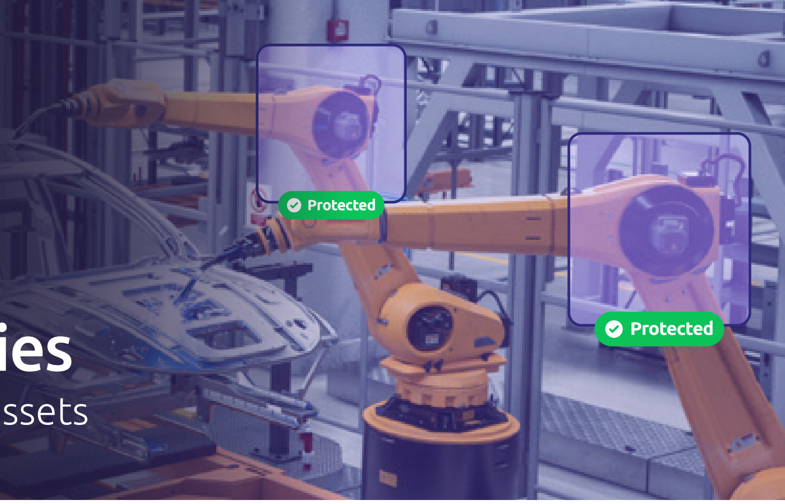
txOne networks | Keep the Operation Running



Shield Unpatched OT/ICS Devices from Vulnerabilities

Virtual patching for plant manufacturing assets

Challenge

Unpatched Machines Running on Production Lines

Legacy and unpatched plant OT assets are the most vulnerable to malware, creating an easy target for adversaries and operational disruption. End of service announcements are inevitable, which means more devices will become legacy equipment without support from traditional antivirus solutions or OEMs with vulnerability patch updates.

Modern equipment also goes unpatched for many automotive and supply chain manufacturers. Some devices perform mission critical functions where the downtime to install software or firmware updates is not an option. Others need alternative protective measures while new patches are tested and validated before getting deployed on automation assets in the production lines.

Solution

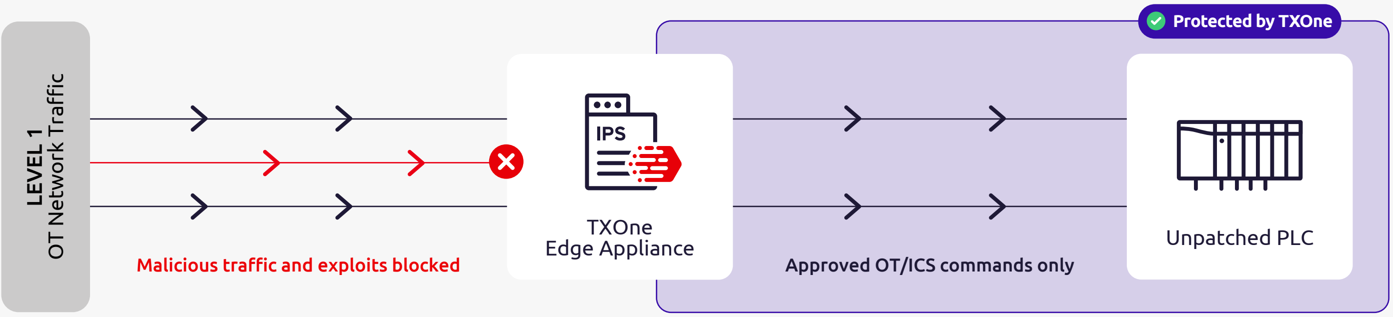
Shield Unpatched Devices with Virtual Patching

Virtual patching is an OT network-based behavior that puts a 'shield' around vulnerable assets without modifying any existing applications or configurations on the asset itself. It offers a critical layer of defense for all plant devices where traditional patching is not feasible due to operational constraints or system compatibility issues.

Unlike many common firewalls or intrusion prevention systems (IPS), TXOne Edge devices sit inline on the OT network (Levels 3-1 of the Purdue Model) to provide virtual patching capabilities that protect PLCs, HMIs, SCADA, and other machines by blocking or intercepting malicious north/south and east/west traffic.

Ruggedized Edge appliances are also designed to comply with production environment requirements. This was especially important for one global automotive component supplier that deployed EdgeIPS devices in front of critical assets, cabinets and switches on the factory floors that are consistently over 104 °F (40 ˚C).

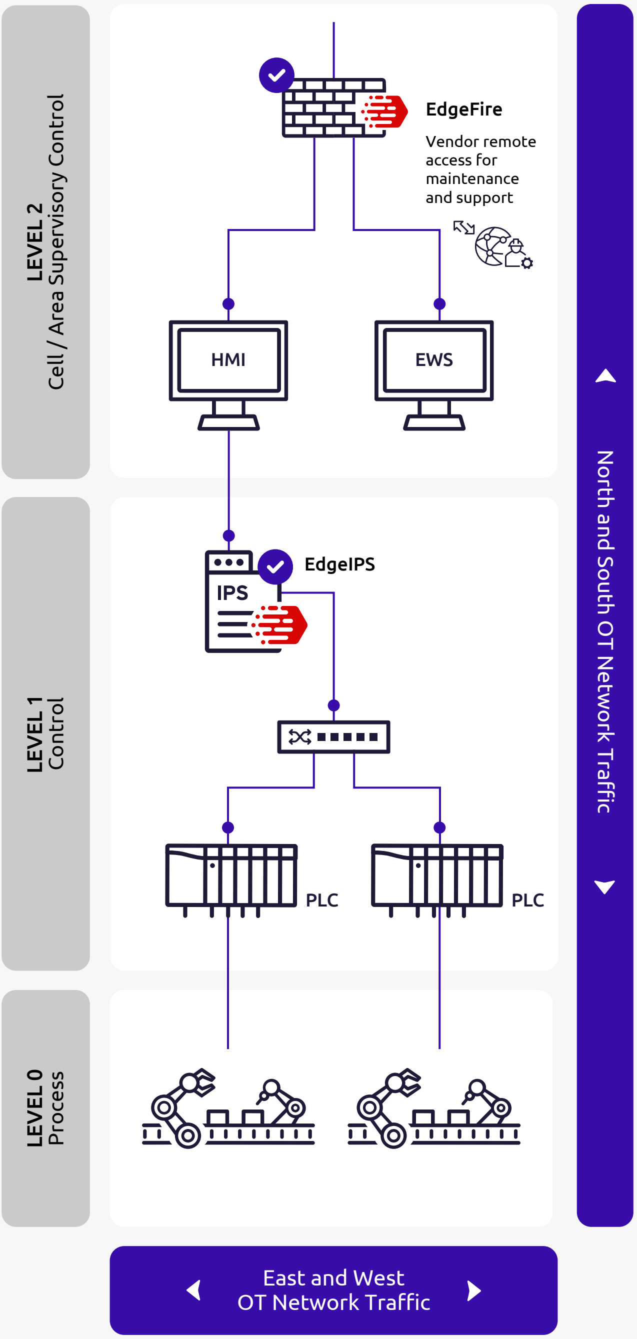
Virtual Patching for OT Assets



This diagram illustrates how the TXOne EdgeIPS appliance creates a virtual shield to protect unpatched OT assets on a production line. The Edge appliance sits deep within the OT network to prevent both known exploits and unknown malicious traffic from reaching the OT device. At the same time, whitelisted OT/ICS commands continue through without disruption to keep the operation running.

Defense-in-Depth OT Network Protection with TXOne Edge Series

OT Network Topography of a Manufacturing Plant


LEVEL 2
Cell / Area Supervisory Control
EdgeFire
Vendor remote access for maintenance and support
HMI
EWS
LEVEL 1
Control
EdgeIPS
IPS
PLC
PLC
LEVEL 0
Process
North and South OT Network Traffic
East and West OT Network Traffic

Result

Protection from known and unknown vulnerabilities without disrupting production

Virtual patching with TXOne's Edge appliances means there is no need to reboot the system or shut down the production line. Unpatched legacy assets are protected, while assets that are still patchable now have a stopgap measure until the machine manufacturer publishes its proprietary security updates that can be deployed during scheduled maintenance.

Large-scale and multisite deployments can be managed from the EdgeOne centralized console to streamline security control processes and minimize administrative efforts.

Most importantly, OT facilities can maximize operational resilience and protect the critical manufacturing process without having to settle for reduced productivity. More automotive OEM and supply chain manufacturers are recognizing the importance of a dedicated, OT-centric security solution that complements the IT security infrastructure. This two-pronged strategy improves collaboration between IT and process control engineers while meeting the unique requirements of production floors to keep plant assets running.

Real Business Impact

Mid-2023, a US-based global automotive supplier experienced a network security incident that halted all manufacturing production for 11-days.

Production downtime resulted in a financial impact of $18 - $20 million and diluted earnings by $0.40 - $0.45 per share.

Source: Upstream Security Global Automotive Cybersecurity Report 2024t

Ready to shield your unpatched OT/ICS assets?
Contact us to get started.

About TXOne Networks

TXOne Networks offers cybersecurity solutions for ICS and OT environments, employing the OT zero trust methodology for Cyber-Physical Systems (CPS). We foster collaborations with leading manufacturers and infrastructure operators to devise effective defense strategies, addrtessing security vulnerabilities in industrial settings.

txOne networks

txone.com