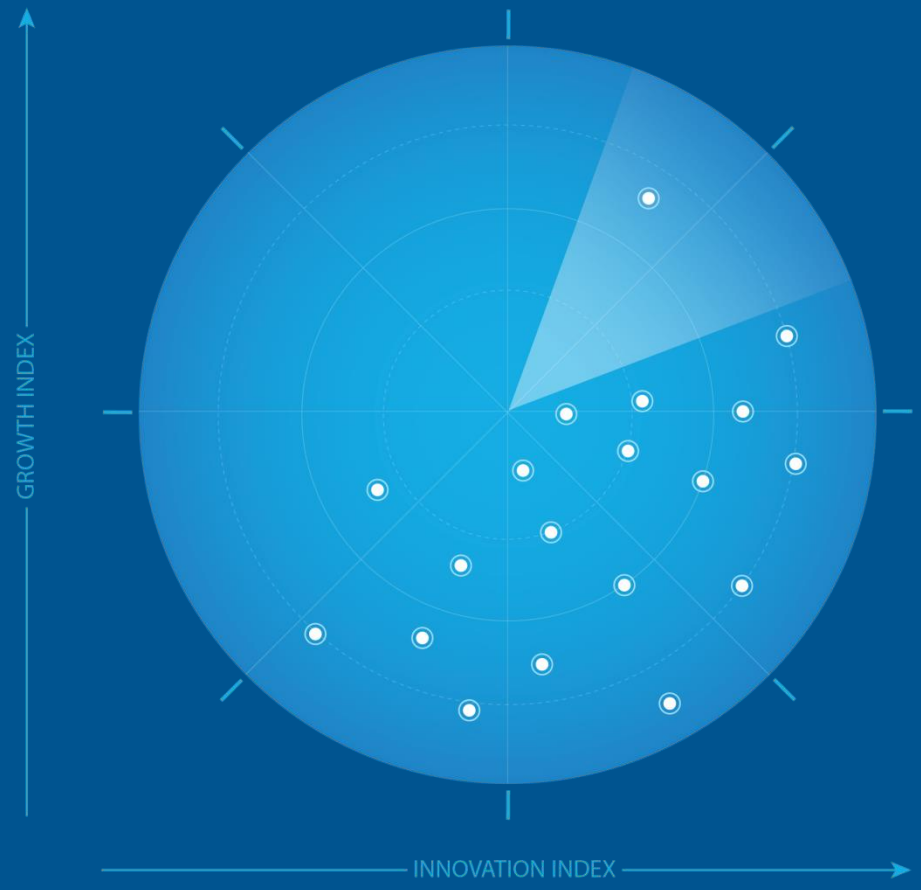
FROST & SULLIVAN

Frost Radar™: Operational Technology Cybersecurity Solutions, 2023

Authored by: Danielle VanZandt

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



December 2023

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Factors Creating Pressure on Growth

- Over the last two decades, significant discussions around cybersecurity typically focused on overcoming how siloed an organization's operational technology (OT) ecosystem was. Businesses typically viewed OT assets as safe from potential cyberattacks because of their disconnect from the larger organizational infrastructure; however, digitalization has folded OT assets and systems into the broader digital infrastructure of a business, albeit without protection.
- Because of IT cybersecurity solutions' gaps when attempting to monitor and protect OT systems and assets, the need for an OT-specific cybersecurity solution took hold among businesses. As such, the OT cybersecurity industry began its rapid growth phase, and the threat landscape grew in parallel, becoming more sophisticated in its attack structure and ability to adapt to available protections.
- Over the last five years, the prevailing hypothesis in the industry was that IT and OT cybersecurity ecosystems would eventually intersect and combine. This belief was further solidified by a host of M&A activity that saw IT cybersecurity vendors jumping into the OT world by attempting to offer converged IT-OT cybersecurity solutions. This strategy resulted in a few successes, but not as many as expected.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- While today's OT cybersecurity options still exist mainly on a parallel path, they can integrate, collaborate, and inform the IT cybersecurity systems and maintain full visibility and awareness of OT environments. This rapid evolution has allowed the OT industry to catch up regarding digital maturity and cybersecurity practices while defending against a more active threat landscape.
- The OT cybersecurity industry continues to evolve in response to this new threat landscape, with the assistance of new regulatory and compliance guidelines that put OT security at the forefront of business operations. With more industry verticals, governing bodies, and critical infrastructure organizations understanding the growing threat landscape, OT cybersecurity solutions are no longer seen as a nice-to-have but a business continuity best practice.

Source: Frost & Sullivan

Growth Environment

- As the need for OT cybersecurity continues to grow in the face of new and evolving digital threats, more businesses are realizing how OT solutions can safeguard their operations and mitigate vulnerabilities already in their environments. With more market verticals embracing OT cybersecurity solutions, spending on these solutions was $5.27 billion in 2022 and is projected to reach $38.87 billion globally by 2030.
- The OT cybersecurity solutions market is reaching a new phase in which specific vendor groups are forming around a standard set of functions and capabilities. In focusing on OT visibility and mitigation platforms, key functions that customers seek include:
  - threat assessment tools, such as risk prioritization, compliance auditing, and automated policy enforcement;
  - visibility tools (such as asset discovery and inventory tools) and configuration management capabilities;
  - threat remediation capabilities such as vulnerability management, threat detection and mitigation, continuous monitoring, and backup and recovery tools;
  - flexible platforms to deploy in converged IT-OT environments, embedded endpoint security tools, built-in zero-trust functionality, and an open ecosystem for partner integrations.

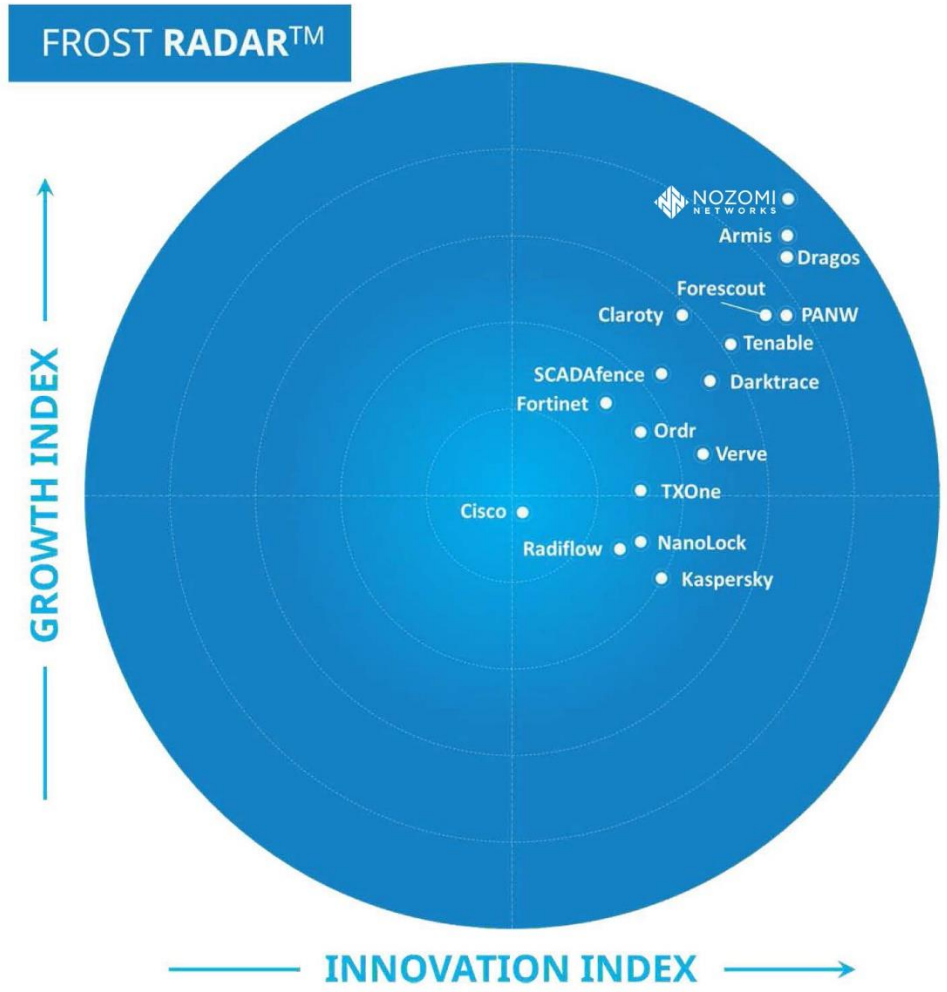
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Operational Technology Cybersecurity Solutions, 2023

Frost Radar™: Operational Technology Cybersecurity Solutions, 2023



Source: Frost & Sullivan

Competitive Environment

- The OT cybersecurity solutions ecosystem has grown rapidly in the past decade as it plays catch-up with the IT cybersecurity industry regarding digital maturity and technological capability. Alongside this growth in new customers and industries embracing OT security solutions, the vendor landscape for OT cybersecurity solutions has created more specific categories based on core functionality:
  - risk assessment tools to understand threats to a business;
  - visibility and mitigation platforms that allow for real-time discovery and response to detected threats;
  - OT cybersecurity services to conduct consultations on OT security best practices; managed security services for OT systems; and other third-party security assistance.
- To allow for a fair comparison of vendors, this Frost Radar analysis focuses solely on visibility and mitigation platform vendors. From a competitive landscape of more than 100 vendors, this analysis highlights the 17 that offer comprehensive platforms for customers across multiple industries to help them understand their current operational landscape and equip them with the tools to detect and mitigate threats in real-time.

Source: Frost & Sullivan

Competitive Environment (continued)

- Leading all vendors on the Frost Radar, Nozomi Networks achieves a perfect score (5 out of 5) in both Innovation and Growth because of its impressive year-over-year revenue growth, strong brand presence through partnerships and thought leadership, and a regular cadence of updates and capability enhancements to its Vantage, Arc, and Guardian solutions.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

Companies to Be Considered First for Investment, Partnerships, or Benchmarking

Company to Action: Nozomi

Innovation

- Nozomi Networks rightfully earns its top spot on the Frost RadarTM due to its OT security portfolio's breadth and match to customer needs across all critical infrastructure sectors. The company offers multiple visibility and threat detection solutions that can fit into any customer environment and a range of threat visibility, detection, mitigation, configuration management, and policy compliance measures requested by customers.
- Vantage, the company's cloud-powered OT and IoT risk management and configuration platform offers the latest in threat intelligence, managed detection and response functions, and internal policy management tools to enhance a customer's operational resilience strategy. Nozomi Guardian provides the network visibility and comprehensive asset inventory necessary for compliance and risk assessment procedures. In contrast, the Nozomi Central Management Console provides an on-premises operational risk management and resilience platform to customers needing to manage their architecture on-site.

Source: Frost & Sullivan

Company to Action: Nozomi (continued)

Innovation

- Nozomi's platforms exist modularly, allowing customers to build a combination of components that fit their operational environment. Additional platform suites include Nozomi Arc, which extends visibility and asset management tasks to the endpoint level; Vantage IQ, which offers AI-powered analysis and response capabilities to Vantage customers, serving as a force multiplier for security teams; Asset and Threat Intelligence modules to provide additional context behind common attack vectors or vulnerabilities active today; and Smart Polling functionality to conduct active polling of suspected devices or vulnerable assets to determine their risk.

Source: Frost & Sullivan

Company to Action: Nozomi

Growth

- Nozomi Networks was among the first vendors to build up the OT cybersecurity industry to what it is today. Since its founding, Nozomi Networks has focused on those critical infrastructure organizations that needed to secure their vital OT networks and systems, even before these businesses realized the risks they were facing. This entrenched brand reputation for OT cybersecurity at its core, plus Nozomi's feature-rich offerings that can fit any customer's operational architecture, have helped the company to almost double its revenue each year through new client acquisition and continued sales.
- Nozomi Networks is staking its market leadership through its solution portfolio and is core to many ongoing leadership activities across the industry. The company works with multiple industry associations and peers to strengthen OT security awareness initiatives, participates in threat intelligence sharing and reporting on key vulnerabilities known throughout the sector, and is active at industry trade shows and conventions.

Source: Frost & Sullivan

Company to Action: Nozomi

Frost Perspective

- While Nozomi Networks remains a recognized name in the OT cybersecurity industry, its OT intelligence capabilities are a newer focus area for the company, at least from a public perspective. With threat intelligence powering many of the security decisions now being made in an organization, ensuring that Nozomi remains a vendor known for bringing the latest intelligence into its OT platforms will be important in helping customers see the long-term viability of Vantage or the Central Management Console solutions.
- Many of Nozomi Networks' partnership and thought leadership activities are done with other OT cybersecurity vendors, despite having partnerships with vendors across the OT infrastructure ecosystem. Strengthening those partnerships can also help the company as the partners expand in infrastructure sectors or geographies where Nozomi does not have a strong brand presence.

Source: Frost & Sullivan

FROST & SULLIVAN

Key Takeaways

Key Takeaways

1

For OT cybersecurity customers, it is no longer just about getting visibility and a handle on their organizational networks and digital sprawl; they need to be able to take some kind of mitigating action when threats to their networks are detected. As such, OT cybersecurity solutions must grant visibility over their operational architecture and allow operators to take proactive remediation measures when the first sign of threat is found.

2

The OT cybersecurity industry has always had a complex mix of vendors that did some aspects of operational security but were all part of the same large, competitive landscape. Recently, the competitive landscape has started to separate into distinct vendor groups that allow for a better comparison between companies, making it easier for new customers to grasp which vendors offer OT security services versus OT visibility and remediation or OT risk assessments.

Source: Frost & Sullivan

Key Takeaways

3

With the OT threat landscape changing constantly and threats targeting OT becoming ever more sophisticated, threat detection and threat intelligence solutions that can be shared across vendors and customers will be essential toward building out a more defensive posture among critical infrastructure organizations. Rather than trending technical functionality, collaboration, open integration, and real-time threat intelligence are far more valuable to OT customers right now than the latest nice-to-have features.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

VERTICAL AXIS

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GROWTH INDEX ELEMENTS

- **GI1: MARKET SHARE (PREVIOUS 3 YEARS)**
  This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.
- **GI2: REVENUE GROWTH (PREVIOUS 3 YEARS)**
  This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.
- **GI3: GROWTH PIPELINE**
  This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.
- **GI4: VISION AND STRATEGY**
  This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?
- **GI5: SALES AND MARKETING**
- This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

HORIZONTAL AXIS

Innovation Index (II) is a measure of a company's ability to develop products/services/solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets, and are aligned to customers' changing needs.

INNOVATION INDEX ELEMENTS

- **II1: INNOVATION SCALABILITY**
  This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.
- **II2: RESEARCH AND DEVELOPMENT**
  This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.
- **II3: PRODUCT PORTFOLIO**
  This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.
- **II4: MEGA TRENDS LEVERAGE**
  This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.
- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com