OPSWAT.

DATASHEET

Neuralyzer™

Rethink OT Cybersecurity

Visibility into OT environments continues to be a major challenge and risk vector for organizations. OT environments are inherently heterogeneous and quite often consist of decades-old devices from multiple vendors. The ability to have full visibility into assets and what is happening on the network is key to any effective OT cybersecurity program.

What We Offer

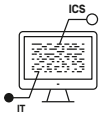
Neuralyzer addresses risks to OT systems from both traditional IT and specific ICS threats. It is extremely simple to deploy and easy to use with OT-native UIs. Neuralyzer can be operated without an expert skillset or training.

It provides unparalleled visibility into converged IT/OT operations and delivers deep situational awareness of threats throughout the network.

It helps to protect your critical assets by maximizing your visibility, security, and control across your entire operations while staying compliant with regulatory requirements.

Neuralyzer leverages AI technologies to gain knowledge of the unique attributes and requirements of OT environments.

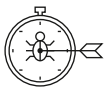
Benefits



Addresses both IT and specific ICS threats to OT systems

Easy to use and built for OT personnel

Offers full visibility and management info into ICS Assets



Timely and accurately informs you of any threats or anomalies on the network

Supports regulatory requirements with wide and objective risk assessments

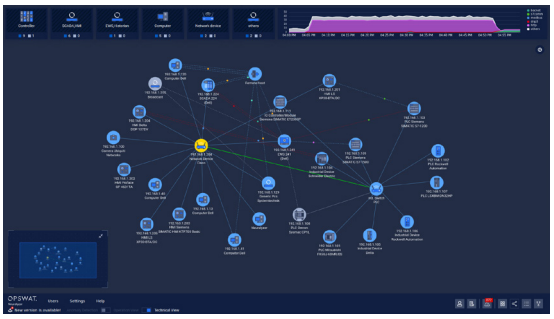
Provides a unified view of operation, security, and compliance in a single pane of glass

OPSWAT.

Neuralyzer

USE CASES

- Asset Inventory & Vulnerability Assessment
- Network Visualization & Monitoring
- Threat Detection & Response
- Exposure Assessment & Alert workflow



REALTIME, AI-BASED ANALYTICS ENGINE

- Behavioral Anomaly Detection
- Asset's Changes Detection
- Unusual Communication Detection
- Violation of Security Policies Detection

DEEP NETWORK ANALYSIS & DEVICE FINGERPRINTING

- Deep Network Traffic Dissection
- Knowledge of OT Devices & Protocols
- Proprietary ICS Fingerprinting & Vulnerability

PART NUMBERS

Neuralyzer All-In-One Network Appliance	NEU-AIO-STD

SPECIFICATIONS

Networking	▪ 1 x Onboard RJ-45 Gigabit Ethernet Network Adapter ▪ 1 x Intel Wi-Fi 6E (6GHz) AX211 2x2 Bluetooth 5.2 Wireless Card ▪ 2 x Add-On USB 3.0 to RJ-45 Gigabit Ethernet Network Adaptor
Voltage	90 – 264 VAC, auto-ranging 47 Hz – 63 Hz
Power Consumption	220W (maximum)
Weight	15.06 lbs. (maximum)
Dimensions	13.54 in. (344.00mm) x 21.26 in. (540.20mm) x 2.07 in. (52.50)

Capabilities

- Rapidly Discover Devices and Build Asset Inventory
- Immediately Explore Connectivity and Visualize Network
- Continuously Monitor Network to detect Threats and Anomalies
- Constantly & Objectively Address OT Vulnerabilities and Risks
- Structured & Streamlined Risk Alert Workflow
- Global, regional & Industry Regulatory Compliance Reporting
- Comprehensive & Customizable Dashboard
- Simple Deployment, OT-Friendly and Easy to Use

OPSWAT.

Protecting the World's Critical Infrastructure