PRODUCT OVERVIEW

Nozomi Arc Endpoint Sensor

The Nozomi Arc endpoint sensor is the latest innovation that detects and defends against malicious and compromised endpoints and insider attacks.

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

More accurate and timely access to data leads to better diagnostics and faster time to repair. Nozomi Networks gives customers more options to collect more data from more sources within critical infrastructure than other OT and IoT security solutions, and provides deeper analysis and insight from the collected data.

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

Customers can now easily identify compromised hosts with malware, rogue applications, unauthorized USB drives and suspicious user activity.

Nozomi Arc forms an ideal complement with existing Guardian sensors in various form factors, including Remote Collectors and the Smart Polling add-on, to aggregate data for analysis and reports either on-premises or in the Vantage cloud.

Nozomi Arc sensors are an endpoint executable that runs on either Windows, Linux or MacOS hosts in mission critical networks. Collected data can be sent to either Guardian or Vantage. By running directly on the host, Nozomi Arc is the only solution that provides continuous visibility to key endpoint attributes.

Benefits

- Detect malicious or compromised hosts
- Accelerated deployments
- Immediate visibility into assets
- Continuous monitoring
- No externally initiated polling requests
- Offline asset monitoring

The Arc Advantage

- User activity correlation
- Asset Visibility + Threat Detection
- Windows, MacOS and Linux support
- Automated installation for scalability
- Monitoring event logs and USB devices

Benefits of Nozomi Arc

Increasingly accurate and more detailed asset information

An endpoint sensor can identify far more relevant cybersecurity details than can be learned from traffic monitoring and remote polling alone, including monitoring log files, user activity and USB drives.

No externally initiated polling requests

Best security practices include minimizing or eliminating connection or data requests from outside the most secure endpoint zones, such as in a Purdue model. Many endpoints sit behind firewalls that block such externally initiated connection requests. Nozomi Arc allows endpoints to initiate all data collection and send data upstream.

Continuous monitoring

Even when the device is not sending or receiving traffic, Nozomi Arc can provide continuous visibility and monitoring since the sensor resides on the host.

Immediate visibility to asset changes and details

By residing directly on the host, any interesting changes in asset configurations, behavior, or traffic can be immediately identified.

Monitoring offline assets

For the first time, assets that were not connected to a Guardian sensor can now be visible with a Nozomi Arc sensor, which can be periodically synced with connected asset data for more complete network visibility and analysis.

More efficient data collection, reduced impact on system resources

Customers can flexibly select how much depth of visibility they want to collect and how much system traffic is ultimately generated.

More Data, Continuous Monitoring, Deeper Insights and Analysis

Nozomi Arc accelerates time to resiliency and scales to fit any enterprise

Nozomi Arc is designed to easily scale in large multi-site enterprise networks, while minimizing management overhead, impact on host resources and potential security and access concerns.

Automated deployment

Nozomi Arc is deployed as a background executable on the host across hundreds or thousands of devices through an automated installation process. This can include existing Mobile Device Management (MDM) platforms that are used to manage consistency of application deployments on large numbers of mobile devices such as laptops, phones, and tablets.

No host credentials stored in Nozomi platform

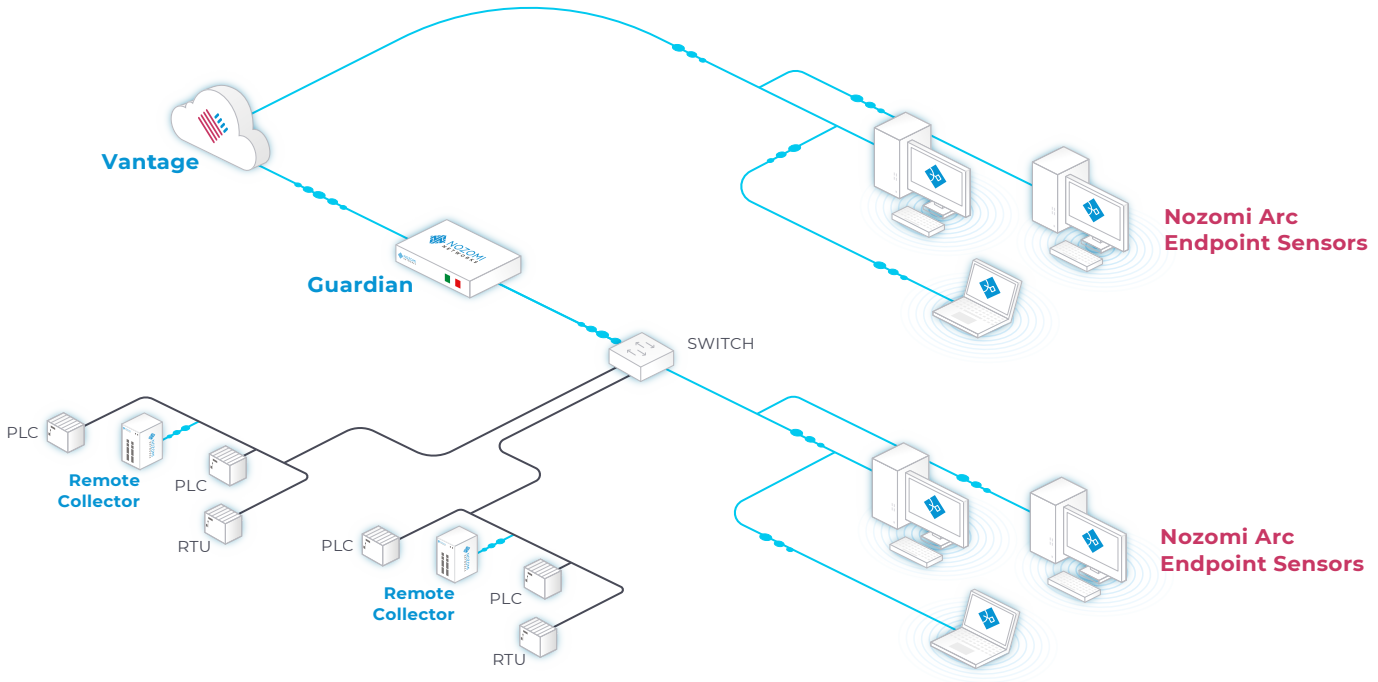
Installing and running the executable and collecting data can leverage existing credential systems. Nozomi Networks does not need to store any host/admin credentials to manage and run Nozomi Arc.

Temporary/ephemeral deployments

The executable does not need to remain on the host after collecting the information and can be automatically uninstalled to conserve host resources and retain a pristine host environment. Policy rules determine how frequently the Nozomi Arc sensor is installed and performs collections.

Multi-platform support

Nozomi Arc supports Windows, Linux and MacOS platforms for the broadest endpoint coverage in the industry.



Sample deployment: Nozomi Arc.

Key Features

Nozomi Arc introduces key features that further enhance system-wide data collection and visibility:

Host-based Smart Polling

The Nozomi Arc sensor can be used to discover additional assets on the network that may not be visible to the local Guardian sensors. Nozomi Arc uses a non-disruptive, low-impact monitoring capability to identify additional devices on its immediate network or subnet.

Log File Analysis with SIGMA Rules

SIGMA rules are similar to the threat detection rules that Nozomi Networks uses, such as STIX, but are applied to endpoint log files rather than network data. SIGMA rules, written in standard and shareable YAML markup language, help identify suspicious activity, cyber threats and anomalies from the log file data. Nozomi Arc uniquely leverages access to log files to provide this greater threat detection capability.

User-specific Activity Monitoring

With more access to endpoint data, Nozomi Arc can now correlate network traffic and anomalies with specific users, where relevant, to identify potential insider threats or accelerate remediation efforts.

Comparison

Only Nozomi Networks Arc has been custom-built to meet the unique requirements of OT environments.

Nozomi Arc Endpoint Sensor	Other Endpoint Agents
✓ Threat detection and deeper asset visibility	✗ Primarily an asset visibility feature
✓ Support for Windows, MacOS, Linux	✗ Windows only
✓ Automated installation	✗ Do not scale beyond a few dozen devices
✓ Additional features (SIGMA rules, Windows Registry monitoring, USB threats, etc.)	✗ No additional features
✓ User activity correlation	✗ No User ID visibility

Use Cases and Deployment Scenarios

Example use cases and deployment scenarios enabled by Nozomi Arc include:

- **Continuous monitoring of employee mobile devices when off the corporate network**
- **Incorporating air-gapped devices into the Nozomi Networks analysis and reporting system**
- **Deeper intelligence or insight on critical endpoint devices**
- **Continuous monitoring of endpoints**
- **Automated sensor deployment across thousands of devices**
- **Low-impact network monitoring solution for air-gapped networks**

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com