



JOINT SOLUTION BRIEF

***SECURING CONVERGED IT/OT
NETWORKS WITH PROFITAP
AND NOZOMI NETWORKS***

Nozomi Networks and Profitap: A Joint Solution

The digital convergence of IT, IoT, and OT environments demands security solutions that offer real-time visibility, intelligent detection, and resilient monitoring. Profitap and Nozomi Networks deliver a seamless, scalable, and secure joint solution for industrial environments facing ever-growing cyber threats and operational challenges.

Combining Profitap's advanced network observability solutions with Nozomi Networks' world-class OT and IoT security platform enables:

- ⦿ *Lossless, low-latency traffic acquisition, management, and optimization.*
- ⦿ *Real-time asset discovery and behavioral anomaly detection.*
- ⦿ *Scalable monitoring architectures purpose-built for ICS/OT.*

Business drivers

As critical infrastructure and industrial control systems (ICS) evolve to support increased automation and connectivity, organizations face challenges in securing converged IT and OT environments. Legacy protocols, lack of encryption, flat network architectures, and blind spots in traffic visibility leave systems vulnerable to increasingly sophisticated cyberattacks.

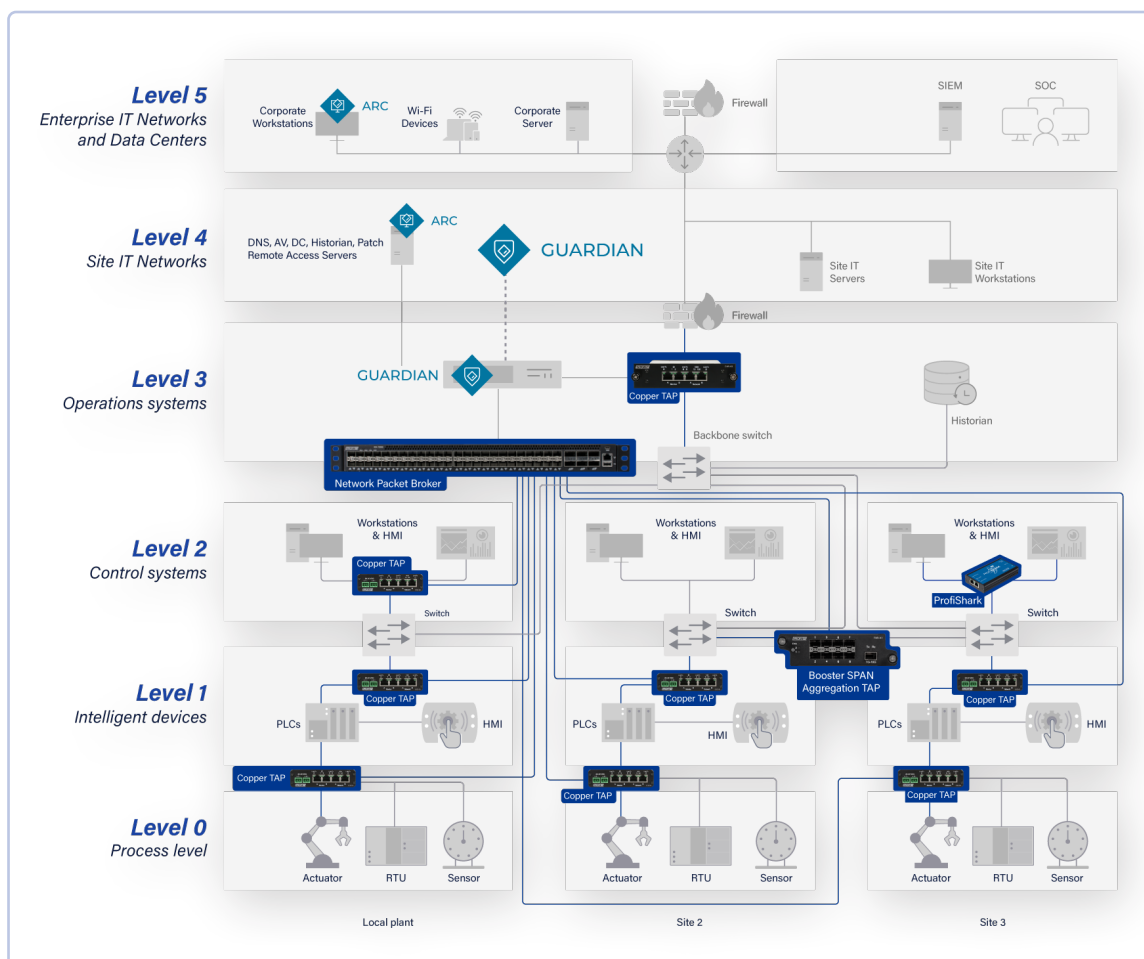
Security teams need:

- ⦿ *High-fidelity access to all traffic, even in hard-to-reach segments*
- ⦿ *Visibility into both IT and OT assets*
- ⦿ *Scalable solutions that adapt to growing data volumes and evolving threat landscapes*



Better together: Profitap and Nozomi Networks

By combining Profitap's TAPs and Network Packet Brokers with Nozomi Networks Guardian and Vantage, customers gain a powerful joint solution that accelerates threat detection, boosts operational resilience, and delivers unparalleled insight across hybrid environments.



Profitap's role in a zero-loss, 100% visibility architecture

Profitap's Observability architecture provides network and security monitoring tools with reliable and secure access to network traffic. The architecture allows for non-intrusive, passive data access without disrupting critical processes. The Network Packet Broker optimization layer provides the relevant traffic to Nozomi and other monitoring tools through intelligent traffic aggregation, filtering, replication, and/or de-duplication. This best-practice approach ensures complete network visibility while making optimal use of resources.

The architecture starts with reliable traffic access through TAPs:

- ⦿ *Remove blind spots and access hard-to-reach areas, with visibility into network segments with varying speeds and feeds, from 10/100M to 1G and up to 400G networks.*
- ⦿ *Data-diode functionality in both fiber and copper TAPs prevents traffic injection back into the network. Additionally, the Secure TAP line has additional tamper-evident measures and meets France's ANSSI CSPN guidelines for use in critical infrastructures, also recognized by the German Federal Office for Information Security (BSI).*
- ⦿ *Industrial TAPs with DIN-rail mount and 24V powering enable local tapping "on the floor".*
- ⦿ *Booster Aggregation TAPs allow for basic aggregation of monitored traffic.*

Network Packet Brokers (NPBs) optimize traffic before distributing to Nozomi Networks by various means, including:

- ⦿ *Aggregating input traffic from various TAPs and SPAN/mirror ports.*
- ⦿ *Optionally replicating monitored traffic to share with multiple tools.*
- ⦿ *Filtering out unwanted monitor traffic to offload unnecessary processing from all monitoring tools. Various and independent filter policies can be applied per monitoring tool.*
- ⦿ *De-duplication to remove multiple copies of the same traffic.*
- ⦿ *Load balancing of the optimized traffic across links to a tool group.*

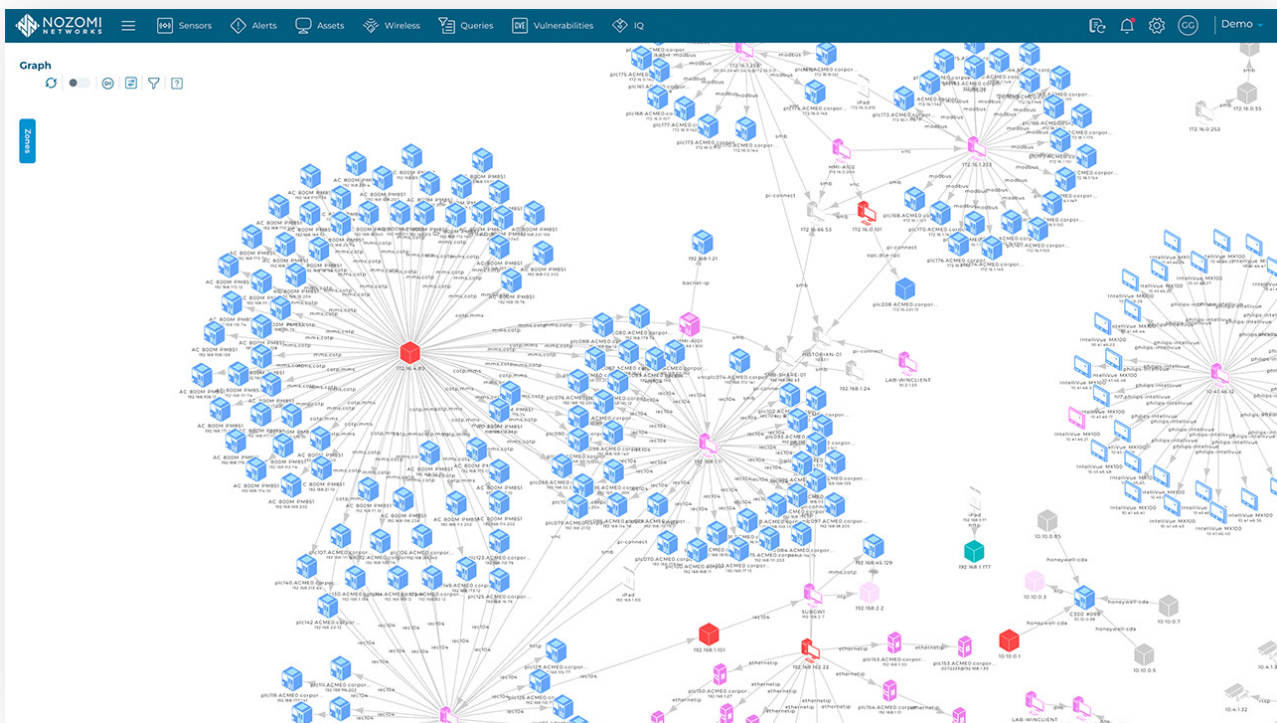
Nozomi Networks' role in the architecture

- ⦿ *Passive Asset Discovery & Behavioral Analysis: Guardian auto-learns OT and IoT environments, profiles behavior, and flags anomalies.*
- ⦿ *Unified Management with Vantage: Vantage provides centralized analytics and threat detection across all local, remote, and cloud sites.*
- ⦿ *Automated Threat Response: Integration with firewall policies and endpoint agents enables rapid containment and remediation.*

Nozomi Networks enables:

- ⦿ *Real-time OT asset visibility and anomaly detection*
- ⦿ *AI-powered threat analytics for ICS and IoT environments*
- ⦿ *Deep protocol awareness across proprietary and standard OT stacks*
- ⦿ *Built-in compliance mapping for NERC CIP, ISO 27001, IEC 62443*

Nozomi Central Management Console is a sensor that manages multiple Guardians in a distributed environment, and provides a consolidated view of all Guardian sensors.



Securing industrial networks with confidence

This partnership is purpose-built for power grids, oil & gas, smart cities, water utilities, and manufacturing plants where uptime and security are equally critical.

The integrated stack enables:

- ⦿ *Continuous monitoring with no network disruption*
- ⦿ *Real-time detection of threats, misconfigurations, and anomalies*
- ⦿ *Operational resilience through enriched security telemetry*
- ⦿ *Scalable deployments across hybrid or segmented networks*



Nozomi Networks is the leader in OT & IoT security for critical infrastructure. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for fast, effective incident response. Customers worldwide rely on us to minimize risk and complexity while maximizing operational resilience.

From day one, our solutions have been deeply rooted in addressing the complex requirements of industrial and critical infrastructure environments. As OT converges with the vastly different worlds of IT and IoT, that experience has given us a unique understanding of the tools and processes associated with the largest networks in the world. We've earned a global reputation for unmatched service, superior cyber and physical system visibility, advanced OT and IoT threat detection, and scalability across distributed environments.

We provide real-time asset visibility, threat detection, and actionable intelligence to keep you in control of your critical infrastructure.



Profitap provides packet-based network intelligence to enhance network monitoring and bolster cybersecurity.

Its unified network observability platform offers reliable data access, traffic optimization, and robust traffic capture and analysis capabilities. These solutions minimize network troubleshooting MTTR, eliminate downtime, support lawful interception, simplify network complexity, and strengthen security for existing and new networks.

Serving over 1,100 clients across more than 70 countries, Profitap's network monitoring solutions deliver comprehensive visibility and analytics across all traffic, ensuring comprehensive insight into physical and virtual infrastructures globally.

To learn more about our joint solution go to <https://www.profitap.com/contact-us/>


FIND OUT MORE ON WWW.PROFITAP.COM

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands

sales@profitap.com
www.profitap.com

 Profitap

 @Profitap

 Profitap-international