NOZOMI NETWORKS

PRODUCT OVERVIEW

Arc Endpoint Sensor

Continuous asset visibility and automated cyber threat prevention for OT endpoints, with no disruption to operations.

When preventing cyberthreats, identifying vulnerabilities or analyzing anomalies in your processes, it's critical to have as much detailed network and system information as possible for better diagnostics and repair.

Nozomi Networks gives customers more options to collect more data from more sources within critical infrastructure than other OT and IoT cybersecurity solutions and provides deeper analysis and insight from the collected data.

Nozomi Arc provides enhanced endpoint data collection and asset visibility for mission critical networks and industries. This enhanced visibility improves vulnerability assessment, traffic analysis capabilities and more accurate diagnostics of in-progress attacks and anomalies.

Arc identifies hosts compromised by malware, rogue applications, unauthorized USB drives and suspicious user activity, and is able to detect, quarantine or delete malicious files in real-time, without disrupting OT operations.

Arc forms an ideal complement to Guardian sensors in various form factors to aggregate data for analysis and reports either on-premises or in the Vantage cloud. Its threat prevention capaibilities enhance the response features of the Nozomi Networks platform, supported by integrations with third-party security systems.

Nozomi Arc, as a lightweight endpoint executable running entirely in user space, is the only solution of its kind that eliminates the risk of system instability, while delivering automated threat prevention and continuous visibility into key endpoint attributes.

Benefits

Expands enterprise security posture and asset visibility into OT environments

Reduces incident containment and response time

Balances automated cyber risk mitigation capabilities for OT/ IoT endpoints with uninterrupted operations

The Power of Nozomi Arc with Threat Prevention

Designed for OT and IoT

Arc is a user space lightweight sensor designed for OT and IoT networks. Users can flexibly select the desired depth of visibility, manage the volume of system traffic generated, and limit endpoint resource consumption by Arc to avoid interference with critical host tasks.

Accurate and Contextualized Asset Information

An endpoint sensor identifies significantly more relevant cybersecurity details than can be learned from traffic monitoring and remote polling alone, including visibility into processes and users, local behavioral analysis, physical access control, and malicious file analysis.

Effective Traffic Monitoring, Discovery and Smart Polling

Best security practices include minimizing or eliminating connection or data requests from outside the most secure endpoint zones. Many endpoints sit behind firewalls that block such externally initiated connection requests. Arc initiates all data collection and sends that data upstream from within the network —implementing traffic monitoring, non-disruptive Discovery mechanisms and Smart Polling from the endpoint. Each Arc-enabled endpoint functions as a network sensor that helps build an up-to-date topology of its surroundings.

Adaptable Threat Prevention Powered by Threat Intelligence

Nozomi Arc enables detection, quarantine, and removal of malicious files—whether local or on USB media—directly from within the host.

This capability is driven by STIX and YARA rules, delivered through OT-focused Threat Intelligence from Nozomi Networks Labs and the TI Expansion Pack, powered by Mandiant Threat Intelligence.

Offline Asset Monitoring and Centralized Management

Arc sensors provide visibility into all assets on the network, including those not monitorable through data mirroring, not connected to a network at all (offline), or when the upstream console is not available.

These assets can be periodically synced with connected asset data for more complete network visibility and analysis. Additionally, all health monitoring, management and configuration can be managed in a single console with either Vantage or Guardian.

Embedded ICS Visibility, Security and Multiplatform Support

Arc is delivered in its embedded form (Arc Embedded) for deeper real-time visibility, anomaly, and threat detection all the way down to Level 0 of the ICS environment. It is also available for Windows, Linux, MacOS devices for the broadest endpoint coverage in the industry, supporting 32- and 64-bit architectures for both Intel/AMD and ARM machines.

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com

NN-ARC-DS-8.5x11-005