OPSWAT.

NEURALYZER™

A Neural Network Cybersecurity Tool for OT Personnel to Protect OT Networks

SOLUTION BRIEF

OCTOBER 2022

CONTENTS

THE OT ENVIRONMENT

Operational Technology (OT) is the combination of hardware and software that monitors and controls industrial processes. Industrial and critical infrastructure organizations use OT and ICS to safely produce and ensure delivery of goods and services which are essential to the daily life of billions of people around the world.

OT CYBERSECURITY CHALLENGES

Shortage of A Skillful Workforce and Effective Security Solutions
We face a significant shortage of cybersecurity workforce as well as effective cybersecurity solutions for OT businesses. Many cybersecurity products were built primarily for IT professionals and are too complex or costly to implement and maintain in an OT environment. This combined shortage makes cybersecurity programs in an OT organization even more challenged.

Increasing Threats from IT/OT Convergence
While IT/OT convergence brings many benefits to OT business, it also increases the risks as OT environments are now exposed to cyberthreats of the IT world. Recent attack campaigns like BlackEnergy, Triton, Colonial Pipeline, and JBS Foods, show that conventional defenses are no longer sufficient to protect OT networks from today's sophisticated attacks.

Lack of Visibility into Assets and Network Activity
You can't protect what you don't see. OT environments are inherently heterogeneous and quite often consists of decades-old devices from a variety of vendors. The ability to have full visibility into the assets and a thorough understanding of what is happening on the network is the key to any effective OT cybersecurity programs.

Complex Regulatory Compliance Requirements
Adhering to OT security compliance requirements is often a manual and inefficient process. Critical infrastructure organizations heavily invest in people, process, and technology to comply with regulatory programs required to meet audit and compliance requirements across global, regional, and industry standards.

Facts & Figures

Cybersecurity labor crunch to hit 3.5 million unfilled jobs

The 2020 WEF's Global Risks Report listed cyberattacks on critical infrastructure as a top concern

The number of industrial control systems connected to the Internet is 100,000+ and continues to grow

Ensuring the reliability and availability of control systems is the number #1 concern for OT/ ICS security for organizations

One of the top 5 concerns for OT/ ICS security businesses is meeting regulatory compliance

NEURALYZER: A NEW APPROACH

Neuralyzer Employs a New Approach to Address the Challenges in OT Cybersecurity

Neuralyzer address risks to OT systems from both traditional IT and specific ICS threats. It provides unparalleled visibility into converged IT/OT operations and delivers deep situational awareness of cyberthreats throughout the network. It helps maximize your visibility, security, and control across your entire operations, protecting critical assets effectively, and stay compliant with regulatory requirements.

Neuralyzer's benefits are from its advanced AI technologies, knowledge of the unique attributes and requirements of OT environments, and deep understanding of OT usage preferences.

Neuralyzer is extremely simple to deploy, easy to use with an OT-native UI, and can be operated without expert skillset or training.

A Powerful Tool to Protect OT Networks

- Purpose-built OT and IT View Mode help OT Personnel and Security professionals address cybersecurity issues with different views and preferences.
- Full visibility into ICS assets and networks; employing smart and advanced discovery techniques for complete assets inventory without impact on OT networks and devices.
- Visualize network topology and connectivity to provide a complete view of what is going on the network in real time.
- Predefined policies incorporate requirements in regulatory standards.
- AI algorithms for auto defining comprehensive security policies and proactively identifying of a variety of vulnerabilities and threats.
- Continuous and real-time monitoring of asset and network connectivity, immediate alert on any violation of security policies or anomalies.

BENEFITS

- Built as an easy-to-use, simple-to-deploy solution to maximize OT personnel's usage and performance
- Address both IT and specific ICS threats to OT systems
- Gain full visibility and management info into ICS Assets
- Timely and accurately informed of any threats or anomalies on the network
- Support regulatory requirements with wide and objective risk assessments
- Unified view of Operation, Security and Compliance, in a single pane of glass

NEURALYZER
PLATFORM ARCHITECTURE

OT- IT View mode

Plug & Play Visibility and Protection

OT Friendly
Simple to Deploy
Easy to Use & Maintain

Capabilities and Use Cases

Asset Inventory and Vulnerability Assessment
Network Visualization and Monitoring
Threat Detection and Response
Exposure Assessment and Alert Workflow
Dashboard & Reporting

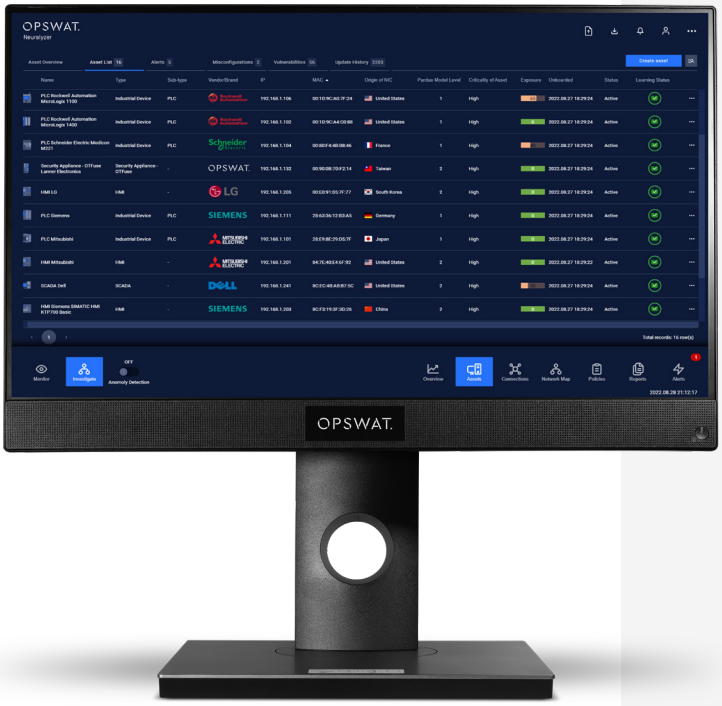
Realtime, AI-Based Analytics Engine

Behavioral Anomaly Detection
Asset Changes Detection
Unusual Communication Detection
Violation of Security Policies Detection

Deep Network Analysis and Device Fingerprinting

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

NEURALYZER: EFFECTIVE, SMART, & SIMPLE



Rapidly Discover Devices and Build Asset Inventory

As soon as Neuralyzer is deployed, it starts looking for the devices on your network. Using the combined non-intrusive passive monitoring and selective smart probing specific to each vendor and device type, Neuralyzer can safely uncover devices on your network. The result is a full, detailed, and ready-to-use asset inventory list.

Asset Inventory & Details

Provides an overview of all assets on your network and features customizable filtering to quickly see what you need.

Insights about device's properties, connectivity, security posture (vulnerability, open port/ service), update history, and alerts. These details are necessary for Asset Management and help provide useful data for meeting regulatory requirements.

Any device on the network becomes fully visible on Neuralyzer

The interactive network map provides a clear view of connectivity between devices

Immediately Explore Connectivity and Visualize Network Map

Neuralyzer captures and analyzes the network traffic, displays connectivity, renders the topology, and visualizes a real-time, interactive network map. All communication (protocol, port, time, and data length), whether between devices on the network or between an internal device and a remote host, is clearly shown in great detail.

Realtime Purdue model network map helps immediately spot abnormal/ unauthorized connection

Customizable Filter and Navigation

The customizable layout allows for both a macro view of the overall network as well as a detailed look into any single connection.

Different Views to facilitate different focuses

"Cluster" view focuses on connections around a device

"Purdue model" view provides insight on connectivity through network levels

Alerts like this supply-chain violation will display with clear action options

CONTINUOUSLY MONITOR NETWORKS TO DETECT THREATS AND ANOMALIES

Neuralyzer continuously monitors ICS network and triggers alerts on detection of potential threats, vulnerabilities, supply chain violations or non-compliant issues of device and network connectivity. Security policies are either inherited from predefined configurations, self-learning, or manually created, altogether creating a comprehensive detection mechanism for potential threats or operational mistakes.

Neuralyzer helps security professionals and control engineers stay ahead of cyberattacks through prompt, concise, and contextual alert notifications when any security policy violation or network anomaly is detected.

Device's CVEs are detected by Neuralyzer

CONSTANTLY AND OBJECTIVELY ADDRESS OT VULNERABILITIES AND RISKS

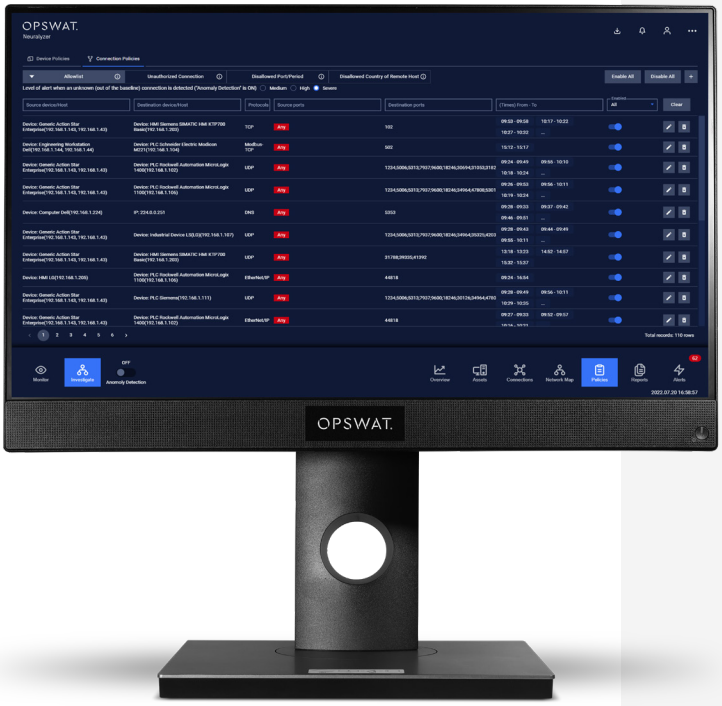
Neuralyzer leverages our team's extensive research in industrial cybersecurity and specific vendor device specifications for finding supply chain risk and vulnerabilities (unpatched CVEs) associated with ICS assets. Neuralyzer also routinely discovers possible misconfigurations such as when a port or service is open but not in use, and improper network segmentation through network connectivity.

Vulnerabilities, supply-chain violations, misconfiguration, threats, or anomalies are employed in Neuralyzer through a proprietary smart algorithm to create a comprehensive Exposure Score. This score is used to measure the exposure (risk) aspect of each asset accurately & objectively on the network.

The exposure score, along with the asset's classified criticality, enables authorized personnel to quickly identify the highest risk for priority remediation before attackers exploit vulnerabilities and cause disruption to operations or even worse damage to the ICS system.

Any change to the asset, either automatically updated by Neuralyzer or manually edited by user/ operator, is recorded with all details. This will help with the audit or regulatory requirements.

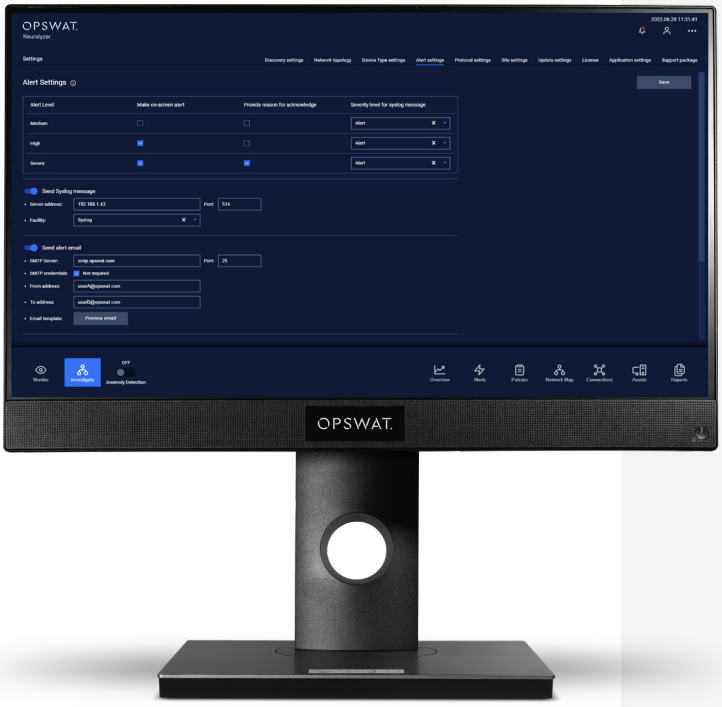
STRUCTURED AND STREAMLINED RISK ALERT WORKFLOW



Security policy settings

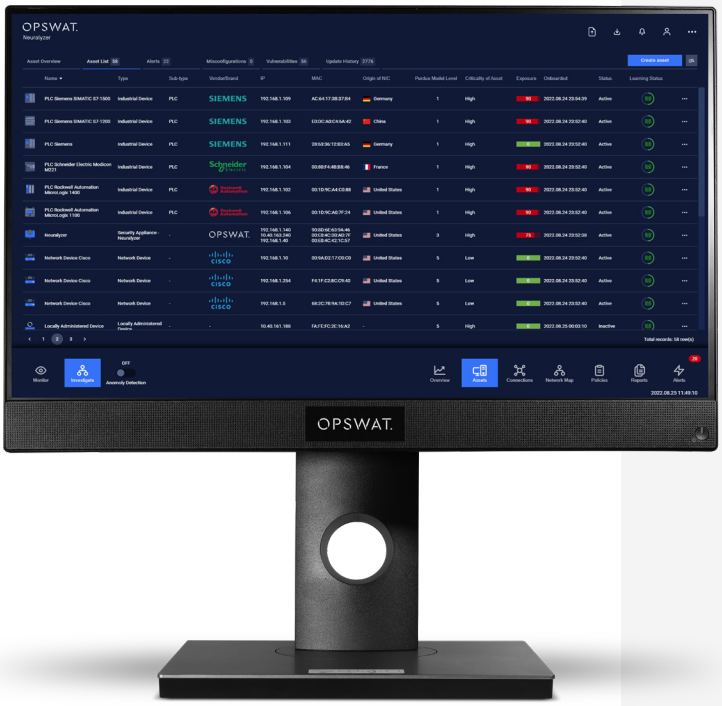
Accurate and timely notifications on cybersecurity incidents or threats are crucial to any OT cybersecurity solution. Equally important are the processes to monitor, collect, classify, and route alerts, for dual (and usually contradictory) purposes. This ensures personnel will not miss a critical incident or report a trivial event.

Neuralyzer enables users to hook alert generations to various data types, including the definition of device types, protocol, device, connectivity, etc. Predefined policies or allowlists (which Neuralyzer automatically learns) are among the places where alert/ risk is defined.



Notification preferences and routing settings for Alerts

Neuralyzer provides flexibility for all users to monitor and control their organization's cybersecurity. Notifications can be tailored to the appropriate channels so all alerts of all levels can be shown on screen, through syslog, or via emails.



Incidents, Alerts and Resolution Status

Global, Regional and Industry Regulatory Compliance Reporting

Neuralyzer supports global, regional, and industry regulatory requirements for OT cybersecurity such as NERC CIP, NIST, NIS Directive, NEI 8-09, ISA/IEC 62443. These compliance and reporting standards help organizations assess and improve their cybersecurity status to meet regulatory requirements.

Customizable dashboards provide overall and quick view of what matters most with regards to OT security

Comprehensive and Customizable Dashboard

Neuralyzer provides real-time, customizable dashboards so users can have many choices of views and levels of detail into the OT network—from overall structure or high-level security status of the whole system to dive deep into properties or behaviors of an asset or network connection.

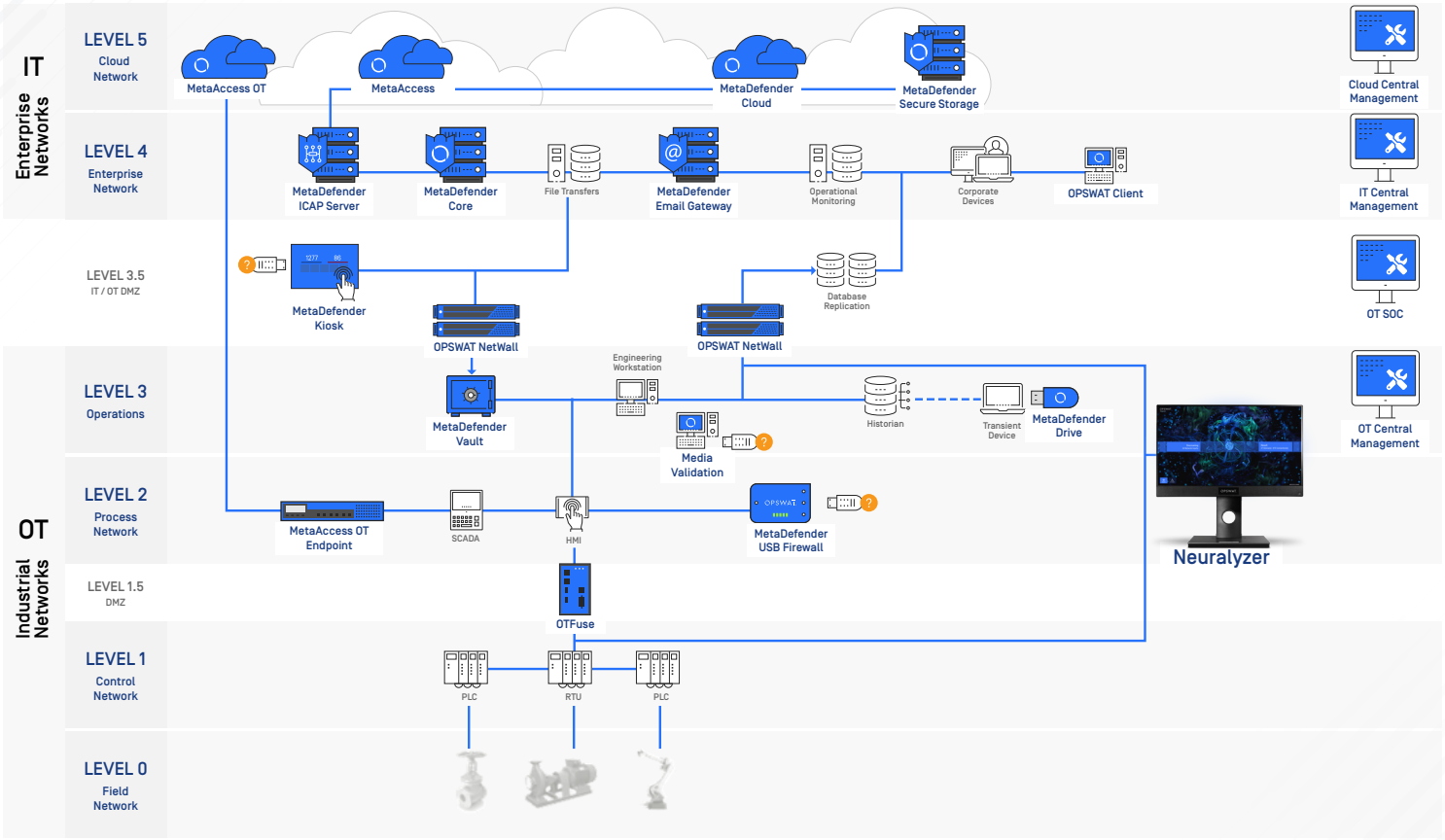
SIMPLE DEPLOYMENT, OT-FRIENDLY AND EASY TO USE

Neuralyzer is built with simplicity and OT-friendliness in mind. The unique dual OT-IT View Mode feature enables the users, either Control Engineers, ICS Operators, or Security Specialists to comfortably work with the system in the most convenient and effective way.

Neuralyzer is super easy to deploy. All the necessary hardware and software is packaged in a ready-to-use appliance. It takes just five minutes to set up Neuralyzer and gain immediate visibility into your OT environment.

DEPLOYMENT

Neuralyzer can be deployed at the Purdue model level 3 or level 2 of the network. The best deployment scenario is to connect one of its ethernet interfaces to the span (mirror) port of the switch for passive monitoring and connect the other ethernet interface to a normal port for selective smart active probing.



SPECIFICATIONS

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 Adapter
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)

SUPPORTED PROTOCOLS

Our current supported protocols are located below and new protocols are continually added. Connect with OPSWAT for the latest list.

Standard OT Protocols
BACNet
CIP
DNP3
EtherCAT
EtherNet/IP
Genisys
HART IP
IEC 60870-5-104
Modbus TCP
MQTT
OPC UA
Profinet IO

Proprietary OT Protocol
BSAP IP
S7
S7 Plus

IT Protocol
ARP
DHCP
DNS
FTP
HTTP
ICMP/PING
IMAP
IRC
Kerberos
LLDP
MySQL
NTLM
NTP
POP3
Radius
RDP
RFB
SIP
SMB
SMTP
SNMP
SOCKS
SSH
TDS
XMPP

OPSWAT.

Protecting the World's Critical Infrastructure