NOZOMI NETWORKS

PRODUCT OVERVIEW

Guardian Air

The First Wireless Security Sensor for OT and IoT Environments

With the proliferation of wireless assets in OT environments, OT organizations need a holistic security strategy that includes not only wired and endpoint security, but also wireless security. Unlike Ethernet-connected devices, wireless devices can be accessed remotely, making it easier for attackers to exploit vulnerabilities, exfiltrate sensitive data, gain access to the corporate network, and initiate cyberattacks. Moreover, wireless communications, like Wi-Fi and Bluetooth, are intrinsically vulnerable to unlawful interception, eavesdropping, Man-in-the-Middle attacks and a host of other security risks.

Guardian Air is the first wireless security sensor purpose-built for OT and IoT environments. It monitors all prominent frequencies to provide customers with the much-needed visibility of the wirelessly connected assets. Guardian Air can detect the appearance of rogue infrastructure like cellphone towers, spoofing devices, LORAWAN, building automation protocols, and the presence of drones as well the equipment attached to them.

Data from Guardian Air sensors is sent to our cloud-based management system, Vantage, for analysis alongside network and endpoint data. This consolidated analysis provides a holistic view of your OT and IoT environments.

Guardian Air Benefits

Get **immediate visibility** into wirelessly connected assets

Continuously monitor all wireless frequencies for potential threats

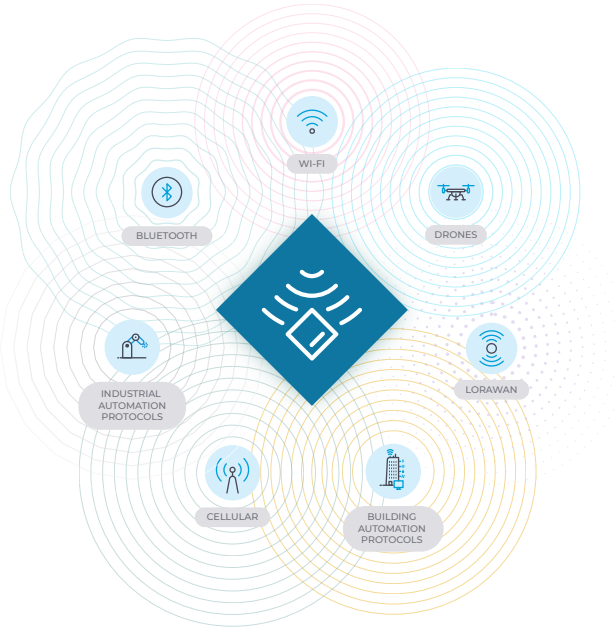
Detect threats and triangulate locations for **faster remediation**

Unified Visibility of All Connected Assets

Continuous Visibility and Monitoring of Wirelessly Connected Assets

While many OT security solutions only see wireless assets once they are connected to the wired network, the Guardian Air sensor continuously monitors all prominent wireless frequencies. This includes Bluetooth, Wi-Fi, building automation protocols, long range technology such as cellular and LoraWAN and drones, to provide immediate visibility of wirelessly connected assets in your OT and IoT environments.

By operating in a wide variety of frequencies, Guardian Air provides real-time monitoring and detailed information of assets such as rogue installations or drones. Drones can be utilized to perform attacks, take pictures of critical facilities or carry equipment for attacks or exfiltration of valuable information. With Guardian Air, operators can detect the presence of drones and the equipment attached to them, enabling security teams to take corrective action.



Ongoing Detection of Wireless-Specific Threats

The nature of a wireless connections means that cyber adversaries don't need to be in close proximity to exploit an asset's vulnerabilities. Guardian Air provides ongoing threat detection of wireless-specific threats, including bruteforce attacks, spoofing, and bluejacking.

For example, Guardian Air can detect de-authentication attacks and triangulate the location of the devices performing the attacks. Alarms can be set to notify security teams enabling them to take immediate countermeasures – bolstering defenses and minimizing impacts to critical operations.

A Complete OT and IoT Network Solution

Today's OT and IoT environments are complex and comprise of network, wireless and endpoint assets. With the addition of the Guardian Air sensor, the Nozomi Networks platform provides a comprehensive network solution for OT and IoT environments. Guardian Air data is seamlessly integrated into Vantage, Nozomi Network's cloud-based management system, along with wired network and endpoint data for unified visibility of connected assets. Security teams have visibility into all attack surfaces, threat detection, and vulnerability assessment in one robust, integrated platform.

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