Brought to you by Informa Tech
OMDIA

Publication date:
24 Jan 2023
Author:
Hollie Hennessy, Senior Analyst, IoT Cybersecurity

On the Radar: Nozomi Networks launches endpoint sensor for OT and IoT networks

Summary

Catalyst

Nozomi Networks has launched its latest product, "Arc," which is a lightweight executable that runs on operational technology (OT) and Internet of Things (IoT) endpoints to monitor and detect threats within the network and across critical assets.

Omdia view

Attacks on critical national infrastructure (CNI) are not new, but they have been picking up traction for 10 years or so (with Stuxnet, a malware targeting OT, being a major event in 2010). However, the geopolitical situation following Russia's invasion of Ukraine in 2022 has resulted in much more awareness and focus on the threats to CNI.

Most recently, the UK's postal service was taken down by ransomware on January 11, the attack being attributed to the LockBit hacking group. While this was not a direct attack on OT, it still highlights threat actors quite clearly targeting CNI.

Thus, within the realm of connected devices, protecting OT and Industrial IoT (IIoT) is top priority. Within the IoT cybersecurity market, solutions aimed at commercial and industrial electronics (which include OT and IIoT) make up more than 30% of the market.

Compared to many other industrial cybersecurity companies, Nozomi Networks enjoys almost veteran status, having been founded in 2013. The vendor has been focused on OT since its inception, enhancing its product portfolio with Vantage (see **Further reading**) and now Arc, and is well placed as the market continues to grow.

Why put Nozomi Networks on your radar?

As mentioned, Nozomi Networks was founded in 2013 and has established itself as a strong player in the OT and IoT cybersecurity market. Nozomi Networks' product portfolio is tailored very well to OT environments. Its two other products, Guardian and Vantage, work together to span across multiple sites and locations, with OT-tailored playbooks, vulnerability workbooks, and capabilities that are focused on both the OT and IT sides of the business.

This focus on OT and expertise in this area sets it up well for being trusted by industrial organizations to utilize agent-based technology in an area where there may be apprehension. Nozomi Networks has purpose-built Arc for OT networks in particular, allowing it to offer low-impact scanning and endpoint threat assessments without disruption.

Market context

OT security is a niche market, with a mix of players that includes service providers (some of which are industrial automation vendors that often have cybersecurity service offerings), cybersecurity vendors, and dedicated technology startups.

With increasing cyberattacks and the geopolitical landscape mentioned above, organizations operating in CNI and in the industrial and manufacturing space are becoming more than aware of the need to secure their devices – from legacy OT to newer IIoT. However, the difference between information technology (IT) security and OT security lies in priorities. When looking at an industrial environment, availability of the device, maintaining operations, and safety is key. Thus, OT environments have been difficult to protect and require specialized solutions, skills, and approaches.

Due to this, the approach to securing OT has been different to securing IT. It has not been viable to put an agent onto the device itself due to the constraints on an industrial network or the risk of a safety issue or downtime. Therefore, the market has focused on passive network-based methods of monitoring and detection.

However, the market is moving toward active methods, and most of the key players are now offering this functionality, with varying levels of adoption due to customer confidence (see **Appendix** for more information). Nozomi Networks has taken this a step further with the launch of Arc – utilizing hosts from as low as Level 2 in the Purdue model (including engineering and supervisory workstations) to widen and enhance visibility across locations and deeper into more attack surfaces.

Product/service overview

Nozomi Arc is an endpoint executable that is compatible with Windows, Linux, and MacOS, operates within OT and IoT networks, and has automated installation, which simplifies deployment. The product both detects and defends against compromised endpoints, as well as insider attacks.

It works in conjunction with Nozomi Networks' other methods of detection and data collection, which includes remote collectors and smart polling (an add-on that uses active rather than passive methods).

Nozomi Arc adds further vulnerability assessment and traffic analysis capabilities on top of these other methods, as well as:

- More accurate diagnostics for anomalies and threats as they are happening
- Log file monitoring and threat detection using SIGMA rules (similar to other threat detection rules that Nozomi Networks uses, such as STIX, used for network data)
- Insight into user activity and USB drives
- Insight even when the device is not sending or receiving traffic.

The sensor can also be used to discover additional assets within the network; i.e., it is not limited to the host endpoint. It uses scanning to identify devices on the host's immediate network or subnet.

The data from options chosen by the customer (remote collectors, smart polling, and Arc) is aggregated for analysis and either reports to an on-premises Guardian platform, or can be sent to the Vantage cloud.

Nozomi Arc does have the capability to provide continuous visibility, monitoring, and threat detection; however, the vendor has made the product flexible. Customers can determine how frequently the sensor performs collections, but can also install and uninstall the sensor on an ad hoc basis for minimal impact on the host device and environment.

Company information

Background

Established in 2013, Nozomi Networks was co-founded by Andrea Carcano (CPO) and Moreno Carullo (CTO). In addition to achieving a PhD in computer science, Carcano spent some of his early career employed as a senior security engineer by the Italian oil and gas conglomerate Eni. Carullo also achieved a doctorate in computer science with a focus on machine learning (ML), and has been a member of the International Electrotechnical Commission (IEC) technical committee on power system information exchange.

In the years since its creation, Nozomi Networks has raised a significant amount of capital. Initially focused on advanced research and development efforts, the company quickly garnered considerable attention. In 2016, the company saw a Series A investment of $7.5m. That number was doubled in January 2018 with a Series B investment of $15m, and a Series C investment raised $30m in September of the same year. This was followed up with a large investment of $100m in July 2021, bringing the total raised to date to $152.5m. Recent investors include Triangle Peak Partners, a venture capitalist that focuses on technology and energy transition, as well as Telefónica Innovation Ventures, Porsche Ventures, Honeywell Venture Capital, and Keysight Technologies.

Current position

Nozomi Networks' offering is subscription based. As of 2022, it also offers its threat feed standalone in a format for use on other platforms. Another interesting launch is Nozomi Networks' latest pricing mechanism, OnePass, which is a single subscription to all Nozomi Networks products, both hardware and software. OnePass was launched in November 2022, and will also be available with Arc later in 2023. The pricing works as a credit-based system, where clients can choose both hardware and software in a flexible, customizable way. This opens up more opportunities for Nozomi Networks, since organizations are able to deploy a combination of the vendor's solution across sites, with less upfront cost compared to purchasing hardware in the first year.

Nozomi Networks also offers professional consulting services, as well as instructor-led training, delivered virtually or on-site. Its team helps with streamlining deployment and tailors engagements to specific customer needs, including infrastructure assessments, design assistance and review, configuration, and checking of the product – plus ongoing monitoring by Nozomi Networks or its partners' services.

Future plans

Nozomi Networks has a structured roadmap and monthly releases with updates that focus on covering new threats and tactics for its customers. The updates are flexible and customer focused. Users are contacted by the vendor for this purpose, and new protocol support can be added, as well as product enhancements, fixes, and a beta version of new features for more agile delivery.

Key facts

Table 1: Data sheet: Nozomi Networks

Product/service name	Nozomi Arc	**Product classification**	OT/IoT cybersecurity Endpoint cybersecurity
Version number	V1.0.0	**Release date**	1Q23
Industries covered	Energy, manufacturing, mining, transportation, utilities, building automation, smart cities, healthcare, and critical infrastructure	**Geographies covered**	Global (Americas, EMEA, APJ)
Relevant company sizes	Enterprise	**Licensing options**	Annual/multi-year subscription
URL	www.nozomi.com/products/arc	**Routes to market**	Direct reach and partner channels
Company headquarters	San Francisco, US	**Number of employees**	290

Source: Omdia

Analyst comment

Unlike some other vendors in the industrial cybersecurity space, Nozomi Networks has been focusing on OT security since its inception a decade ago – meaning it is well versed in navigating the requirements of OT cybersecurity as opposed to IT.

Alongside the need to focus on safety and operations in an industrial environment, there is also the issue of being able to see into various sites, plants, and parts of the organization quickly and smoothly. Vendors in the space have therefore developed their product portfolios to be as simple and easy to deploy as possible.

In the current market, there are only a select few vendors with an agent-based approach. These include Verve Industrial (which began as an OT systems integrator known as RKNEAL), Check Point (with its Nano Agent for IoT and OT devices, which forms part of its IoT security portfolio), as well as some activity from CrowdStrike (including partnerships with Rockwell Automation and Claroty, another OT/IoT security vendor).

Nozomi Networks' addition of Arc essentially provides another visibility and threat detection option for its customers, allowing the user to deploy the agent quickly and offer visibility faster than if a manual site install was required.

This in itself is not unprecedented, in that there are other vendors in OT security that promise installation and visibility within the day. However, the fact that Arc is agent based allows not only speedy visibility but also enhanced visibility, above and beyond what can be seen from a network SPAN or TAP, or even active methods such as Nozomi Networks' own smart polling technology. In addition, nested and offline devices can be reached by the solution, which can also identify unauthorized USB drives – thus adding multiple additional layers of functionality from just one further product. It also aids scalability, covering devices that would otherwise be difficult to reach with a Guardian sensor.

While Omdia has identified a trend in the market toward a more active approach than the traditional passive one, there is still some apprehension among end users. That said, there is growing recognition of the need for active monitoring and detection, which bodes well for the adoption of products such as Nozomi Arc, particularly for the most critical of networks where accurate, timely insight is key. This added approach provides more flexibility for customers who choose to adopt an endpoint perspective.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

2023 Trends to Watch: IoT Cybersecurity (December 2022)

Market Radar: Security Operations Solutions for Industrial IoT and OT, 2022 (October 2022)

Author

Hollie Hennessy, Senior Analyst, IoT Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com