TXOne Overview

Richard Ku

Sr. Vice President Commercial IoT Security Business and Market Development

IT Devices vs OT Devices

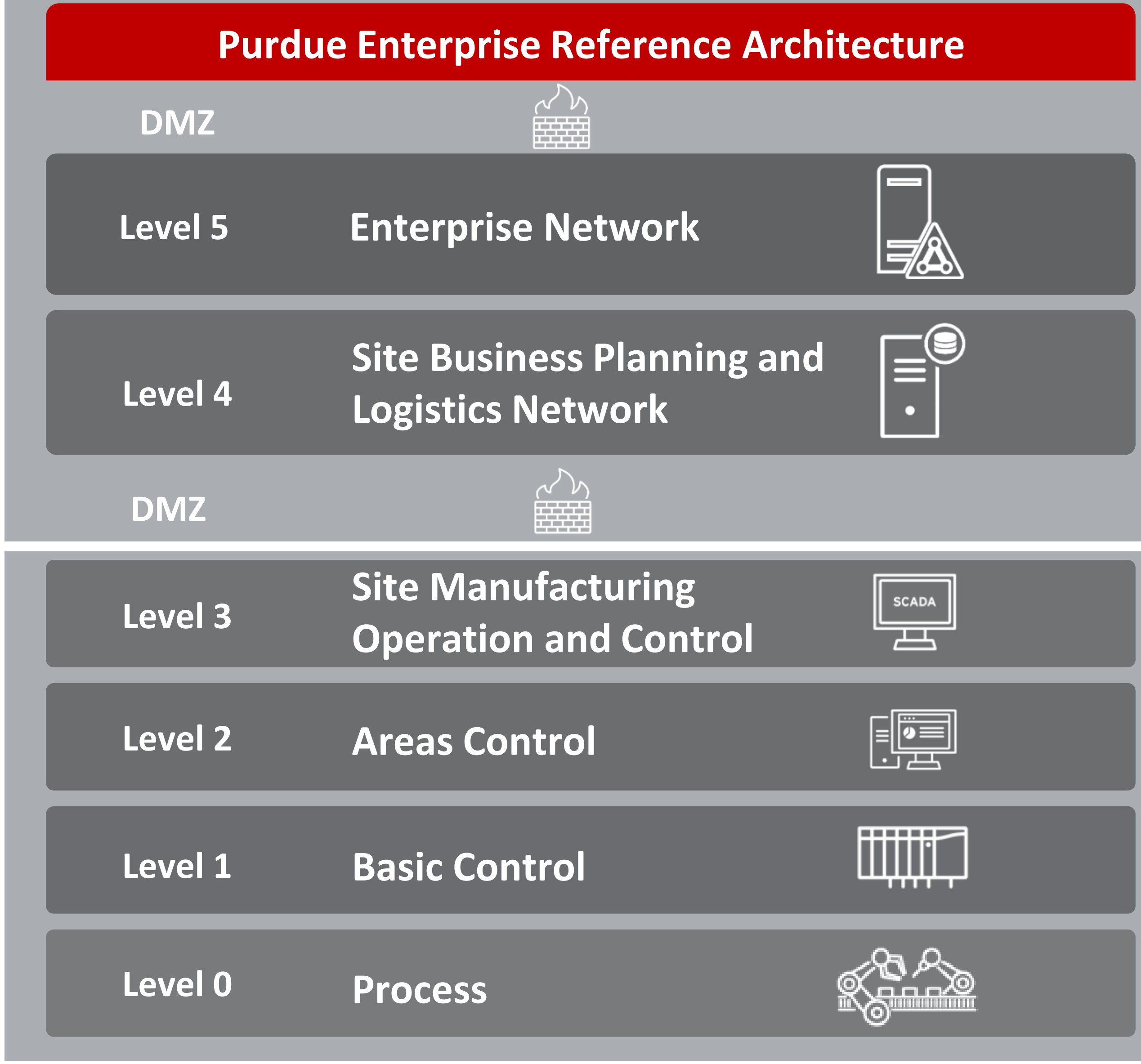
IT Environment

- Multipurpose – MS Office, video conferences, etc.
- Usually have the latest OS available
- Require internet connectivity for task completion
- Higher tolerance to interruption and latency
- Convenient to regularly update and patch
- Confidentiality is first priority

OT Environment

- Mission critical, carrying both productivity and availability
- Low tolerance for interruption and latency
- Often runs legacy and modern OS’s side-by-side
- Air-Gapped / No internet connection
- Updates and patches only available during maintenance
- Availability and Safety is first priority

Solution Position



Purdue Enterprise Reference Architecture

DMZ

Level 5 Enterprise Network

Level 4 Site Business Planning and Logistics Network

DMZ

Level 3 Site Manufacturing Operation and Control

Level 2 Areas Control

Level 1 Basic Control

Level 0 Process

Cooperate IT
Cybersecurity Solution

TREND MICRO™

txOne™ networks

Adaptive Cybersecurity Solution
for OT Shop Floor Environment

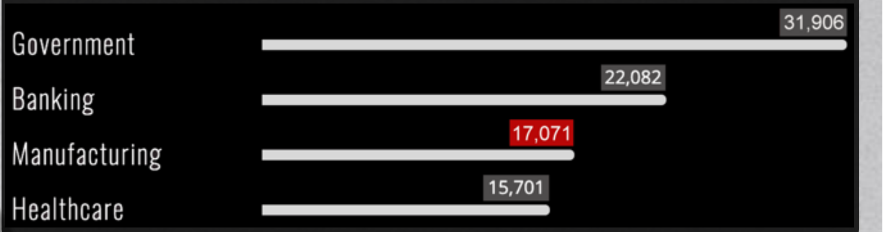
The Ugly Truth of ICS Security

Diverse and outdated operating systems in ICS

Top operating systems in the manufacturing industry

Windows 7 60.2%	Windows 10 28.9%	Windows 8.1 5.3%	Windows XP 4.4%
Windows XP 64 0.5%	Windows 8 0.4%	Windows Vista 0.2%	Windows 2000 0.1%

Manufacturing was #3 for most ransomware attacks in 2020



Fractured and Vulnerable

Less than 50% of asset owners deploy antivirus for ICS endpoints

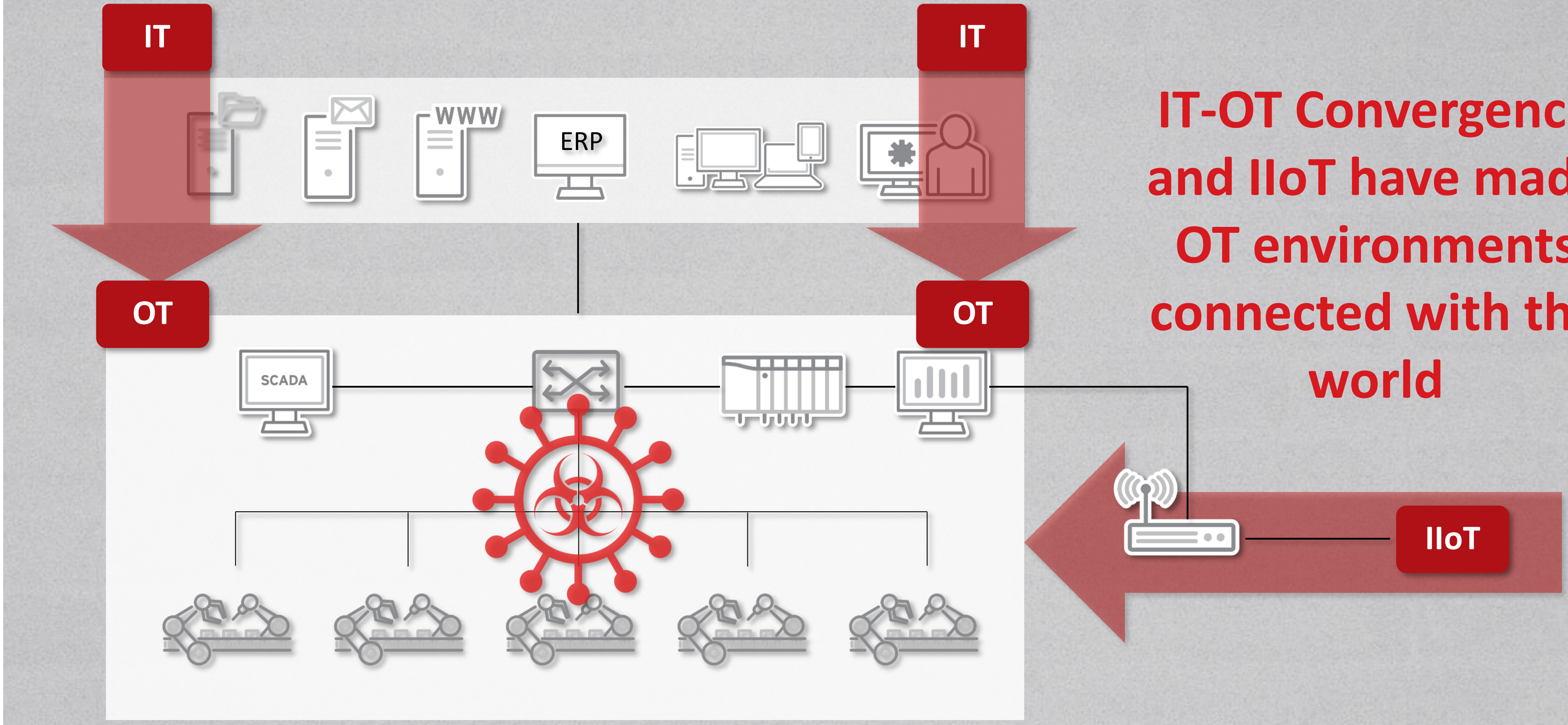
According to Trend Micro's 2020 *The State of Industrial Cybersecurity* survey of 500 manufacturers, on average the antivirus installation rate on ICS endpoints was less than 50%

Attack target: data at rest and data in use

Data in transit is usually protected by network defense. Data at rest and data in use are both generally found on endpoints, making endpoints that much more attractive to attackers

Source:
Trend Micro Securing Smart Factories Threats to Manufacturing Environments in the Era of Industry 4.0
A CONSTANT STATE OF FLUX Trend Micro 2020 Annual Cybersecurity Report

txOne networks



IT-OT Convergence and IIoT have made OT environments connected with the world

TXOne Product Suite

Single Segment
300Mbps

- Deployment Versatility
- IP/ Protocol White-listing
- Harsh environments
- Virtual Patch
- Hardware Bypass

EdgeIPS

2 WAN & 8 LAN Interfaces
300Mbps

- Micro network segmentation
- Harsh environments
- Virtual Patch
- East-West Protection
- NAT - Firewall

EdgeFire

12/24/36/48 Segments
10 Gbps+/20Gbps+

- Network segmentation
- Dedicated Management port
- Virtual Patch
- Programmable Hardware Bypass
- East-West Protection
- IP/ Protocol white listing

EdgeIPS Pro

Supports up to 1000 Network Segments

- Centralized Deployment for policies and patterns
- Full Visibility of assets, operations and security events
- 3rd-Party Integration (SIEM, ICS Detection)
- Virtual Machine Platform (VMWare ESXi / Workstation, KVM, Hyper-V)

ODC

OT Defense Console

Lockdown with AV

- File and Application Lockdown
- AV Scanning
- Supports legacy OS
- USB device lockdown

StellarEnforce

OT Endpoint Protection

- Real-Time Scanning
- Behavioral learning and detection
- Virtual Patch
- Supports legacy OS

StellarProtect

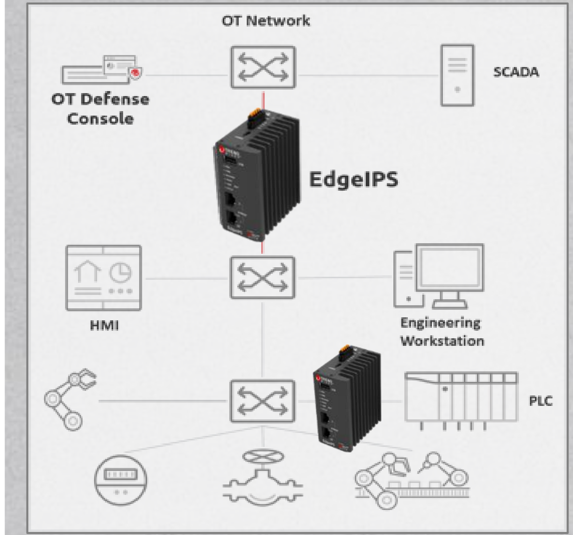
Malware scanner in USB form factor

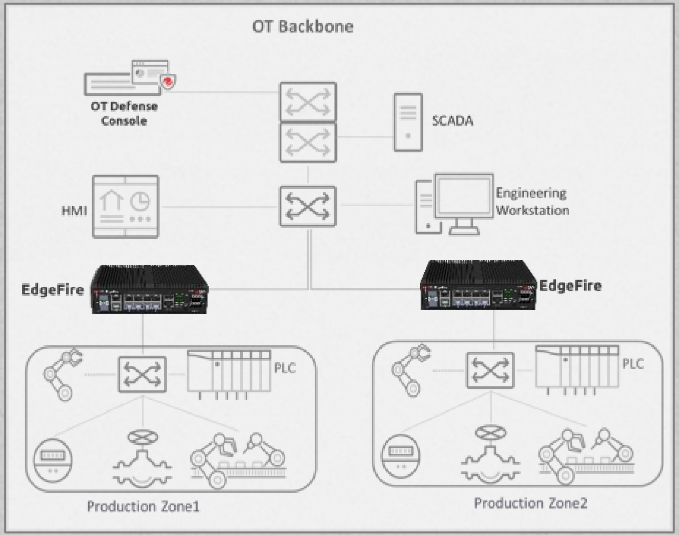
- Object Quarantine and Remediation
- Visibility of assets, patch levels, and security events
- Supports legacy OS
- No software installation needed on asset
- Minimal system resource usage

Portable Security 3

txOne networks

EdgeIPS | EdgeFire





Harsh Environments

- Small and ruggedized form factors
- Dual power inputs
- Fan-less for dirty environments
- Wide Temperature range (−40℃ to 75℃)
- Vibration and Shock Resistance

Enhanced Visibility

- Operate with comprehensive asset visibility by inspecting OT traffic
- Identify IT/OT protocols and control commands for network whitelisting policies
- Pinpoint threats and insecure assets with Edge Series' built-in UI

Protect vulnerable unpatched devices and legacy systems

- Use virtual patching to leverage the worlds-leading vulnerability research of Zero Day Initiative (ZDI)
- Granular access control over OT network protocols and control commands prevents the misuse of critical assets
- IP and Protocol lockdown

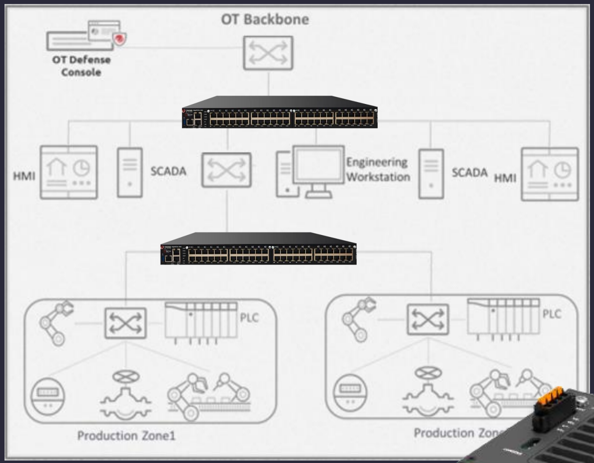
EdgeIPS – Single Segment 300Mbps

- Level 3-1 deployment versatility
- Hardware Bypass

EdgeFire – 2 WAN & 8 LAN Interfaces 300Mbps

- Network segmentation into easily managed security zones
- Built-in NAT and network switch for East and West protection
- Supports Gateway and Bridge modes

txOne networks



EdgeIPS Pro™

IT-friendly deployment with sophisticated OT network segmentation and protection for large scale production environment

Virtual Patching

Network Segmentation

Network Trust List

High Availability with Fail-Safe Design

- Module-based swappable extendable cards
- Equipped with Gen3 hardware bypass to ensure OT operational continuity
- Redundant Power

OT- Aware Operational Intelligence

- Build in TXOne One-Pass DPI (TXODI™) allowing for interoperability between key nodes and deep analysis of L2-L7 network traffic.

High Port Density with Flexible Deployment

- OT security protection deployed in IT standard rackmount
- Available for 24 segments (48 ports) up to 48 segments (96 ports)
- Local and central console supported

High Performance with full protection on

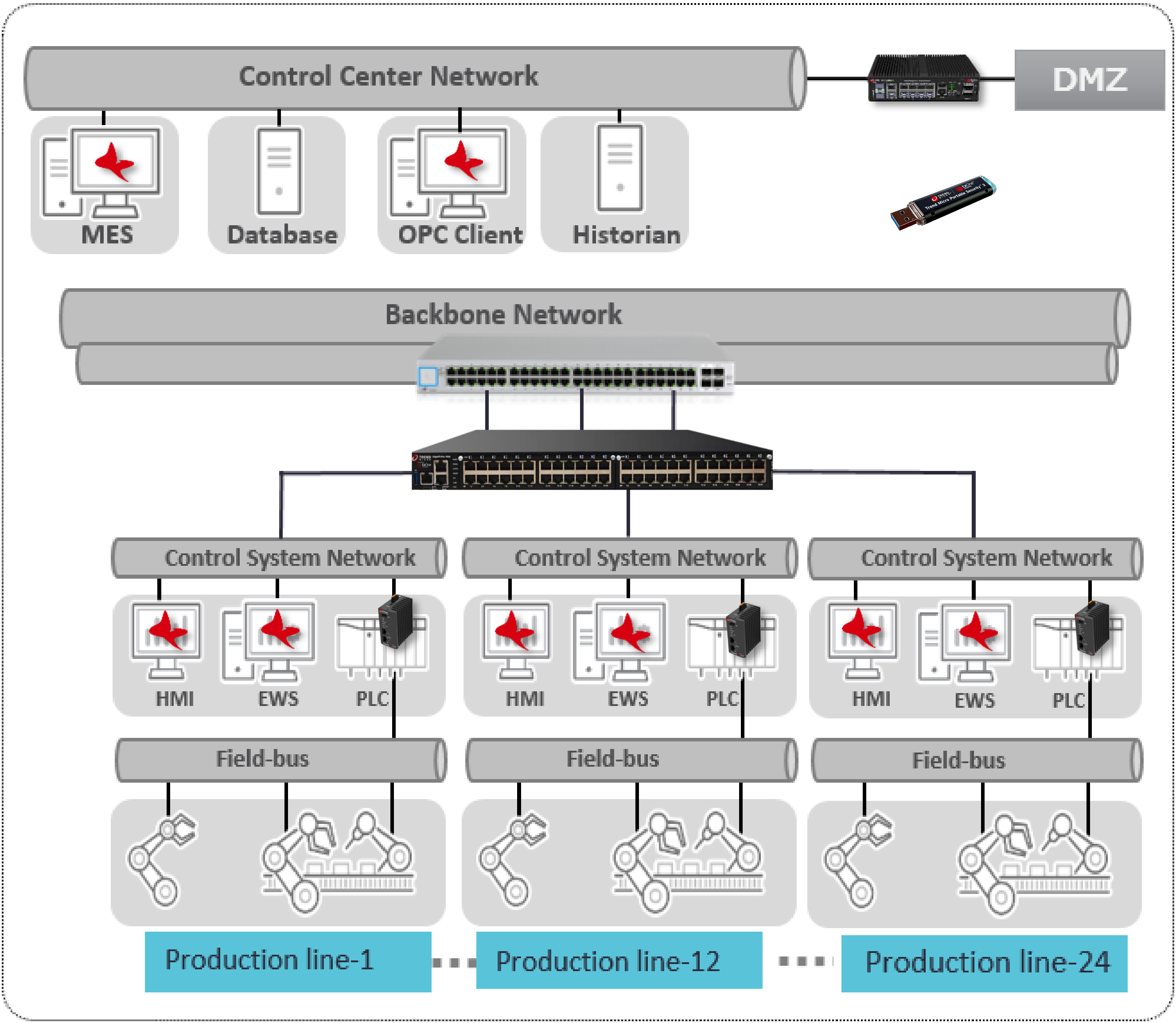
- 1048 model supports 10 Gbps total throughput with 2 M concurrent connection
- 2094 model supports 20 Gbps total throughput with 4 M concurrent connection

Variant Industrial Protocols with shadow OT detection

- Support multiple industrial protocols with advance control option
- Detect OT assets for network security visibility

IPS Pro
OFF
OT Defense Console™
48 Ports
24 Segments
96 Ports
48 Segments
EdgeIPS

TXOne Manufacturing Use Case



Manufacturing

Scenario #1

- EdgeFire – Perimeter Protection
- EdgeIPS Pro – Network Zone Protection
- EdgeIPS – One to One PLC Protection
- Stellar – Endpoint Protection
- PS3 – 3rd Party Vendor Scanning

Scenario #2

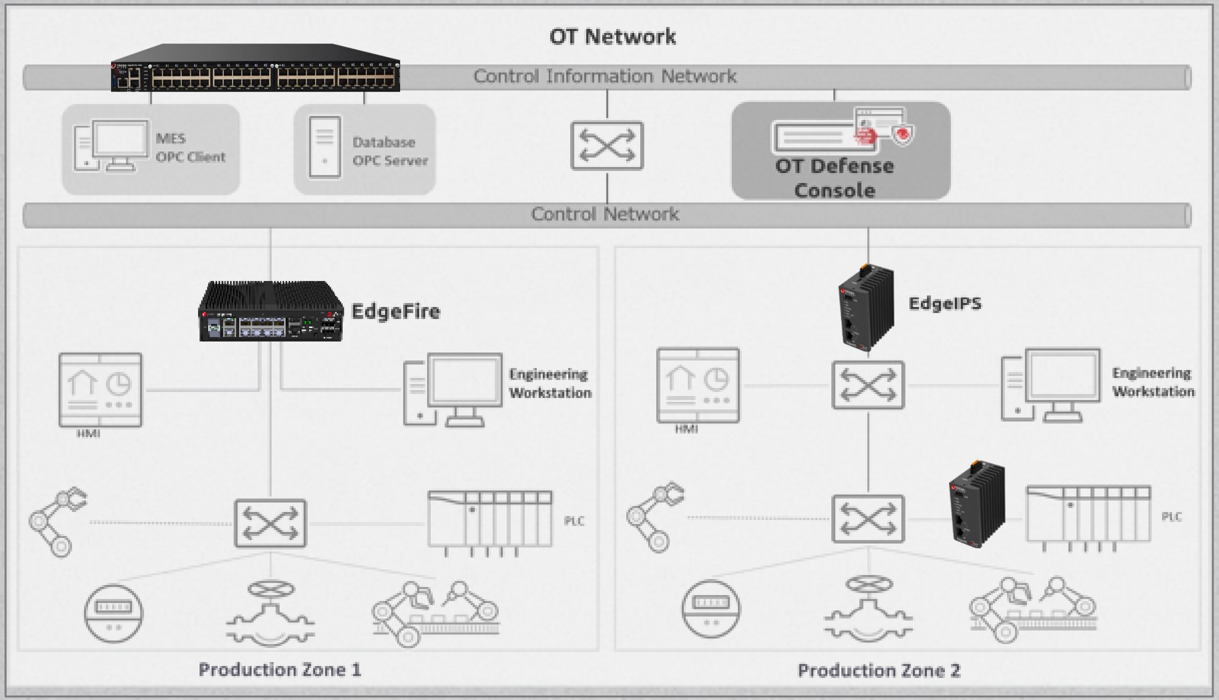
- EdgeIPS/Pro – 1 to 1 Machine Protection
- PS3 – 3rd Party Vendor Scanning

Scenario #3

- EdgeFire – Network Segregation/Protection
- Stellar – Endpoint Protection
- PS3 – 3rd Party Vendor Scanning

txOne networks

OT Defense Console™



Centralized Management

Full Visibility of Assets and Threats

Complete Node control

Broad visibility for large-scale OT networks

- Use the dashboard to easily monitor logs, receive notifications, and analyze activity in the OT environment
- Maintain an overview of system cyber risk status, threat vulnerability, and resistance to attack
- Scalable to hundreds or even thousands of nodes at multiple sites with EdgeFire and EdgeIPS

Increase convenience and interconnectivity

- Easy-to-use management policies as well as up-to-date security signature updates and provisioning
- Provide firmware and pattern updates to EdgeIPS and EdgeFire units by node group
- ODC logs activity at each EdgeFire and EdgeIPS node, including cybersecurity, policy enforcement, protocol filtering, system logs, audits, and asset detection

Flexible virtual environment and external integration

- ODC supports CEF and LEEF log export and can be easily integrated with SOC/SIEM, including Splunk and IBM Qradar
- ODC VA supports multiple hypervisors, such as VMware ESXi, VMware workstation, Hyper-V and KVM

txOne networks

txOne™ networks

Thank you