

# Technology Vendor Snapshot for OT Security

June 2022: Complimentary Abstract / Table of Contents



# Our research offerings

This report is included in the following research program(s):

## Cybersecurity

- ▶ Application Services
- ▶ Banking and Financial Services Business Process
- ▶ Banking and Financial Services Information Technology
- ▶ Catalyst™
- ▶ Clinical Development Technology
- ▶ Cloud and Infrastructure
- ▶ Contingent Staffing
- ▶ Contingent Workforce Management
- ▶ Conversational AI
- ▶ Customer Experience Management Services
- ▶ CX Excellence
- ▶ Cybersecurity
- ▶ Data and Analytics
- ▶ Digital Adoption Platforms (DAP)
- ▶ Digital Engineering Services
- ▶ Digital Services
- ▶ Digital Workplace
- ▶ Employee Experience Management (EXM) Platforms
- ▶ Engineering Services
- ▶ Enterprise Platform Services
- ▶ Finance and Accounting
- ▶ Financial Services Technology (FinTech)
- ▶ Global Business Services
- ▶ Healthcare Business Process
- ▶ Healthcare Information Technology
- ▶ Human Resources Outsourcing
- ▶ Insurance Business Process
- ▶ Insurance Information Technology
- ▶ Insurance Technology (InsurTech)
- ▶ Insurance Third-Party Administration (TPA) Services
- ▶ Intelligent Document Processing (IDP)
- ▶ Interactive Experience (IX) Services
- ▶ IT Services Executive Insights™
- ▶ Life Sciences Business Process
- ▶ Life Sciences Information Technology
- ▶ Locations Insider™
- ▶ Marketing Services
- ▶ Market Vista™
- ▶ Mortgage Operations
- ▶ Multi-country Payroll
- ▶ Network Services and 5G
- ▶ Outsourcing Excellence
- ▶ Pricing-as-a-Service
- ▶ Process Mining
- ▶ Procurement
- ▶ Recruitment
- ▶ Retirements Technologies
- ▶ Rewards and Recognition
- ▶ Service Optimization Technologies
- ▶ Software Product Engineering Services
- ▶ Supply Chain Management (SCM) Services
- ▶ Sustainability Technology and Services
- ▶ Talent Excellence GBS
- ▶ Talent Excellence ITS
- ▶ Technology Skills and Talent
- ▶ Trust and Safety
- ▶ Work at Home Agent (WAHA) Customer Experience Management (CXM)

If you want to learn whether your organization has a membership agreement or request information on pricing and membership options, please contact us at [info@everestgrp.com](mailto:info@everestgrp.com)

Learn more about our  
**custom research capabilities**

Benchmarking

Contract assessment

Peer analysis

Market intelligence

Tracking: providers, locations, risk, technologies

Locations: costs, skills, sustainability, portfolios

# Contents

<b>1. Introduction and overview</b>	<b>5</b>
• Research methodology	6
• Introduction	7
<b>2. OT security market overview</b>	<b>8</b>
• Market size	9
• Threat perception of OT/ICS security	10
• Demand drivers	11
– Geography-based	11
– Vertical-based	12
• Key enterprise concerns	13
• Enterprise commentary	14
• PE investments in OT security	15
• Key considerations for enterprise buyers for OT security vendor evaluation	16
<b>3. Tech vendor profiles for OT security</b>	<b>17</b>
• Armis	18
• Cisco	19
• Claroty	20
• Dragos	21
• Forescout	22

For more information on this and other research published by Everest Group, please contact us:

**Kumar Avijit**, Practice Director

**Arjun Chauhan**, Senior Analyst

# Contents

<b>3. Tech vendor profiles for OT security (continued)</b>	<b>5</b>
• Nozomi Networks	23
• Ordr	24
• Radiflow	25
• Scadafence	26
• Tenable	27
<b>4. Appendix</b>	<b>28</b>
• Glossary	29
• Research calendar	30

# Introduction to the research

## Technology vendors for OT security

With the ever-increasing complexity of the cyberattack surface and the evolving global threat landscape, organizations of all types and sizes now need to make conscious efforts to protect their critical data and assets including the OT and ICS.

At Everest Group, we have been tracking the OT security provider market for the past few years. In Q2 2021, we published IT MSS PEAK Matrix Assessment 2021, where we presented an analysis of 28 global service providers providing IT Managed Security Services (MSS). Our published state of the market report on Next gen IT MSS provides an overview of the IT MSS market, typical deal characteristics, enterprise challenges, as well as best practices, and focuses on MDR.

As a part of our ongoing research agenda, this document presents insights into the OT provider ecosystem. This long tail or the specialist OT security providers have gained significant importance over the past few years, as they cater to rising enterprise demand for OT and ICS security. Service providers and enterprises approach these specialist players to bring in OT-specific capabilities to integrate with the larger cybersecurity ecosystem, thereby focusing on IT-OT convergence.

Especially during the pandemic, OT security has gained a lot of traction making these specialist providers an attractive investment destination for the VC and PE community. Most of these providers have been in the business for a few years now and have invested heavily in scaling partner ecosystem, solution development, creating professional services, and have witnessed YoY growth rates exceeding 100%.

### Scope of this report



**Geography**  
Global



**Industry**  
Cross industry



**Services**  
IT Security Services

# This study focuses on leading technology vendors for OT security; below are four charts to illustrate the depth of the report

## Adoption trends for IT, non-voice BPS, and voice-based BPS

### North America

- Demand for better OT cyber resilience, underpinned by the rise in supply chain attacks and ransomware
- Push from the government via regulations such as the IoT Cybersecurity Improvement Act of 2020
- Strong demand push led by verticals such as manufacturing, public sector, and oil and gas

### Europe

- Strong data privacy regulations and higher breach costs
- Europe is considered to be a major manufacturing hub, a vertical that is heavily reliant on IoT and OT devices



### APAC

- Proliferation in digital assets, serving as new attack surface area
- Increased demand for coherent OT solutions to fill security gaps formed by the weak security posture of OT devices

Source: Everest Group (2021)

## Technology building blocks for consumer banks



### Manufacturing

Securing production secrets and minimizing the risk of business disruption, while catering to the needs of IIoT-led digital transformation

### Oil & gas

Averting sophisticated supply chain attacks, while ensuring operations safety and adherence to compliances



### Power utilities

Securing the critical grid assets and substations that are distributed over a large geography, and laying the foundation for IoT readiness



### Transportation

Securing communication over the network while ensuring passenger safety and overall efficiency of the system



### Ports and shipping

Protecting network communication and port assets, while maintaining operational efficiency

## Mix of digital technology leveraged by consumer banks

1

### Threat and asset intelligence

Threat management tools are ineffective without tailored intelligence. Choose vendors that have made investments in in-house OT threat and asset intelligence.



2

Compatibility with existing investments  
choose a solution compatible with the existing investments and can seamlessly integrate with other platform vendors.



3

### Industry use case

choose a solution that can cater to specific use cases for the enterprise's industry vertical rather than a solution with support for generic use cases.



4

### Talent needs

talent remains a key cause of concern within enterprises and service providers. Evaluate carefully if the service provider can support the new tool without any hiccups. Vendor professional services, if available, can aid in talent requirement challenges.



5

### Support for cognitive intelligence

assess offerings that can hunt and analyze threats using behavioral analytics supported by cognitive intelligence rather than leveraging static correlation techniques for threat detection.



## AI elements actively explored by payers

“

Being alerted to vulnerabilities in real-time is a must-have for our manufacturing operations. We need solutions that allow our organization to quickly identify which assets have potential vulnerabilities and prioritize actions we need to take to reduce and eliminate potential risks.

– Vice President, Global Cybersecurity, US-based automobile company

“

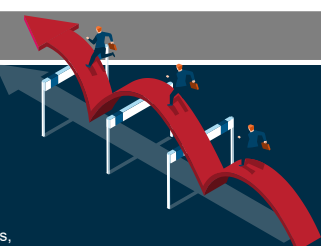
The Colonial Pipeline attack that happened this year has been an eye-opener for us, especially people from our industry. One thing which is very clear now is that as a leader I need to look at ways to be prepared for adversaries like this and certainly we are exploring specialist providers that can provide more visibility and risk profiling.

– Head, IT infrastructure, North American oil and gas company

“

We have been investing in securing our OT environments for a few years now. We are evaluating tools that can provide a single platform for visibility and threat monitoring. But our key criteria has been to ensure that it provides seamless integration with our existing investments.

– Head of cybersecurity initiatives, European utilities major



# Research calendar

## Cybersecurity

Published Planned Current release

Reports title	Release date
Supplier Management Toolkit: Cybersecurity Risk Management in the Supplier Life Cycle	January 2022
Getting to the Bottom of Zero Trust (ZT) Security	April 2022
<b>Technology Vendor Snapshot for OT Security</b>	<b>June 2022</b>
IT Security Services PEAK Matrix® Assessment 2022: North America	July 2022
IT Security Services PEAK Matrix® Assessment 2022: Europe	July 2022
State of the Market: IT Security Services	Q3 2022
IT Security Services North America Compendium 2022	Q3 2021
IT Security Services Europe Compendium 2022	Q3 2021

Note: [Click](#) to see a list of all of our published cybersecurity



Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our research also covers the technologies that power those processes and functions and the related talent trends and strategies. Our clients include leading global companies, service and technology providers, and investors. Clients use our services to guide their journeys to maximize operational and financial performance, transform experiences, and realize high-impact business outcomes. Details and in-depth content are available at [www.everestgrp.com](http://www.everestgrp.com).

## Stay connected

### Website

[everestgrp.com](http://everestgrp.com)

### Social Media

 [@EverestGroup](https://twitter.com/EverestGroup)

 [@Everest Group](https://www.linkedin.com/company/everestgrp)

 [@Everest Group](https://www.facebook.com/EverestGroup)

 [@Everest Group](https://www.youtube.com/EverestGroup)

### Blog

[everestgrp.com/blog](http://everestgrp.com/blog)

### Dallas (Headquarters)

[info@everestgrp.com](mailto:info@everestgrp.com)  
+1-214-451-3000

### Bangalore

[india@everestgrp.com](mailto:india@everestgrp.com)  
+91-80-61463500

### Delhi

[india@everestgrp.com](mailto:india@everestgrp.com)  
+91-124-496-1000

### London

[unitedkingdom@everestgrp.com](mailto:unitedkingdom@everestgrp.com)  
+44-207-129-1318

### Toronto

[canada@everestgrp.com](mailto:canada@everestgrp.com)  
+1-647-557-3475

*This document is for informational purposes only, and it is being provided "as is" and "as available" without any warranty of any kind, including any warranties of completeness, adequacy, or fitness for a particular purpose. Everest Group is not a legal or investment adviser; the contents of this document should not be construed as legal, tax, or investment advice. This document should not be used as a substitute for consultation with professional advisors, and Everest Group disclaims liability for any actions or decisions not to act that are taken as a result of any material in this publication.*