ISG Provider Lens™

Manufacturing Security Solutions

OT Security Solutions

A research report comparing software vendor strengths, challenges and competitive differentiators

Customized report courtesy of:

ARMIS

QUADRANT REPORT | DECEMBER 2022 | GLOBAL

Table of Contents

Report Author: Avimanyu Basu

OT security and mobility security solutions witness soaring demand.

OT SECURITY SOLUTIONS

Advances in machine-to-machine (M2M) technology and machine learning have led to radical changes in operational technology (OT). Factories with inherent automation are realizing its benefits in the form of predictive maintenance and improvements in machine life, quality and volume throughput. However, many enterprises depend on a complex mix of legacy OT and connected technologies, which has created gaps in security. This has also led to factories retrofitting solutions into legacy systems. With increasing adoption of industrial IoT (IIoT) and connected IoT devices, companies are in a growing need for security that would not only ensure seamless operations but also avoid the risks of cyber breaches. This means that legacy OT systems must be fortified with security extensions to ensure continuity of operations and prevent downtime that results from security attacks.

The adoption of OT security technologies in some companies in the manufacturing industry is higher than others, and they are actively working to mitigate vulnerabilities. Healthcare, utilities and manufacturing companies being a few of them. Attacks on COVID vaccine manufacturers, wherein attackers tried to fabricate the vaccine formula, prompted the life science market to address such vulnerabilities by setting up a dedicated security operations center (SOC) for OT. In the past, automotive and other heavy industries have stayed away from OT security implementations and, as a result, have fallen prey to malicious attacks.

OT and mobility security are **hotbed of innovations.**

For instance, a Japanese automotive company faced a cyberattack a few months ago, causing several of its plants to go offline and resulting in millions of dollars in losses. Nowadays, several advanced attack tools are freely available, which can be used to launch cyber-physical attacks against infrastructure systems. Such cyberattacks are compelling heavy industries to invest heavily in OT security across their manufacturing facilities.

Enterprises usually prefer security solutions that can be scaled and applied to their on-premises cloud and specialized networks, such as a fuel sensor network in an oil refinery. Two main types of security solutions for OT are gaining interest, namely, (1) accurate detection and proactive derailment of threats and (2) decoy and deception of attackers. The first kind represents OT security solutions that can manage and secure all types of devices via an open platform. They proactively address issues such as resetting passwords, changing configurations, reverting to original settings and upgrading firmware. On the other hand, advanced deception technologies prevent attacks by firstly disrupting the discovery activity of attackers and providing them with fake information that leads to their derailment. They then raise an alert along with the information required for fast remediation.

In a typical plant, these two technologies operate in tandem, with comparatively limited decoy-based deployment. Most enterprises today are opting for visibility and monitoring solutions, while some segments have started exploring solutions with managed deception. Some other trends witnessed by ISG are as presented below.

ISG witnesses a rapid shift toward adoption of digital technologies in the OT segment. Manufacturing environments with heavy OT equipment and other legacy infrastructure have started adding digital components. Similarly, factories, oil platforms and refineries are also introducing digitization, AI and cloud. Therefore, customer requirements in the OT space have changed over time, and end-to-end OT solutions are gaining traction. ISG predicts that the next level of evolution in the OT security space will be around big data. Technology suppliers are anticipated to work extensively with enterprises with a stable cloud infrastructure to collect information. Similar information from multiple customers, especially in the manufacturing sector, will be used to create a data lake, on which machine learning algorithms can be applied to provide additional insights and recommendations.

MOBILITY SECURITY SOLUTIONS

An exponential rise in the number of reported automotive cyberattacks indicates that mobility security is critical to counter threats in connected cars. A successful attack can cause irreversible damage to the OEM's reputation. Many lean technology suppliers have emerged globally that want to leverage the cybersecurity-related disruption in the automotive industry. Thus, multinational OEMs and Tier-1s support these technology providers and use their services to help protect millions of vehicles. The launch of security regulations, such as WP.29 by The United Nations Economic Commission for Europe (UNECE) and ISO 21434 in 2020, has been a major driver for these businesses. The OEMs and Tier-1s are seeking solutions to comply with this regulation. Several companies (such as Upstre0am Security) not only monitor and protect vehicles but

also maintain intelligence analyst teams to research and stay updated on the latest incidences and vulnerabilities.

Companies such as Regulus Cyber conducted several R&D exercises across mobility industries (for e.g., automotive and aerospace) with widely available tools, such as free online software. These companies imitated the attacks on global positioning system (GPS), which were taking place globally and proved that any system can be hacked; this highlighted the severity of the problem. For instance, Regulus Cyber did an experiment on a Tesla, where it used a global navigation satellite system (GNSS) spoofing to take control of a vehicle steering and speed and managed to divert the vehicle into incoming traffic. Several vulnerabilities concerning the use of satellite-based navigation and timing across GNSS receivers, which are embedded in high-end systems, have been exposed by these companies. Teams conducting these tests were able to take control of timing systems using traditional spoofing methods and used this to control drones that were trying to enter certain parameters. Global Tier-1s, such as Harman, are integrating products from these emerging players (such as Pyramid GNSS from Regulus Cyber) as a part of their cybersecurity offering to provide an end-to-end security solution, spanning GNSS spoofing and connected threats.

In the automotive cybersecurity segment, ISG witnessed developments in two main categories, which are the two ways to enter a vehicle's decision-making system — connected threats (through the Internet) and sensor threats (attacks that exploit the use of sensors on smart vehicles). A few emerging companies, such as Argus Cyber Security, offer solutions and services that protect the electronic control units (ECUs) or door control units (DCUs), vehicle communication model, telematics, etc., from connected threats. GNSS, which consists of the U.S. GPS, the Russian GLONASS, the European Galileo and the Chinese BeiDou systems, is prone to sensor threats. GNSS is at the core of multiple technologies, and approximately 70 percent of the world's GPS depend on the timing and location of GNSS. Thus, if the GNSS signal is interrupted, it can lead to catastrophic failure of different systems, such as malfunctioning of force positioning and guided ammunitions in the defense sector. Some automobiles use all four of these constellations simultaneously and, thus, fall prey to GNSS spoofing and jamming — the most serious threats on satellite-based navigation and timing. Jamming involves ways of blocking the signal, and spoofing corresponds to manipulating the signal. The world has faced GNSS spoofing and jamming incidents across industries, such as aviation, automotive and maritime, as well as in consumer electronics such as mobile phones.

From a market evolution perspective, the involvement of new players can be expected. Orolia, InfiniDome and Javad are a few other GNSS interference specialists, which, however, do not focus on automotive. Their involvement in the mobility cybersecurity segment and a greater level of integration between GNSS service providers, such as u-blox and Furuno, and security solution providers can be expected in the future.

Innovative startups are mushrooming in the global security space.

Provider Positioning

Page 1 of 4

	Mobility Security Solutions	OT Security Solutions
Airbus	Not In	Market Challenger
Argus Cyber Security	Leader	Not In
Armis	Not In	Leader
Attivo Networks	Not In	Leader
AUTOCRYPT	Contender	Not In
C2A	Product Challenger	Not In
CENTRI	Contender	Not In
Cisco (Cyber Vision)	Not In	Market Challenger
Claroty	Not In	Leader
CYMOTIVE	Leader	Not In

Provider Positioning

Page 2 of 4

	Mobility Security Solutions	OT Security Solutions
Darktrace	Not In	Product Challenger
Dellfer	Rising Star ★	Not In
Dragos	Not In	Product Challenger
ESCRYPT	Market Challenger	Not In
FireMon	Not In	Product Challenger
Forescout	Not In	Product Challenger
GuardKnox	Leader	Not In
Industrial Defender	Not In	Leader
Irdeto	Product Challenger	Not In
Karamba Security	Leader	Not In

Provider Positioning

Page 3 of 4

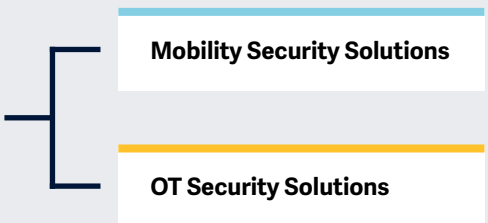
	Mobility Security Solutions	OT Security Solutions
Kaspersky	Not In	Product Challenger
Microsoft (CyberX)	Not In	Market Challenger
Mocana Corporation	Product Challenger	Not In
Nozomi Networks	Not In	Leader
OPSWAT (Bayshore Networks)	Not In	Contender
Penta Security	Product Challenger	Not In
Red Balloon Security	Product Challenger	Contender
Regulus Cyber	Leader	Not In
Sabanci (Radiflow)	Not In	Leader
SCADAfence	Not In	Leader

Provider Positioning

Page 4 of 4

	Mobility Security Solutions	OT Security Solutions
SheeldS	Leader	Not In
SIGA	Not In	Product Challenger
SynSaber	Not In	Rising Star ★
Tenable	Not In	Leader
Upstream Security	Leader	Not In
Vector	Market Challenger	Not In
Zscaler (Smokescreen)	Not In	Product Challenger

This study focuses on critical aspects of **Manufacturing Security Solutions.**



Simplified Illustration Source: ISG 2022

Definition

The Manufacturing Security Solutions 2022 study tracks and analyses offerings related to OT, IoT, IIoT and mobility security to enable effective cybersecurity. The study examines solution providers or product vendors that address the security challenges of enterprises depending on a complex mix of legacy OT and connected technology. These challenges are primarily driven by the accelerated adoption of IIoT and connected IoT devices plus the integration of retrofitted solutions that integrate with legacy systems. These security solutions should typically ensure seamless operations and avoid the risks of cyber breaches. This means that legacy OT systems must be fortified with security extensions to ensure continuity of operations and avoid downtime arising from security attacks.

In the past, heavy industries such as automotive have stayed away from OT security implementations and are subsequently exposed to malicious attacks. These industries are compelled to provide board-level funding for OT security across their manufacturing facilities. United Nations Economic Commission for Europe (UNECE) has come up with the World Forum for Harmonization of Vehicle Regulation (WP.29) guideline that mandates cybersecurity for every new vehicle variant launching in 2022 and for every individual vehicle starting in 2024. It is worth noting that the WP.29 guideline overlaps with the ISO 21434 standards. In addition to vehicle development, the standards span the entire lifecycle to include manufacturing, organizational and development processes, and the supply chain. The study also analyses these mobility security businesses in terms of new-age technologies such as vehicle vulnerability management solutions for the vehicle fleet lifecycle, intrusion detection solutions to identify compromised components within a vehicle network, and management dashboards for real-time security intelligence and visibility.

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following two quadrants on OT Security Solutions and Mobility Security Solutions.

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

- Transparency on the strengths and weaknesses of relevant solution vendors
- A differentiated positioning of providers by segments
- Focus on regional market

Our study serves as the basis for important decision-making in terms of positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing vendor relationships and potential engagements.

Provider Classifications

The provider position reflects the suitability of IT providers/ software vendors for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions IT providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly.

Each ISG Provider Lens quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

Number of providers in each quadrant: ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).

Provider Classifications: Quadrant Key

Product Challengers offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not in means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.

OT Security Solutions

Who Should Read This

This report is relevant to industrial, manufacturing and overall OT ecosystem players, including OEMs, component suppliers, distributors and contract manufacturers, that are evaluating cybersecurity solution providers.

In this quadrant, ISG lays out the current market positioning of the providers of OT security solutions and how they address the key challenges enterprises face, globally.

ISG observes that the traditional OT security market is niche and mature, with focused products that address legacy industrial platforms and networks. As these legacy systems evolve into cyber-physical systems, their security becomes strategically important for both OT and IT stakeholders.

Enterprises are facing a scarcity of skilled engineers in the market and are struggling to improve their security budgets to have a certified workforce that can monitor and counter cyberthreats in-house. As a result, they are currently looking to outsource these responsibilities to external firms that specialize in OT cybersecurity.

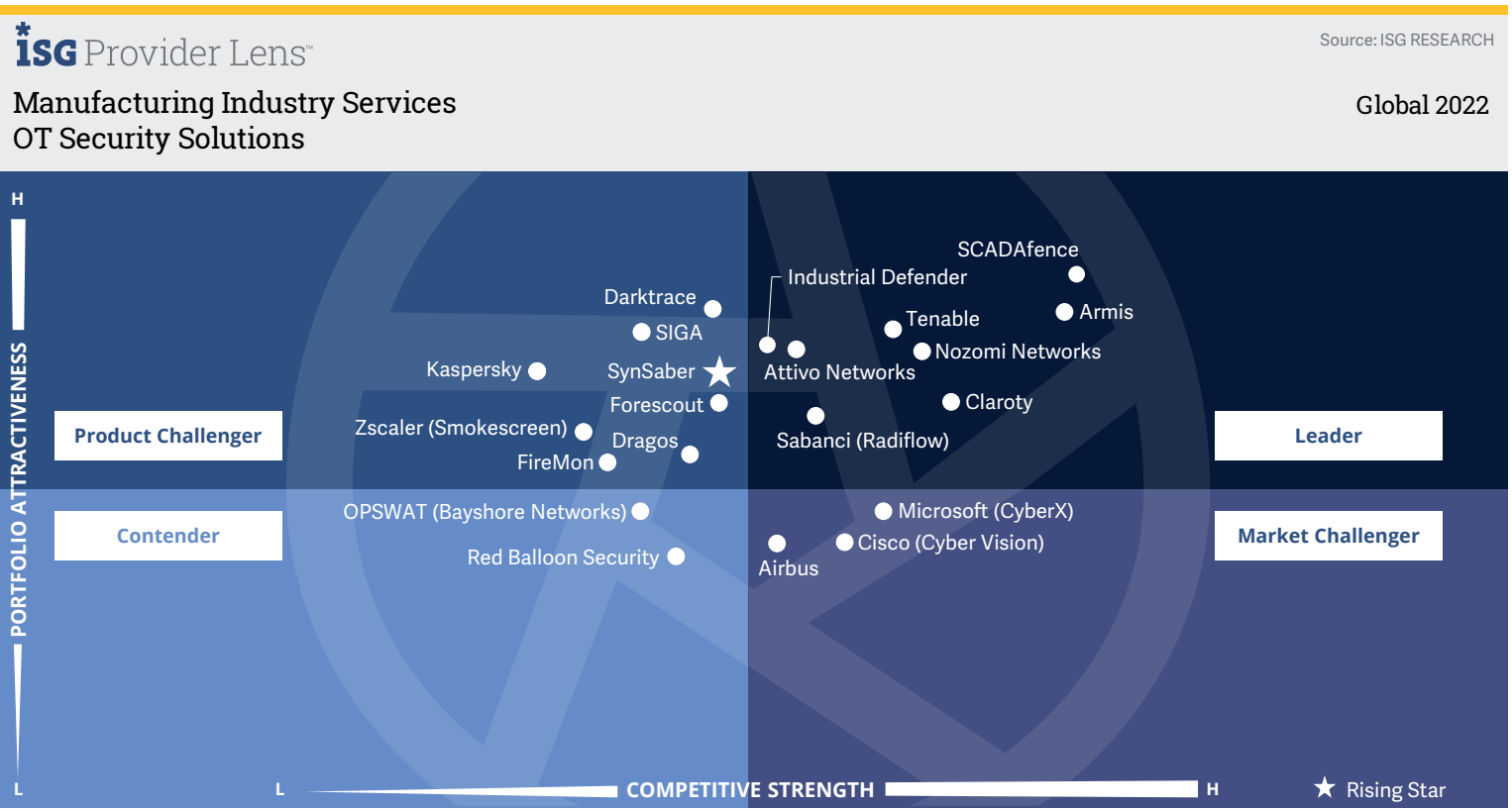
The growing importance of OT security and its direct relationship with enterprise risk management have led enterprises to recognize the need for sourcing solutions from an expert provider. Globally, there is an increased need for acquisitions and strategic partnerships among traditional OT security solution providers to meet the demand for comprehensive cybersecurity solutions.

IT leaders should read this report to understand the relative positioning and capabilities of providers that can help them effectively assess needs and deploy OT security solutions. The report also shows how a service provider's technical and integration capabilities and partnerships compare with others in the market.

Security leaders in charge of online infrastructure and physical assets should read this report to understand how service providers address the specific and significant challenges related to securing data, sensors and other connected systems that make up production automation in a manufacturing environment.

Manufacturing professionals should read this report to learn more about the domain expertise of service providers and how they connect the services offered to enterprises' legacy machinery and technologies to support their approaches.

Product engineering leaders should read this report to understand the relative positioning and capabilities of providers that can help them plan and select cybersecurity services and solutions. The report also shows how a provider's technical and integration capabilities are compare to others in the market.



OT security is gradually evolving into a **decision-making factor** for enterprises in **selecting service providers** and **system integrators.**

Avimanyu Basu

Definition

OT can be defined as the suite of hardware and software that monitors and controls the activities of equipment in a manufacturing environment. OT systems such as industrial control systems for heavy industries, which include manufacturing, transportation and utilities that have been in existence for decades, are traditionally not connected, thereby making them redundant (or obsolete) in the modern, advanced networked infrastructure. The lack of automation in legacy mechanical systems necessitates manual operation of equipment, log collection and monitoring. With the emergence of smart, connected devices, providers have more control over these systems. The growth of machine-to-machine (M2M) technologies and machine learning has led to a radical change in industry dynamics, wherein setups are geared toward autonomy.

The benefits are being realized in the form of preventive maintenance that improves machine longevity. ISG analyzes the security solutions offered by a solution provider to monitor Modbus, Profibus, Ethernet traffic and proprietary traffic and protect OT components such as PLC, human-machine interface (HMI), SCADA software, physical equipment, machine control systems and remote industrial software that are not connected to the external world.

Eligibility Criteria

1. Have offerings in **at least one segment of OT security**, for example, monitoring and visibility or decoy and deception technologies
2. Demonstrate capabilities in at least few of the functions, including **asset discovery, vulnerability management, threat detection, NGFW (next-generation firewall) and zero trust**
3. Have a track record of providing seamless security against **all kinds of data breaches** in the manufacturing campus or networks
4. Ability to **integrate complex and emerging technologies**, including network technologies, into an overall security solution
5. Demonstrate the capacity to **rapidly innovate and stay apace** with the latest threats from the rapidly advancing community of cybercriminals

Observations

Several enterprises have been deploying OT security solutions for several years now but still lack complete visibility into infrastructure assets. They gain visibility only into a few OT and IT elements but not the IoT and IIoT assets, mobile devices and wireless devices. Thus, the demand for easy-to-deploy enterprise-class solutions that can display all assets without compromising on the operations is increasing. Furthermore, enterprises need to have control over their infrastructure and must simultaneously use the collective, correlated intelligence of all other deployed solutions, such as Qualys, Cisco ISE, configuration management databases (CMDBs), Rapid 7 and security information management (SIM) technologies. The need for more value out of the existing IT security investments has led to increased demand for enterprise-grade, easy-to-deploy and single-pane-of-glass solutions that provide unified visibility across infrastructure assets and add value immediately.

From the 85 companies assessed for this study, 22 have qualified for this quadrant, with eight being Leaders and one Rising Star.

Attivo Networks

Attivo Networks specializes in accurate detection and proactive derailment of security concerns using its unique deception technology. The solution raises alerts with information required for fast remediation.

Armis

The evolution of the OT threat landscape and anatomy of modern attacks depict the criticality of unified visibility across OT and IT, IoT and IIoT devices. Several enterprise customers are, thus, gravitating toward **Armis** to have this visibility, along with the provision of in-depth knowledge about the existing infrastructure.

Claroty

A close connect with the OT world enables **Claroty** to reverse-engineer OT protocols and use them. Furthermore, the company partners with IT security specialists to offer end-to-end enterprise security solutions.

Industrial Defender

Once a part of Lockheed Martin, **Industrial Defender** considers cyber resilience as the foundation of enterprise functions and provides modular offerings to clients. It offers its platform-as-a-service enablement tool that supports client service teams assigned for cybersecurity assignments.

Nozomi Network

Nozomi Network's flagship product, Guardian, which is a management console, centralizes visibility and monitoring. The Guardian console drives functionalities such as Smart Polling for active monitoring, threat intelligence to update Guardian appliances and asset intelligence to recognize the device behavior prior to installing solutions.

Sabanci (Radiflow)

Enterprises often face challenges while transferring information from industrial sub-networks from small or remote sites into the analytics engine, which results in limited coverage of the threat landscape. **Sabanci (Radiflow)** collects information from remote sub-networks and ensures extensive coverage for the detection system.

SCADAfence

The **SCADAfence** platform is a passive solution that provides visibility into the OT side, depicting connectivity between machines, the protocols used, the network subnet, location of devices and overall asset management.

Tenable

Indegy's portfolio has been seamlessly integrated into **Tenable's** capabilities, expanding the breadth of the company's OT-specific capabilities in areas such as vulnerability management, asset inventory, configuration management and threat detection.

SYNSABER

SynSaber (Rising Star) enables enterprises to avoid the complexities of getting a new SIM solution for OT data and instead brings the OT data into the existing infrastructure of the enterprise.

Leader

"Armis is an "all assets-all environments" security specialist that provides optimum visibility."

Avimanyu Basu

Armis

Overview

Armis, based in California, U.S., was acquired by Insight Partners in 2020. The company provides agentless, enterprise-class, passive cloud-based solutions to protect managed, unmanaged, OT, IT, IIoT and IoT devices. The Armis solution provides end-to-end visibility of business-critical assets in the enterprise network, especially unmanaged devices that cannot accommodate a traditional security agent. The company provides solutions to customers from different cross-sections of the enterprise ecosystem globally.

Strengths

Value proposition around data collection and processing: The key differentiator of the Armis platform for asset discovery and network monitoring is its innovative ways of data collection. Collectors are placed where they can consume Switched Port Analyzer/ Test Access Point (SPAN/TAP) traffic from switches and wireless LAN controllers. Collectors process network traffic and telemetry data from different integrations in real time, extracting details about all devices connected to the network. No raw data or payloads (PII/HPI) is sent to the Armis SaaS. As the solution does not process the data at the collectors that are deployed onsite, it is not restricted by any processing capability and allows quick scalability.

Granularity in information about assets: The Armis platform integrates seamlessly with the enterprise IT and security technology stack, enabling it to source information about various devices that are included in the network. It provides intelligence on the vulnerability of the assets, their owners, and their physical locations. This holistic visibility provides relevant insights into the organization's security status.

Caution

Armis had its inception when IoT devices were being inducted into the enterprise network. It was created to address the need for a solution that could detect the vulnerabilities of the devices. As the enterprise landscape evolved into a converged environment of IT, OT and IoT components, the holistic visibility offered by Armis became critical to assess the security status of the organization. However, due to its origin in IoT security, Armis is often considered an IoT security specialist.

Appendix

Methodology & Team

The ISG Provider Lens™ 2022 – Manufacturing Security Solutions analyzes the relevant solution vendors in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Lead Author:
Avimanyu Basu

Editor:
Upasana Hembram

Research Analyst:
Varsha Sengar

Data Analyst:
Pooja Rani Nayak

Consultant Advisors:
John Lytle and Christian Decker

Project Manager:
Ridam Bhattacharjee

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 ISG believes to be current as of November 2022, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars ($US) unless noted.

The study was divided into the following steps:

1. Definition of Manufacturing Security Solutions 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. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
   * Strategy & vision
   * Tech Innovation
   * Brand awareness and presence in the market
   * Sales and partner landscape
   * Breadth and depth of portfolio of services offered
   * CX and Recommendation

Author

Avimanyu Basu
Senior Lead Analyst

Avimanyu Basu brings over 10 years of extensive research experience to handle telecommunication and engineering and R&D services specific research deliverables for the program called ISG Provider Lens™ that is designed to deliver research on service provider intelligence. He is responsible for authoring reports on software defined networks and network function virtualization (SDN/NFV) and engineering services.

He is also responsible for key vertical-oriented reports and thought leadership papers for manufacturing along with whitepapers revolving around specialized technologies showcased by different cross-section of enterprises.

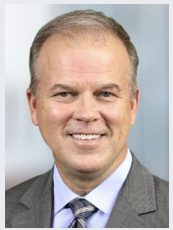
Research Analyst

Varsha Sengar
Senior Research Analyst

Varsha Sengar is a senior research analyst at ISG and is responsible for supporting and co-authoring Provider Lens™ studies on Intelligent Automation, Software Defined Networking, and Workday Ecosystem. She has over 5 years of experience in the technology research industry and in her prior role, she has carried out. She supports the lead analysts of multiple regions in the research process and authors the global summary.

She is responsible for delivering an enterprise perspective for IPL and collaborates with analysts, advisors, and enterprise clients on various ad-hoc requests which include primary and secondary research. Her area of expertise lies across various technologies like IoT, Artificial Intelligence, Smart Homes, and Autonomous Driving.

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a partner and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens research, please visit this webpage.

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.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the 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.

ISG Provider Lens™

DECEMBER, 2022

REPORT: MANUFACTURING SECURITY SOLUTIONS