OPSCURA

Joint Solution Brief

NOZOMI NETWORKS

Increase Threat Protection with Enriched OT Monitoring Data

Industrial operators and critical infrastructure providers can increase threat protection by combining solutions from Opscura and Nozomi Networks. Opscura expands industrial operator layers of defense from identifying and detecting threats to live protection of assets and data. Opscura connectivity makes it easy and fast to share deep level network data with Nozomi Networks solutions in a controlled fashion, for better threat prevention coverage without operational disruption. Opscura and Nozomi Networks solutions are already working together in critical infrastructure environments.

A Joint Solution

Nozomi Networks provides leading solutions for OT, IT and IOT security and visibility to anticipate, diagnose and respond to cybersecurity threats.

Opscura provides deeper-layer OT network data from Purdue Model Level 2 to enrich Nozomi Networks threat visibility, and provides cloaking, segmentation, and other methods to protect industrial processes from the risk of unauthorized access, operational disruption, data theft, and hacker reconnaissance.

Opscura can also control communications between OT network segments or IT-OT networks, providing only the data the operator deems safe to share to threat monitoring solutions and appliance-based visibility tools such as Nozomi Networks Guardian.

Nozomi Networks and Opscura solutions can be deployed either in sequence, with Opscura first to segment and gather data and Nozomi Networks second to perform monitoring, or simultaneously as a plant security upgrade during regular maintenance cycles.

Joint Solution Benefits

Opscura reduces operational risks by protecting vulnerable legacy industrial assets and data, eliminating deeper-level attack surfaces, and enriching threat monitoring data with deeper visibility. Together with Nozomi Networks, Opscura provides a complete monitoring and protection solution for OT environments.

- Detects threats for the entire OT environment, without requiring taps or network reconfiguration
- Continuously updates with the latest threat information
- Protects OT assets, isolating them from threats
- Enables operators to quickly identify at-risk equipment and safely isolate it

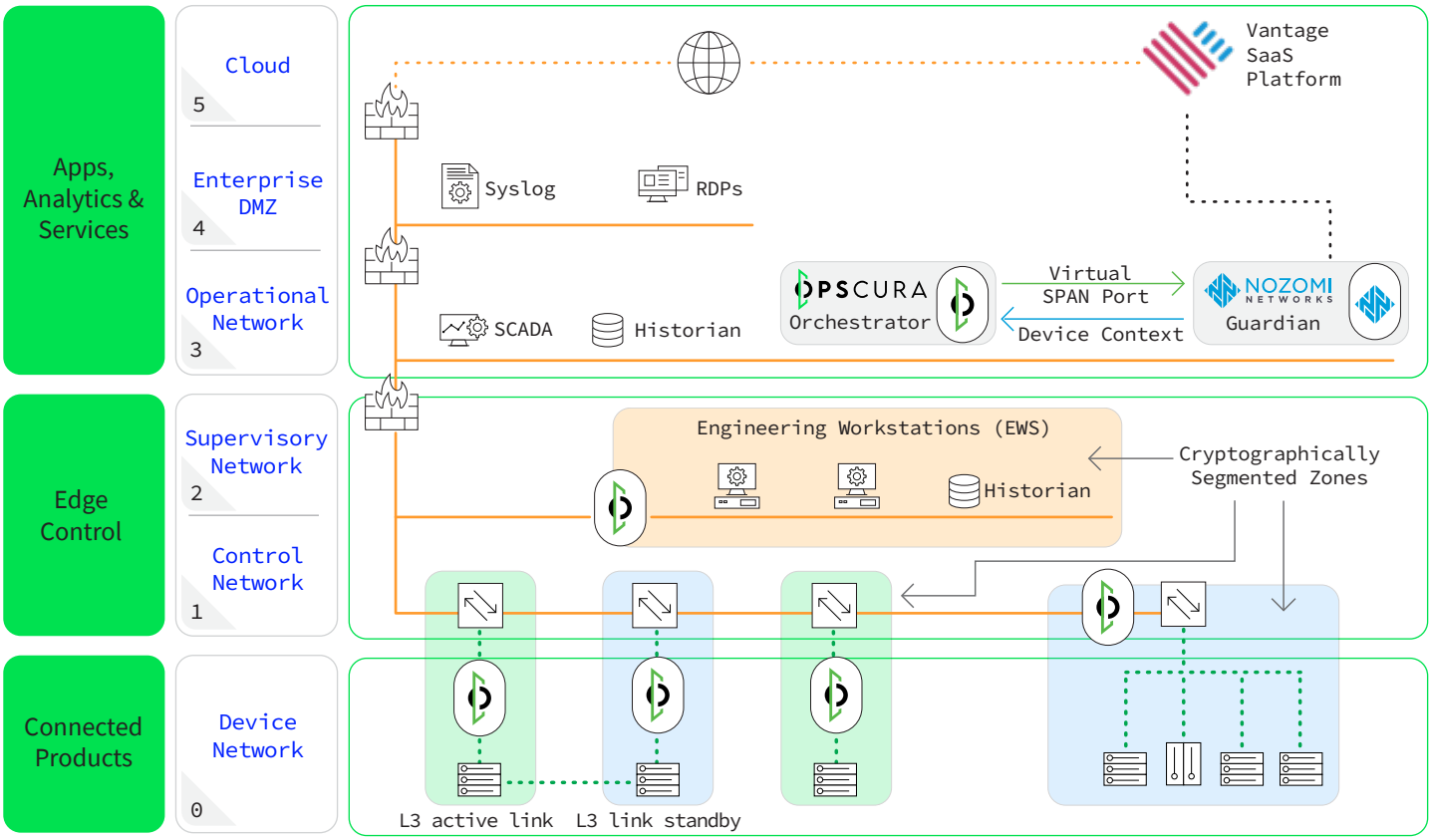
Opscura Solution Benefits

- Easy to deploy in both OT and IT environments
- Deploys transparently without rearchitecting the network, reconfiguring switches or routers, or changing IP addresses
- Cloaks traffic from observation, preventing attacker discovery and reconnaissance
- Shields vulnerable assets from attack
- Allows selective communication between IT and OT assets, while maximizing OT security
- Can be deployed without disrupting time-critical, latency sensitive processes
- Deploys quickly without requiring IT networking experts
- Enables network monitoring and observability tools
- Enforces Zero-trust access to OT assets

Opscura Solution Features

- Available as an industrial appliance with hardware Ethernet bypass or a virtual machine
- Operates at Layer 2
- Transparent encrypted tunnels
- High-speed low-latency encryption
- Integral Layer 2 and Layer 3 filtering
- Temporal ports
- Integral network discovery tools
- Virtual SPAN port

Joint Solution Architecture



The architecture diagram depicts Opscura's solution deployed to protect an industrial control systems network. Three cryptographic segments have been created: orange for engineering workstations, and blue and green for different plant processes. Opscura allows the operator to easily control what traffic is allowed to flow between and within the different cryptographically segmented zones. Should an attacker penetrate the IT/OT (Level 3.5) firewall, the traffic is fully encrypted, cloaking it from observation. Traffic from outside the zones is rejected, preventing access to sensitive equipment and protecting OT assets.

As operators monitor their OT network for threats and vulnerabilities, Opscura mirrors all traffic observed on different zones to Nozomi's Networks Guardian solution. Clear-text traffic from the zones is compressed, encrypted, and transmitted to the Opscura Orchestrator, which replays it out a dedicated SPAN port to Nozomi's Networks solution. Connecting Opscura to Guardian provides the Nozomi Networks solution the data it needs to be effective – data that is often unavailable because of the limitations of network equipment common in industrial environments.

Assets identified by Nozomi Networks as vulnerable can be placed in dedicated zones or protected with additional filtering. Assets identified by Nozomi Networks as malicious can be prevented from accessing protected assets. Nozomi Networks and Opscura solutions together enable operators to know what is occurring on their network and to take action safely and rapidly.

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.

Contact us

For more details,
nozominetworks.com/contact

About Opscura

Opscura protects and connects industrial networks with easy-to-use innovations that are safe to use deep within operational infrastructure. Validated by global partners such as Schneider Electric, Opscura reduces operational risks by protecting vulnerable legacy industrial assets and data, eliminating deep-level attacker footholds, and enriching threat visibility data. Brownfield and greenfield global customers rely on Opscura for OT cloaking, isolation, and Zero Trust authentication, together with simplified IT-OT connectivity.

Learn more about Opscura's Spanish Basque region roots and follow us through www.opscura.io

Contact us

For more details,
reach us at
contact@opscura.io