JOINT SOLUTION BRIEF

Comprehensive Zero Trust IoT/OT Security Platform from Visibility to Policy Enforcement

Combining AI-powered network visibility and analysis with industry-leading security policy enforcement and segmentation for Zero Trust architectures on industrial networks

Challenge

Modern industrial and IoT networks are facing increasing requirements to be connected to the internet, with greater remote access for service, monitoring and data sharing. Smart buildings and smart cities are removing the traditional network security perimeter, opening critical infrastructure to a myriad of emerging threats, attack vectors and malware. Many of the most critical systems are lights-out devices that are not easily patched, updated or protected from zero-day attacks. Often a single system being compromised can quickly spread to other devices and throughout the entire network, well ahead of the chance for remediation or root cause analysis with traditional monitoring tools.

Organizations require more immediate visibility, analysis and detection of threats and anomalies appearing on the network, as well as an automated remediation process or policy enforcement capability that can isolate potential threats, reduce their impact and keep the network and business up and running.

Integration Highlights and Key Benefits

- Industry-leading threat prevention and network visibility for industrial networks
- AI-powered analytics, anomaly detection and event correlation
- Automated remediation against perceived threats through network segmentation and isolation
- Military-grade encryption for secure overlay tunnels and policy enforcement
- Centrally managed policy store simplifies management across existing multi-vendor networks and public cloud providers
- Reduced cost and complexity over alternative security policy enforcement solutions
- Access control policies extended right up to the protected endpoints such as industrial SCADA systems and IoT devices rather than remote access gateways or VPN devices
- Easily defined micro-segmentation policies to implement Zero Trust Network Architectures (ZTNA)

Tempered Airwall

Tempered Airwall offers a dramatically more secure, easier to manage, network infrastructure based on a zero-trust model, or software-defined perimeter. Airwall deploys quickly on existing networks and can ultimately replace a myriad of tedious, error-prone layered network security solutions such as firewalls, VLAN/VRF's, VPN's, and access control products. It provides straightforward network segmentation and secure remote access between any two systems anywhere in the world over a global public network, or within the confines of your on-prem infrastructure. In a world of dissolving network perimeters, more sophisticated network attacks/cyberwarfare, and requirements for more critical IoT/5G infrastructure to be connected and accessible online, Airwall is the only effective and efficient solution that can address today's requirements.

Nozomi Guardian

Nozomi Guardian™ unlocks visibility across OT, IoT, and IT for accelerated security and digital transformation. Its physical or virtual appliances monitor network communications and device behavior, delivering instant awareness of your OT/IoT network and its activity patterns. You see the highest priority vulnerabilities as well as threats and anomalous behavior, enabling you to respond faster, ensuring high reliability and security. Guardian reduces OT risks for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world.

The Joint Solution

The joint offering integrates Nozomi's leading network visibility, threat monitoring, detection and incident response system with Tempered Network's Zero Trust policy enforcement and centralized, software-defined perimeter management console. Today's most sophisticated security threats are driving requirements for not only extreme visibility and intelligent threat detection, but also automated remediation that can lock-down vulnerable systems while ensuring continued availability for authorized access and continuity of business.

The product integration includes the ability of Tempered to mirror secure traffic to Nozomi Guardian systems through a fully encrypted overlay tunnel for greater analysis and insight. With additional Guardian AI-driven insights from the Airwall secured traffic, Nozomi can take remediation steps or refine Tempered security policies through the Airwall Conductor management console API. Nozomi Guardian leverages Tempered's centralized policy Conductor to refine Airwall zero trust policies to uniquely address identified problems, which are not possible using traditional network security approaches like internal firewalls, VLAN's or remote access systems.

> “*A two-way integration of network monitoring of IoT devices and secure, zero-trust, communications is brilliant. Ensuring that all communications is stealthed and encrypted while preserving visibility into traffic is a winning combination.*”
>
> **Richard Stiennon, Industry Analyst and author of Security Yearbook 2020**

> “*Tempered Airwall delivers the military-grade encryption and secure access policy enforcement that many of our joint customers rely upon to quickly remediate anomalies and threats in their networks. The combination of threat visibility and automated enforcement significantly improves security response. Ubiquitous threats like the SolarWinds attack continue to emerge and industrial connectivity for remote work and connected smart devices continue to accelerate. Our combined offerings provide strong detection and defense against the rapid proliferation of advanced persistent threats, actively buttoning down attack surfaces.*”
>
> **Chet Namboodri, Nozomi Networks Senior Vice President of Business Development and Alliances**

Use Case 1

Challenge

How can you monitor and analyze traffic at remote sites including devices like a SCADA environment in a water treatment facility or an oil rig? It hasn't been feasible to deploy threat analysis at each site or remote system and sending traffic to a centralized correlation engine was not secure.

Response

Now, with the integration of Tempered Airwall and Nozomi Guardian, secure Airwall devices already protecting the remote sites can mirror traffic to the Nozomi Guardian system. Multiple sites can connect to the same centralized threat analysis engine through secure encrypted tunnels established by Airwall. There is no security risk introduced by sending remote site traffic to the corporate data center or consolidation point. Organizations can now monitor and analyze traffic from potentially hundreds of remote sites that they couldn't before. And since these operational endpoints are frequently the most vulnerable and visible points of attack, the new threat awareness and traffic visibility can be critical.

Use Case 2

Challenge

A trusted device on the network begins to initiate anomalous network connections or scanning the network for available ports. How should the network respond?

Response

When a system is suspected of having been compromised by malware or otherwise exhibiting anomalous behavior, the Nozomi Guardian analytics will quickly identify the suspect device and issue a quarantine request to the Airwall Conductor, allowing Tempered to segment the infected device into its own isolation segment, preventing the propagation of any malware within the network until the threat can be remediated. The response is both rapid and automated through the Airwall Conductor API.

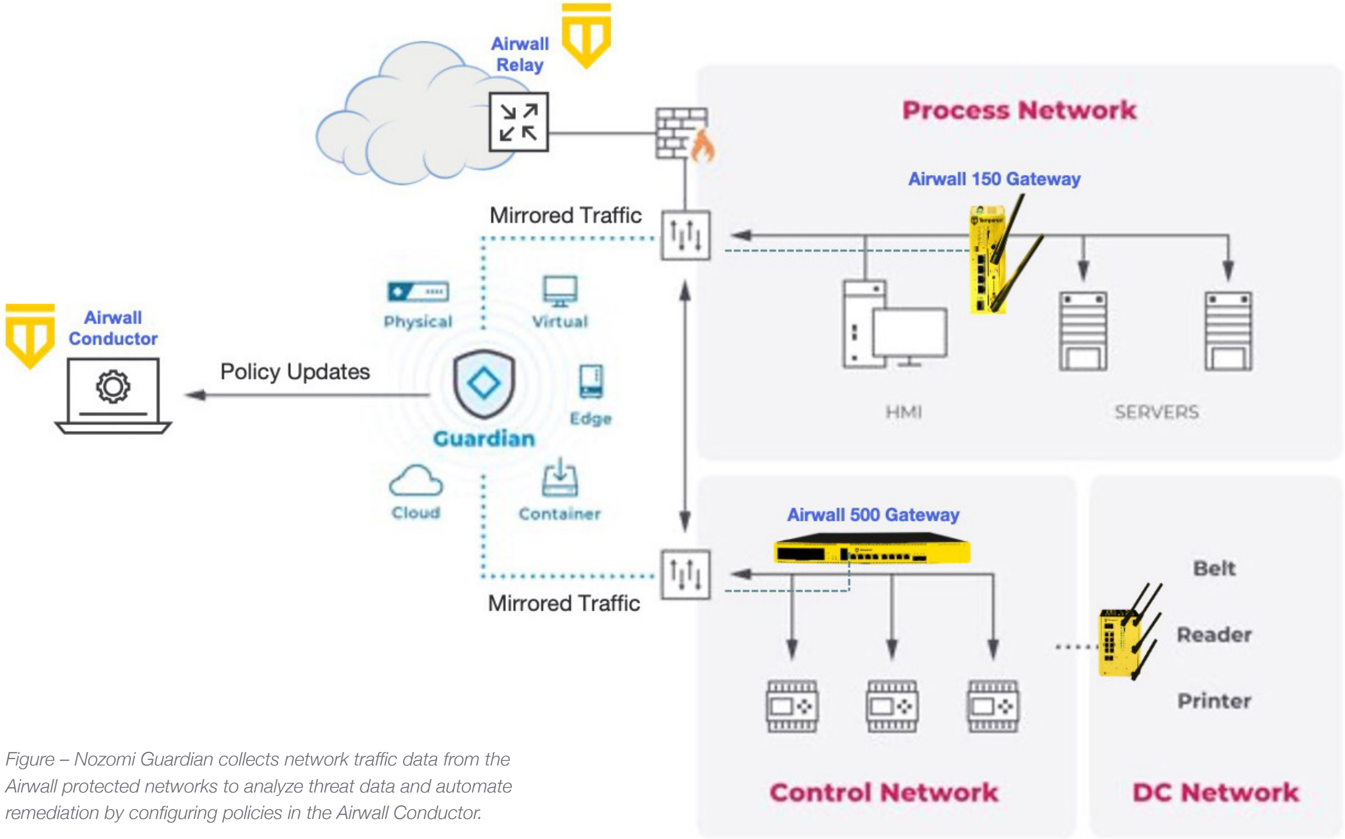

Figure – Nozomi Guardian collects network traffic data from the Airwall protected networks to analyze threat data and automate remediation by configuring policies in the Airwall Conductor.

About Tempered Networks

Tempered makes the industry's only truly native Zero Trust Software-Defined Perimeter (SDP) solution. Airwall is the modern air gap for all connected things. Airwall makes it easy to create and maintain hyper-secure networks across complex infrastructure anywhere, including IT/OT/ICS/SCADA, remote and in the cloud. Airwall networks are multi-factor authenticated, micro-segmented, encrypted end-to-end, and impervious to lateral movement. Ready to make your company's critical assets and infrastructure invisible to threats? Visit https://tempered.io.

About Nozomi 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.
www.nozominetworks.com

Want to see what Airwall can do for you?
Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500