zscaler™

WHITE PAPER

# Zscaler Zero Trust Device Segmentation for Industry 4.0

In the era of Industry 4.0, where smart manufacturing and interconnected industrial systems are becoming the norm, Zero Trust architecture has emerged as a critical security framework. Traditional perimeter-based security approaches are no longer sufficient to protect the complex ecosystem of operational technology (OT) devices and industrial control systems. Zero Trust's fundamental principle of "never trust, always verify" eliminates implicit trust in the network and provides secure, authenticated access to critical systems. This approach is particularly crucial in industrial environments where a security breach could lead to significant business downtime, loss of reputation, and regulatory repercussions.

## CyberSecurity for Manufacturing

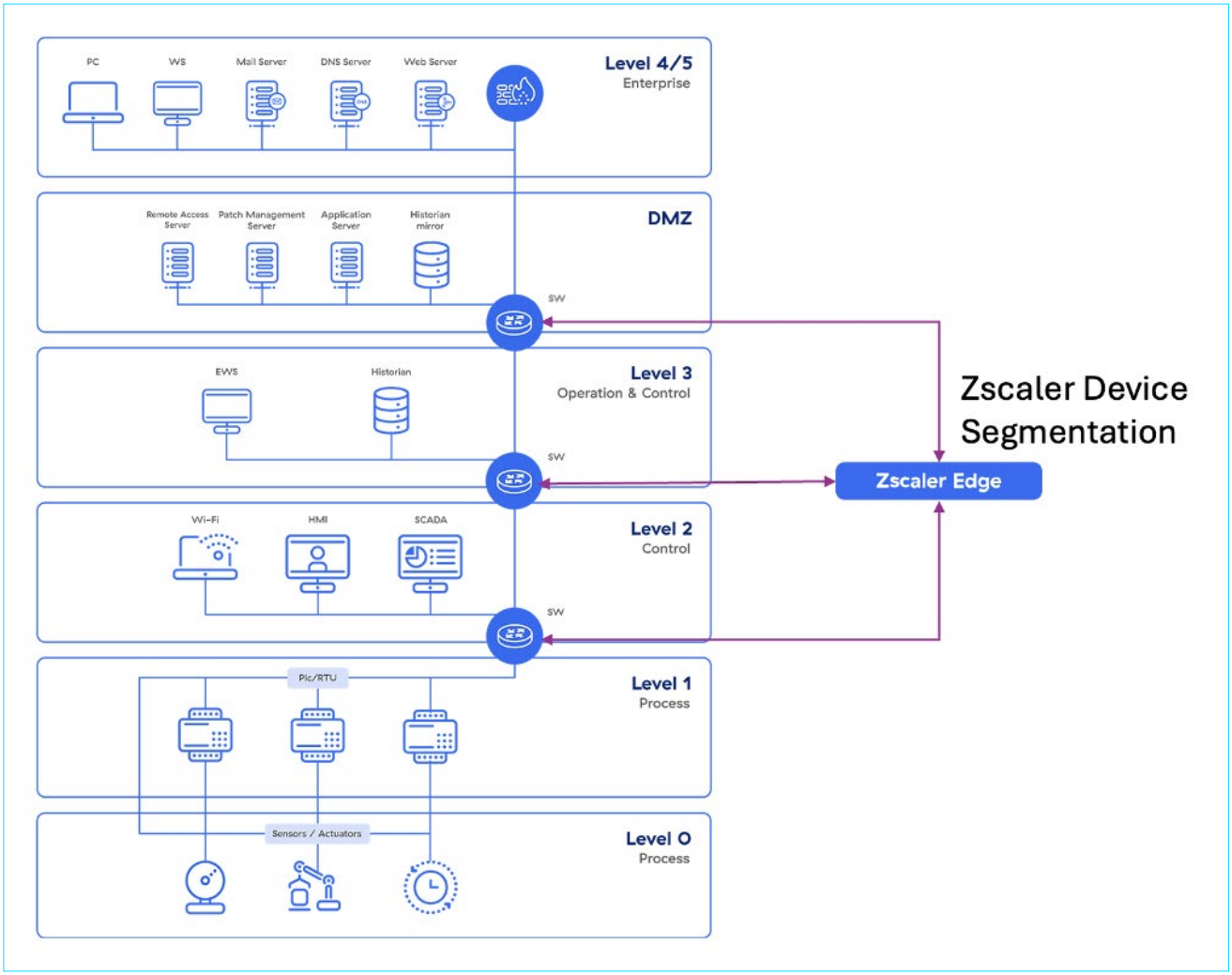
Modern manufacturing networks have evolved into complex ecosystems where operational technology (OT) and information technology (IT) systems are deeply intertwined. This convergence enables advanced capabilities such as predictive maintenance, supply chain integration, and remote operations management. However, this interconnectivity also creates new security challenges as traditionally isolated OT networks become exposed to IT-related threats. There are two big areas organization are focusing

- **Secure Access to OT Assets:** Manufacturing environments require strict control over who can access operational technology assets like PLCs, HMIs, and industrial control systems. Zscaler Privileged Remote Access enables fast, direct, and secure access to operational technology (OT) assets in field locations, the factory floor, or anywhere without relying on VPNs or agents. More details on the Zscaler Privileged Remote Access – https://cms.zscaler.com/resources/data-sheets/privileged-remote-access-for-ot-and-iiot.pdf
- **Segmentation:** A critical security concern in manufacturing environments is the potential for threats to move laterally across the network. This is particularly dangerous in industrial environments where legacy systems, which often lack modern security features, are interconnected with modern equipment. Implementing Zero Trust principles through micro-segmentation helps contain threats by enforcing the strict policy-based network access control, effectively limiting an attacker's ability to move laterally even if they breach initial defenses.

Together, Zero Trust Private Access and Segmentation work in tandem to establish a robust security framework for OT assets in manufacturing networks. This comprehensive security strategy ensures that manufacturing operations remain protected against both external threats and internal vulnerabilities, while maintaining the flexibility needed for efficient operations.

## Segmentation in Manufacturing

In typical manufacturing or industrial control networks, there are several types of devices connected to the network. As per the Purdue model, these devices can be classified into distinct levels.




| Purdue Level | Devices | Description | Risk |
|---|---|---|---|
| Level 3 | Historian, Jump Servers, Patch Servers | Runs well-known OS e.g. Windows. Despite of having EDR options, still pose a security risks for lateral threats | Medium to High |
| Level 2 | HMI, SCADA | Run embedded OS (e.g. Windows CE, Windows XP). Due to their legacy nature, these systems have serious vulnerabilities and significant security risks | High |
| Level 1 | PLCs, RTUs | Low-end headless devices that require special tools to program & modify settings | Low to Medium |
| Level 0 | Sensors, Actuators | Mostly non-IP based systems that perform very specific functions | Low |

These various types of OT devices establish complex communication patterns and dependencies with each other for seamless manufacturing processes, maintain operational continuity, and ensure reliable production output across the factory floor. Zscaler Zero Trust Device Segmentation (Zscaler ZTDS) provides comprehensive security measures to protect manufacturing operations by implementing robust access controls and establishing clear communication boundaries between different types of industrial devices. This advanced segmentation strategy helps maintain the integrity and reliability of manufacturing processes while safeguarding against potential security threats and unauthorized access attempts.

USE CASE 1

## Internet Communications

In modern manufacturing environments, OT systems increasingly require internet connectivity for various operational needs, including software updates, vendor support, and cloud-based analytics. However, this internet exposure significantly expands the attack surface of industrial networks. Previously isolated OT systems become vulnerable to common cyber threats like malware, ransomware, and advanced persistent threats (APTs). The risks are particularly acute because many OT devices were designed without built-in security features and often run legacy operating systems that cannot be easily patched or updated.

All internet communications are protected by Zscaler ZIA, with outbound connections from OT assets being routed through this service.

Zscaler ZIA Key Value

- **Advanced threat protection:** ZIA provides comprehensive security against malware, ransomware, and zero-day threats through multi-layered inspection of all internet traffic from OT assets
- **Egress filtering:** Enforces strict access controls by limiting OT device communications to only authorized destinations and blocking potentially malicious websites and content
- **Real-time threat intelligence:** Leverages global cloud intelligence to identify and block emerging threats before they can impact OT assets

USE CASE 2

## Inter OT and IT Communications

Inter OT and IT communications in manufacturing environments represent a critical intersection where OT systems must interact with IT infrastructure. This integration enables essential functions like data analytics, remote monitoring, and enterprise resource planning. However, these communications also create significant security vulnerabilities. IT networks, which are typically connected to the internet and regularly updated, must interface with OT systems that often-run legacy software and protocols not designed with modern security in mind.

This disparity in security capabilities creates potential entry points for cyber-attacks.

**Zscaler Device Segmentation Key Value:**

- Traditionally, IT and OT networks were built separately with physical air gaps between them. However, with modernization, these boundaries are blurring. Zscaler Device Segmentation helps maintain separation between IT and OT networks without compromising the productivity and value that modernization brings to industrial networks.
- Despite having separate VLANs, IT and OT systems often end up sharing the same network due to misconfiguration or rapid business changes. Zscaler ZTDS patented technology identifies all IT and OT systems in the shared network (e.g. VLANs) and logically separates them without requiring VLAN reconfiguration, IP changes, or network redesign.
- To protect legacy equipment and prevent unauthorized access to OT networks, Zscaler ZTDS helps eliminate implicit trust and restricts network access from a specific system such as JumpHosts, Zscaler ZPA, and Zscaler PRA.
- A highly scalable, centralized cloud-based management system with strong role-based access control and multi-tenancy capabilities simplifies IT and OT network operations while maintaining separate administrative duties and controls

USE CASE 3

## Operations Level Communications

At Level 3, operations level communications encompass the interactions between various manufacturing execution systems (MES), historians, and other operational management applications. These systems typically operate on standard TCP/IP networks, often utilizing protocols like OPC UA, MQTT, or REST APIs for data exchange. Network segmentation is particularly important here as these systems often bridge the gap between IT and OT networks, making them potential targets for cyber-attacks.

Zscaler Device Segmentation Key Value:

- Unlike traditional firewalls, Zscaler ZTDS operates independently of network-level details and enables dynamic policy control regardless of how operations level systems connect to the network. A centralized adaptive policy engine significantly reduce operational complexity associated with traditional firewall
- Effective incident response is crucial for reducing the impact of cyber incidents in mission-critical environments. The Zscaler Ransomware Kill-Switch is a powerful incident response tool that prepares organizations for emergency response and surgically stops threat propagation at the network level.
- Zscaler ZTDS's unique architecture centralizes all network-level intelligence and eliminates dependencies on point products and complex technologies like VLANs, ACLs, 802.1X, Firewall and L3 routing.

USE CASE 4

## Supervisory Level Communications

At Level 2, supervisory level communications involve critical interactions between HMIs, SCADA systems, and other supervisory control systems over TCP/IP networks. These systems typically communicate using industrial protocols like Modbus TCP, EtherNet/IP, and OPC UA, operating on standard network ports (502 for Modbus, 44818 for EtherNet/IP, 4840 for OPC UA). They are responsible for monitoring and controlling industrial processes, collecting real-time data, and providing operator interfaces. Due to the legacy nature of many supervisory systems, their use of potentially vulnerable protocols, and their critical role in operations, securing these communications is particularly important through proper network segmentation and protocol-specific security controls.. These communications can be further divided into:

1. Inter-Level 2 communications (e.g., HMI-to-HMI interactions)
2. Level 2 to Level 3 communications (e.g., HMI-to-Historian data transfer)

**Zscaler Device Segmentation Key Value:**

- Zscaler ZTDS patented technology uniquely ringfence supervisory systems (e.g. HMI) connected at Purdue Level 2, creating secure isolation boundaries that significantly reduce the attack surface on these legacy and vulnerable systems.
- Zscaler ZTDS detects and visualizes all device-to-device communications in Supervisory level and interactions with Level 3 (Operation Level) regardless of VLAN configuration. It creates traffic maps of these communications and maintains transaction logs in the built-in Elastic SIEM.
- Built with Zero Trust principles, Zscaler ZTDS integrates with various enterprise tools including CMDB and EDR to automatically adjust access control policies based on behavioral changes. A hierarchical policy framework enables implementation of policies across a single site, multiple site groups, or all sites.
- Simplified policy framework that uses device attributes and tags (through auto-tagging, manual entry, or third-party import) rather than complex IP and MAC addresses
- One of the biggest advantages of Zscaler ZTDS is that it's agentless, interoperates with existing networking equipment (regardless of vendor, model, or version), and requires minimal network configuration changes.

USE CASE 5

## Control Level Communication

At Level 1, PLCs and RTUs interact with each other to coordinate machine operations and process control. These devices also communicate upward with Level 2 systems like HMIs and SCADA systems to enable real-time monitoring and control of industrial processes. This communication layer is critical for maintaining operational efficiency and requires robust security measures to protect against potential cyber threats while ensuring minimal latency and high reliability. These communications can be further divided into:

1. Inter Level 1 (e.g., PLC-to-PLC communications)
2. Level 1 & Level 2 (e.g., PLC-to-HMI communications)

**Zscaler Device Segmentation Key Value:**

- Due to its unique architecture advantage, the Zscaler ZTDS visualizes and analyzes various communications and provides an ability to fingerprint and profile the connected OT systems. It analyzes the various protocols including HTTP, ENIP, Modbus, SSL etc and extract meta-data information to accurately identify and tag the OT assets.
- Visualizes all communications between L1 devices (PLCs, RTUs) and L2 systems (HMIs, SCADA). Implements restricted access controls to protect sensitive L1 devices (e.g. PLCs) from potentially vulnerable high-risk L2 devices (e.g. HMIs).
- When deployed in the learning mode, the Zscaler ZTDS accurately identifies the communication patterns from the L1 (PLC, RTUs) to the L2 devices (HMI etc). This helps in modeling the segmentation policies.
- Purdue Level 1 devices are designed for specific functions and don't implement all standard network principles. This makes it challenging to implement Zscaler ZTDS Ringfence for these devices. However, the lack of per-device segmentation or ring-fencing doesn't compromise the overall security controls.
  - Since threats typically originate from vulnerable and high-risk Level 2 devices, ZTDS restricts Level 1 devices to only the minimum necessary access to Level 2 devices required for business operations.
  - Rather than per-device segmentation, ZTDS implements macro-level segmentation (using existing network definition) or group-level segmentation (L1 devices can be grouped into small segments using Airgap-Plus).
  - Because communication between L1-to-L1 devices requires special programming, ZTDS reduces unauthorized or incorrect programming changes by restricting inbound access to L1 devices.
  - All other capabilities—including asset discovery and profiling, traffic visualization, adaptive policy control, and ransomware kill-switch remain fully applicable to Layer 1 devices.

Purdue Level O or process level devices (e.g. Sensors, actuators) does not support TCP/IP and usually directly to each or Level 1 devices using the custom protocols, serial bus etc. These devices are outside scope of the Zscaler Devices Segmentation.

## Summary

Zscaler Zero Trust Device segmentation, as a key component of Zero Trust security, plays a vital role in eliminating the implicit trust by creating logical boundaries between different types of industrial devices and systems. By implementing granular segmentation policies, organizations can isolate critical production systems from potentially vulnerable devices, contain potential security breaches, and maintain strict access controls between different layers.

| | **Use Case 1** (Internet) | **Use Case 2** (IT & OT) | **Use Case 3** (L3– Operations) | **Use Case 4** (L2 — Supervisory) | **Use Case 5** (L1 — Control) |
|---|---|---|---|---|---|
| Agentless | ✓ | ✓ | ✓ | ✓ | ✓ |
| Network Agnostic | ✓ | ✓ | ✓ | ✓ | ✓ |
| Asset Discovery & Profiling | ✓ | ✓ | ✓ | ✓ | ✓ |
| Traffic Visibility | ✓ | ✓ | ✓ | ✓ | Inter Segment |
| 3rd Party Integration | N/A | ✓ | ✓ | ✓ | ✓ |
| Adaptive Policy Control | ✓ | ✓ | ✓ | ✓ | Inter Segment |
| Ransomware Kill–Switch | N/A | ✓ | ✓ | ✓ | ✓ |
| Centralized Management | ✓ | ✓ | ✓ | ✓ | ✓ |

Segmentation projects often fail to complete because current alternatives require significant network changes (like equipment upgrades or refreshes), lack granular control, or fail to cover all layers of manufacturing networks. Zscaler ZTDS offers a unique solution, providing comprehensive coverage through an agentless, network–agnostic, and user–friendly platform. Zscaler ZTDS deploys quickly and requires no operational downtime. Manufacturing organizations can now join Fortune 500 companies in using Zscaler Zero Trust Device Segmentation (ZTDS) to quickly implement zero trust segmentation, protecting their critical operational technology (OT) and industrial control networks.



+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com