ISG Provider Lens™

Manufacturing Industry Services

OT Security Solutions

Global 2021

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

December 2021

Customized report courtesy of:

SCADAfence

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 ISG believes to be current as of November 2021, 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 lead author for this report is Avimanyu Basu. The editors are Sajina B and John Burnell. The research analyst is Srinivasan PN and the data analyst is Kankaiah Yasareni. The Quality and Consistency Advisors are John Lytle, Gaurav Gupta, Vishnu Andhare, Doug Saylors and Doug Glair.

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

OT Security Solutions

As the world recovers from the COVID-19 pandemic, advances in machine-to-machine (M2M) technology and machine learning have led to radical changes in operations technology (OT). Factories with inherent automation are realizing benefits in the form of predictive maintenance and improvements to machine life, quality and volume throughput. However, many enterprises depend on a complex mix of legacy OT and connected technology that has created a security gap. This has led to factories retrofitting solutions to integrate with legacy systems. With the accelerated adoption of industrial IoT (IIoT) and connected IoT devices, companies are facing a growing need for security protections that ensure seamless operations and avoid the risks of cyber breaches. This means legacy OT systems must be fortified with security extensions to ensure continuity of operations and avoid downtime due to security attacks.

Some companies in the manufacturing industry have embraced OT security technology more than others and are actively working to mitigate vulnerabilities. We see healthcare, utilities and manufacturing companies taking these threats most seriously. Recent attacks on COVID vaccine manufacturers, wherein attackers tried to fabricate the vaccine formula, have prompted the life sciences market to address 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. 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. These cyberattacks are compelling heavy industries to provide board-level funding for OT security across their manufacturing facilities. Several advanced attack tools are freely available nowadays, which can be used to launch cyber-physical attacks against infrastructure systems (for example, the Triton attack in Saudi Arabia).

Enterprises usually prefer security solutions than can scale up and be applied to their on-premises, cloud and specialized networks such as the fuel sensor network in an oil refinery. We are seeing a growing interest in two main types of security solutions for OT, which are accurate detection and proactive derailment of threats, and decoy and deception of attackers.

OT security solutions can increasingly manage and secure all device types via an open platform, proactively addressing issues such as resetting passwords, changing configurations, reverting to original settings and upgrading firmware. New deception technologies prevent attacks by disrupting the discovery activity of attackers and then providing them with fake information that leads to their derailment. Finally, the alert is raised with the information required for fast remediation.

In a typical plant, these two technologies operate in parallel 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 of the other trends witnessed by ISG are as presented below.

Enterprises outgrowing niche OT point solutions and demanding unified visibility across all assets: ISG witnesses a rapid shift in the OT segment. The manufacturing environments with heavy OT equipment and other legacy infrastructure have started adding digital components. Consistently, factories, oil platforms and refineries have been introducing digitization, AI and cloud. Accordingly, the customers in the OT space have different requirements compared to the past and are seeking complete OT solutions.

Demand for best-in-class, unified visibility and risk management across infrastructure assets: 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 some 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, which can show all the assets without compromising on the operations, is increasing. Furthermore, the enterprises require control over their infrastructure and simultaneously use the collective, correlated intelligence of all the other deployed solutions such as Qualys, Cisco ISE, configuration management databases (CMDBs), Rapid 7 and SIM technologies. The need for getting more value out of the existing IT security investments has led to increased demand for enterprise-grade, easy-to-deploy, single-pane-of-glass solutions that provide unified visibility across infrastructure assets and add value immediately.

ISG predicts the next level of evolution in the OT security space to be around big data. The technology suppliers will work extensively with the enterprises with a stable cloud infrastructure to collect information. Similar information from multiple customers, especially on the manufacturing sector, would 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 makes the mobility security scourge a serious threat to connected cars. A successful attack can cause irreversible damage to the OEM's reputation. Many lean technology suppliers have emerged globally that tend to leverage the cybersecurity-related disruption in the automotive industry. Thus, multinational OEMs and Tier 1s support these technology providers and use them to help protect millions of vehicles. The launch of security regulations such as WP.29 by UNECE and ISO 21434 in 2020 has been a major driver for these businesses. The OEMs and Tier 1s would, thus, need to prepare themselves and are seeking solutions to comply with this regulation. Several companies (such as Upstream) not only monitor and protect the vehicles, but also maintain an intelligence analyst team that researches the automotive industry to be up to the minute on the latest incidences and vulnerabilities.

Companies such as Regulus Cyber conducted several R&D exercises across mobility industries (e.g. automotive and aerospace) with widely available tools like free software that is available online. The companies imitated the attacks on GPS that were taking

place globally and proved that any system can be hacked, highlighting the severity of the problem. Regulus, for example, did an experiment on a Tesla where it used GNSS spoofing to take control of the vehicle steering and speed and managed to divert the vehicle into incoming traffic. Several vulnerabilities around utilizing satellite-based navigation and timing across GNSS receivers embedded in high-end systems have been exposed by these companies, where a team was able to take control of timing systems using traditional spoofing methods to control drones that are trying to enter certain parameters, etc. 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.

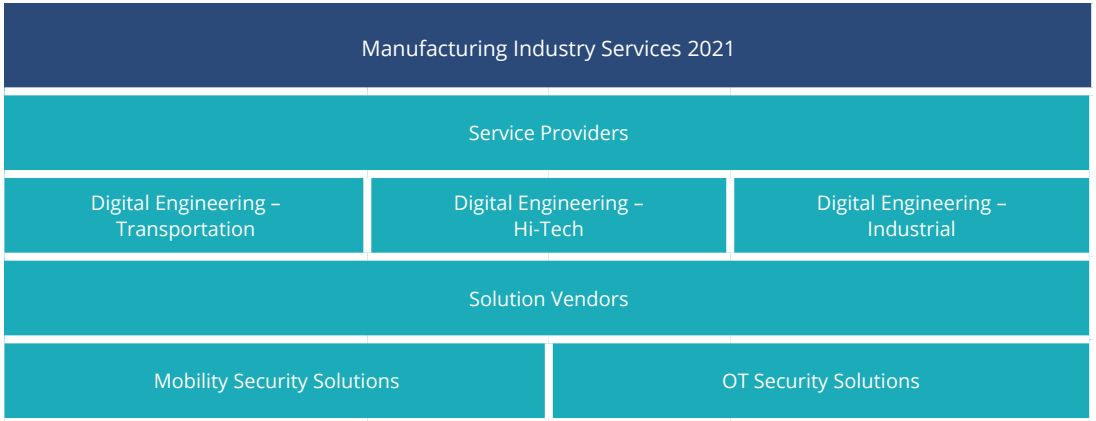
In the automotive cybersecurity segment, ISG witnessed development in the two main categories that are the two ways to enter the vehicle decision-making system — connected threat (through the Internet) and sensor threat (attacks that exploit the use of sens ors on smart vehicles). Some of the emerging companies such as Argus Cyber Security offer solutions and services that protect ECUs/DCUs, the vehicle communication model, telematics, etc., from connected threat. Global Navigation Satellite System (GNSS), which consists of the U.S. GPS, the Russian GLONASS, the European Galileo and Chinese BeiDou systems are prone to sensor threats. GNSS is at the core of multiple technologies, and approximately 70 percent of the world's GPS depends on the timing and location of GNSS. Thus, if the GNSS signal is interrupted, it can lead to catastrophic failure of different sys- tems 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 largest threats on satellite-based navigation and timing. Jamming represents 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, maritime as well as in consumer electronics such as mobile phones.

From a market evolution perspective, 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.

Several companies such as Argus Cyber Security are offering solutions to detect intrusion in the network arena, which, in turn, enables OEMs to integrate sensors throughout the vehicle for collecting information from various ECUs and other systems and send the information to the vehicle SOC. In case an action is required, the OEMs can respond with a security configurations update or an over-the-air (OTA) software update. The former option is generally faster as it does not involve the chain of processes involved in the latter. Security configurations updates skip the testing and validation of the loose solution before the rollout, while the OTA software update solution tends to be more holistic as it can be used for any firmware or software other than cybersecurity.

Introduction

Simplified illustration



Source: ISG 2021

Definition

The Manufacturing Industry Services 2021 study tracks and analyzes the offerings around several elements of manufacturing, from the intricacies of product engineering, spanning design and development to the pilot scale production to industry scale, shop floor manufacturing and remote product operations. Considering the entire lifecycle of a product, ranging from whiteboarding, 3D simulation to shop floor robotics, ISG tends to analyze the major disruptions taking place in the industry. Automation plays a significant role here, spreading across components such as manufacturing operations management (MOM) and manufacturing execution systems (MES), as well as capturing process data and storing it in the cloud or inside the new edge. Service providers have been working extensively on shop floor transformation and integrated product development. They are bringing together electrical, electronic, mechanical, embedded and software components with conventional mechanical, electronics and electrical engineering. This has resulted in a combination

Definition (cont.)

of MES and product lifecycle management (PLM) solutions with cutting-edge machine-to-machine (M2M) connectivity and AI-driven insights. The solutions use insights to drive the underlying product and manufacturing engineering for the IoT stratagem.

The study examines the role of service and solution providers across the entire value chain of the manufacturing industry — including product engineering, spanning design capabilities and pilot scale implementations, virtual layout or simulation of the shop floor, ergonomics for machinery, IT and operational technology convergence, and aftermarket services. It also analyzes providers' capabilities around after-sales support, such as leveraging digital twins to check the condition of machinery while it reaches the wear-out period of the wear curve.

ISG sets out to deliver a comprehensive research program with clear and extensive evaluation criteria, covering the developments and deliverables of service providers and solution suppliers in this dynamic market. This study accounts for changing market requirements and provides a consistent market overview for the segments, along with concrete decision-making support, to help user organizations evaluate and assess the offerings and performance of providers.

Scope of the Report

The ISG Provider Lens study offers IT, engineering, manufacturing, procurement and CDOs as well as R&D decision-makers the following:

- Transparency on the strengths and weaknesses of relevant services and solution providers
- Differentiated positioning of providers by segments
- Perspective on several markets, including global, the U.S. and Europe.

Our study serves as an important decision-making basis for positioning, key relationship and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current vendor relationships and potential engagements available.

Quadrant Research

As part of this ISG Provider Lens™ quadrant study, we are introducing the following five quadrants on Manufacturing Industry Services, as shown in the graphic below. Each regional report may not cover every quadrant.

Provider Classifications

The provider position reflects the suitability of IT providers 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 US$20 million and US$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 US$1 billion, with activities worldwide and globally distributed decision-making structures.

Provider Classifications

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.

Leader

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.

Product Challenger

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.

Market Challenger

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.

Contender

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 both products and services and a sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Provider Classifications (cont.)

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).

Rising Star

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

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.

Manufacturing Industry Services - Quadrant Provider Listing 1 of 3

	Mobility Security Solutions	OT Security Solutions
Argus Cyber Security	Leader	Not In
Arilou	Leader	Not In
Armis	Not In	Leader
Attivo Networks	Not In	Leader
Autocrypt	Contender	Not In
OPSWAT (Bayshore Networks)	Not In	Contender
C2A	Product Challenger	Not In
Centri	Contender	Not In
Cisco (Sentryo)	Not In	Market Challenger
Claroty	Not In	Leader
CYMOTIVE	Leader	Not In
Darktrace	Not In	Product Challenger

Manufacturing Industry Services - Quadrant Provider Listing 2 of 3

	Mobility Security Solutions	OT Security Solutions
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
Irdeto	Product Challenger	Not In
Karamba Security	Leader	Not In
Kaspersky	Not In	Product Challenger
Microsoft (CyberX)	Not In	Market Challenger
Mocana Corporation	Product Challenger	Not In
Nozomi Networks	Not In	Leader

Manufacturing Industry Services - Quadrant Provider Listing 3 of 3

	Mobility Security Solutions	OT Security Solutions
Optiv	Not In	Market Challenger
Penta Security	Product Challenger	Not In
Pratum	Not In	Contender
Radiflow	Not In	Leader
Regulus Cyber	Leader	Not In
SafeRide	Contender	Not In
SCADAfence	Not In	Leader
SIGA OT	Not In	Rising Star
Tenable	Not In	Leader
Upstream Security	Leader	Not In
Vector	Market Challenger	Not In
Zscaler (Smokescreen)	Not In	Product Challenger

Manufacturing Industry Services Quadrants

ENTERPRISE CONTEXT

OT Security Solutions

This report is relevant to the industrial, manufacturing and overall OT ecosystem players such as OEMs, component suppliers, distributers and contract manufacturers for evaluating cybersecurity solution providers.

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.

As OT cybersecurity is a top priority, many enterprises face difficulties expanding their security budgets to cover enough full-time employees to monitor and respond to cyberthreats in-house. They also may have difficulty finding employees fit for the job, because there is a significant shortage of cybersecurity skills in the market.

As enterprises start to realize the extent of the skill shortage and their budget gaps, many of them look into outsourcing those responsibilities to other firms specializing in OT cybersecurity. Notable acquisitions and strategic partnerships with traditional OT security solution providers are accelerating to meet the demand for comprehensive cybersecurity solutions.

Enterprises recognize the increasing importance of OT security and how it relates to enterprise risk management. The growth of strategic security services is being driven by the need to independently document compliance with adopted security frameworks and local regulations, identify and prioritize gaps, develop a security strategy that meets enterprise objectives, and lay out an implementation roadmap.

IT leaders should read this report to understand the relative positioning and capabilities of providers that can help them effectively assess needs and deploy production automation solutions on the shop floor. The report also shows how service providers' technical and integration capabilities, as well as partnerships, compare with the rest in the market.

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

Product engineering manufacturing technology leaders should read this report to understand the relative positioning and capabilities of providers to help them effectively plan and select cybersecurity-related services and solutions. The report also shows how the technical and integration capabilities of a service provider compare with the rest in the market.

Digital transformation professionals should read this report to understand how providers of OT cybersecurity solutions fit their digital transformation initiatives and how they compare with one another.

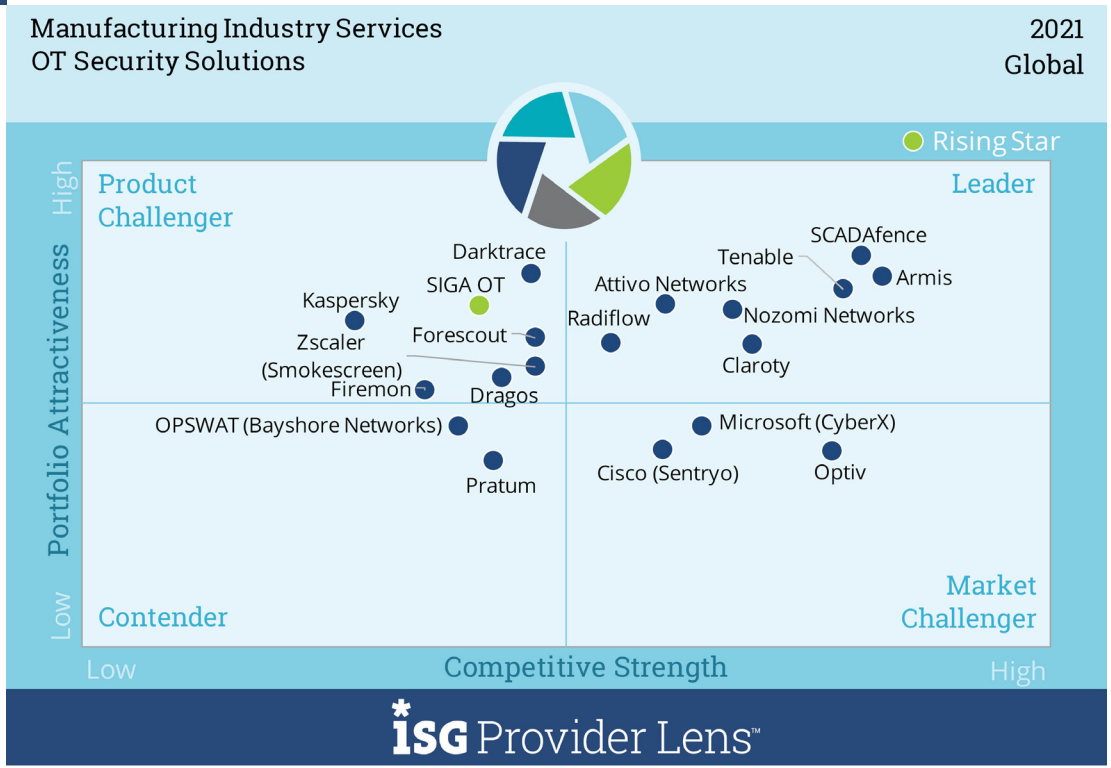
Engineering and R&D services professionals should read this report to develop a better understanding of the current landscape of OT cybersecurity solutions.

Security analysts and leaders should read this report to see how solution providers address the significant challenges associated with compliance and security.

OT SECURITY SOLUTIONS

Definition

Operational technology (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 (ML) has led to a radical change in industry dynamics, wherein setups are gearing 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.



Source: ISG Research 2021

OT SECURITY SOLUTIONS

Eligibility Criteria

- Have offerings in at least one segment of OT security, for example, monitoring and visibility or decoy and deception technologies
- Have a track record of providing seamless security against all kinds of data breaches in the manufacturing campus or networks
- Ability to integrate complex and emerging technologies, including network technologies, into an overall security solution
- Demonstrate the capacity to rapidly innovate and stay apace with the latest threats from the rapidly advancing community of cyber criminals

Observations

- **Armis'** agentless security platform is used to discover, identify and classify assets by connecting to the network environment. The solution provides high visibility on the devices connected to the network, down to make, model, operating system, version, etc., and accordingly correlates that to a second function such as the risks, gaps and vulnerabilities.
- **Attivo Networks** has been constantly expanding the library of devices that it can host, emulate and support. The company has been operating an environment architected to run any operating system, providing customers with the ability to customize the environment as per their convenience.
- **Claroty's** newly enhanced portfolio with Continuous Threat Detection (CTD) 4.1 and Secure Remote Access (SRA) 3.0 solutions effectively addresses OT risk with enhanced visibility, threat detection, vulnerability management, as well as triage and mitigation.

OT SECURITY SOLUTIONS

Observations (cont.)

- **Nozomi Networks** has showcased several vulnerability discoveries and its capability in making its own common vulnerabilities and exposures (CVEs), which complement its threat reporting proficiency. The company has leveraged the intelligence to enhance its products and has made it available to its customers for anomaly detection.
- **Radiflow's** tool is focused on risk analytics. It tends to be a game-changer in the OT security space as it guides customers on the mode of action following detection system deployments. Radiflow's solution has enabled customers to prioritize the alerts and work on the mitigation.
- **SCADAfence's** proprietary platform provides a holistic view of the system on a dashboard, highlighting the vulnerabilities against each asset by leveraging locally stored machine data and other types of advanced analytics. The customers can conveniently feed this data to their SOC with application programming interface (API) integration.
- **Tenable** specializes in protecting industrial control system (ICS) networks from cyber threats, malicious insiders and human error. Its Industrial Cybersecurity Suite equips security and operations teams with optimal visibility, security and control of ICS activities and threats with an innovative combination of hybrid, policy-based monitoring, network anomaly detection and device integrity checks.
- **SIGA OT Solutions (Rising Star)** has been engaged at the proof of concept (POC) level and eventually emerged as a turnkey partner for large-scale processes due to its strong skills in creating value in OT monitoring and visibility.

SCADAFENCE

Overview

SCADAfence is an Israel-based OT and IoT cybersecurity technology supplier with a presence in the U.S., Germany and Japan.

Strengths

Expansive detection and response solution extended to IT/OT governance and compliance: 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. The company has enhanced it further with the SCADAfence Governance portal, which takes the passive data existing in the network. Enabling customers to find their degree of compliance with industry standards such as IEC 62443, ISO 27001, NERC, NIST, CMMC and other important compliances and reporting on them has been a differentiator for SCADAfence.

Improving scalability with SCADAfence multisite portal: Operating multiple monitoring and visibility platforms is inconvenient for customers with multiple global sites. To address this, SCADAfence created a multisite portal that aggregates the different points into a specific dashboard, enabling enterprises to see and control OT assets from a single interface and to push updates centrally. Furthermore, the clients benefit with central configuration, management, licensing and centralized software updates.

Cloud-based, active IoT security offering to fortify enterprise IoT networks: The IoT security product is the latest one in the SCADAfence portfolio. It projects all the IoT devices in a network, along with the providing central management, central orchestration and resetting configurations

Avoiding critical infrastructure network overload and blackouts with DPI: SCADAfence aggregates the network data through port mirroring, taps, RSPAN, Netflows and through sensors. The solution performs deep packet inspection (DPI) on the sensor, so the data extracted in the SCADAfence platform is de-integrated. Instead of collecting the data and pushing it to the platform, the fragmented data is transmitted through the available bandwidth to the platform.

Caution

Compared to other solution providers in the OT security space, SCADAfence has raised less funding. However, the company still continues to gain and expand its prominence in the market.

2021 ISG Provider Lens™ Leader

With OT security DNA integrated into its IoT security solution, productized approach around IT/OT governance and compliance, and proprietary DPI-based technology, SCADAfence is all set to dominate the OT security market.

Methodology

METHODOLOGY

The research study "ISG Provider Lens™ 2021 – Manufacturing Industry Services" analyzes the relevant software vendors/service providers in the global 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 Manufacturing Industry Services market
2. Use of questionnaire-based surveys of service providers/vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities and use cases
4. Use of ISG's internal databases and advisor knowledge and experience (wherever applicable)
5. Detailed analysis and evaluation of services and service documentation based on the facts and figures received from providers and 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

Avimanyu Basu, Author

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.

Srinivasan PN

Senior Research Analyst

Srinivasan PN is a senior research analyst at ISG and is responsible for supporting and co-authoring ISG Provider Lens™ studies on AWS Ecosystem, Insurance BPO, Mainframe and Cybersecurity studies. His area of expertise lies in the space of engineering services and digital transformation. Srinivasan has over 6 years of experience in the technology research industry and in his prior role, he carried out research delivery for both primary and secondary research capabilities. Srinivasan is responsible for developing content from an enterprise perspective and author the global summary report. Along with this, he supports the lead analysts in the research process and writes articles about recent market trends in the industry.

Authors and Editors

Jan Erik Aase, Editor

Partner and Global Head – ISG Provider Lens/ISG Research

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 research director, principal analyst 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™ | Quadrant Report
December 2021

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.