not In	● Product Challenger
Computacenter	● Not In	● Not In	● Not In	● Product Challenger
ESET	● Not In	● Not In	● Product Challenger	● Not In
Cigniti	● Not In	● Not In	● Not In	● Contender

Cyber Security Solutions and Services - Quadrant Provider Listing 2 of 4

	Network Security	Datacenter and Cloud Security	Endpoint Security	Security Services
F Secure	● Not In	● Contender	● Product Challenger	● Not In
FireEye	● Not In	● Product Challenger	● Market Challenger	● Not In
Forcepoint	● Product Challenger	● Not In	● Not In	● Not In
Fortinet	● Product Challenger	● Product Challenger	● Product Challenger	● Not In
Fujitsu	● Not In	● Not In	● Not In	● Product Challenger
HCL	● Not In	● Not In	● Not In	● Leader
Huawei	● Market Challenger	● Not In	● Not In	● Not In
IBM	● Leader	● Leader	● Not In	● Leader
Infosys	● Not In	● Not In	● Not In	● Leader
Juniper Networks	● Market Challenger	● Leader	● Not In	● Not In
Kaspersky	● Not In	● Not In	● Leader	● Not In
Lastline	● Contender	● Not In	● Not In	● Not In
LogRhythm	● Not In	● Product Challenger	● Not In	● Not In

Cyber Security Solutions and Services - Quadrant Provider Listing 3 of 4

	Network Security	Datacenter and Cloud Security	Endpoint Security	Security Services
LTI	● Not In	● Not In	● Not In	● Rising Star
Matrix42	● Not In	● Not In	● Product Challenger	● Not In
McAfee	● Market Challenger	● Market Challenger	● Leader	● Not In
Microfocus	● Not In	● Product Challenger	● Not In	● Not In
Microsoft	● Not In	● Not In	● Market Challenger	● Not In
NTT	● Not In	● Not In	● Not In	● Leader
Owl Cyber Defense	● Contender	● Not In	● Not In	● Not In
Palo Alto Networks	● Leader	● Leader	● Product Challenger	● Not In
Rapid7	● Not In	● Product Challenger	● Rising Star	● Not In
Secureworks	● Not In	● Not In	● Not In	● Leader
Sentinel One	● Not In	● Not In	● Product Challenger	● Not In
SonicWall	● Product Challenger	● Not In	● Not In	● Not In
Sophos	● Product Challenger	● Not In	● Not In	● Not In

Cyber Security Solutions and Services - Quadrant Provider Listing 4 of 4

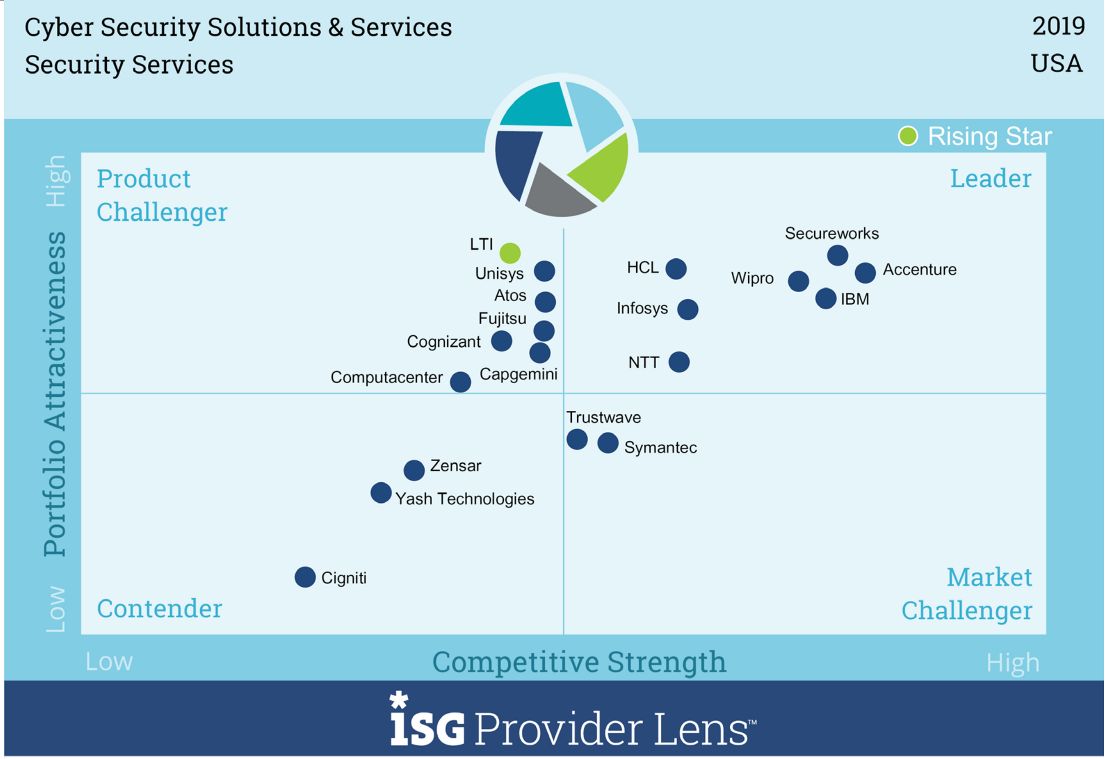
	Network Security	Datacenter and Cloud Security	Endpoint Security	Security Services
Splunk	● Not In	● Leader	● Not In	● Not In
Symantec	● Not In	● Leader	● Leader	● Market Challenger
Trend Micro	● Leader	● Market Challenger	● Leader	● Not In
Trustwave	● Not In	● Market Challenger	● Not In	● Market Challenger
Unisys	● Not In	● Not In	● Not In	● Product Challenger
WatchGuard	● Product Challenger	● Not In	● Not In	● Not In
Webroot	● Not In	● Not In	● Contender	● Not In
Wipro	● Not In	● Not In	● Not In	● Leader
Yash Technologies	● Not In	● Not In	● Not In	● Contender
Zensar	● Not In	● Not In	● Not In	● Contender

Cyber Security Solutions and Services Quadrants

SECURITY SERVICES

Definition

The Security Services category covers services provisioned for security solutions. These services include consulting, training, integration, maintenance, support and managed security services. Managed security services comprise the IT security infrastructure operations and management for one or multiple customers by a security operations center. This analysis examines services that do not have an exclusive focus on the respective provider's own proprietary products (the focus is on independent security services). This category also includes cloud services by providers that are not product vendors.



Source: ISG Research 2018

SECURITY SERVICES

Observations

- To be successful in the highly complex and challenging security services market, providers must have international experience with a broad scope of solutions and should be able to support their clients accordingly. Providers such as Accenture, IBM and Secureworks distinguish themselves through their large teams with international experience.
- Clients are increasingly interested in managed security services that provide comprehensive support and help in handling their security systems. Wipro, Infosys and HCL have made significant investments in new age technologies like automated incident response, advanced threat analytics and proactive threat management driven by artificial intelligence and machine learning to cater to this requirement.
- NTT offers security consulting and managed services through a single managed security service platform that leverages security capabilities from all the company's subsidiaries.
- L&T Infotech's (LTI's) strong focus on intelligent cybersecurity services that are driven by AI and analytics help it offer faster incident response in security operation centers and a holistic view of the threat landscape through visibility across stages of a kill chain.

RISING STAR: LTI

Overview

Larsen & Toubro Infotech (LTI) started its cybersecurity practice in 2017 and delivers Cyber Defense Resiliency Consulting and Managed Security Services globally.

Strengths

Layered approach to end-to-end managed security service: LTI has developed a five-layer Cyber Defense Resiliency system based on its Mosaic platform to offer a holistic and proactive security management solution. The solution covers threat detection and vulnerability management at an early attack stage and also offers cyber risk management, multi-cloud threat defense, mobile threat defense, advanced threat deception with security automation and orchestration, and IoT/OT cyber threat defense.

AI-driven cyber analytics: The company's cyber defense solution provides real-time visibility to enable rapid response to a cyber threat and leverages artificial intelligence in the exploitation phase for reduced response times. The ability to leverage AI-driven threat hunting and detection capabilities helps in early detection and enhances the threat vulnerability management offering.

Threat intelligence based on machine learning: The Cyber Defense Resiliency system provides threat intelligence at the dark web level. It uses machine learning extensively to run behavioral analytics on threats and offer predictive vulnerability management.

Caution

LTI has a strong portfolio of security services; however, the company needs to invest in marketing its next-generation cyber threat management capabilities and grow its footprint in the U.S. market.

2019 ISG Provider Lens™ Rising Star

LTI leverages artificial intelligence and machine learning to ensure its threat detection and management capabilities are updated and help deliver proactive risk management and holistic security operations for clients.

Methodology

METHODOLOGY

The ISG Provider Lens™ 2018 – Cyber Security Solutions & Services research study analyses the relevant software vendors and service providers in the US 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 Cyber Security Solutions & Services
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

Shachi Jain, Supporting Author

Lead Analyst, ISG Provider Lens™

Shachi Jain is an analyst focusing on research in digital transformation, F&A outsourcing and Internet of Things. She is responsible for handling custom research assignments and analyst reports pertaining to these areas. She has authored a few reports on the impact of digital technologies on workplace services and IoT services adoption in retail sector. She has also been responsible for vendor assessments, thereby helping ISG clients with key strategic insights around market trends and service providers' capabilities in these areas.

Jan Erik Aase, Editor

Editor

Jan Erik Aase is a director and principal analyst for ISG. He has more than 35 years of collective experience as an enterprise client, a services provider, an ISG advisor and analyst. Jan Erik has overall accountability for the ISG Provider Lens™ reports, including both the buyer-centric archetype reports and the worldwide quadrant reports focused on provider strengths and portfolio attractiveness. He sets the research agenda and ensures the quality and consistency of the Provider Lens™ team.

ISG Provider Lens™ | Quadrant Report
October 2018