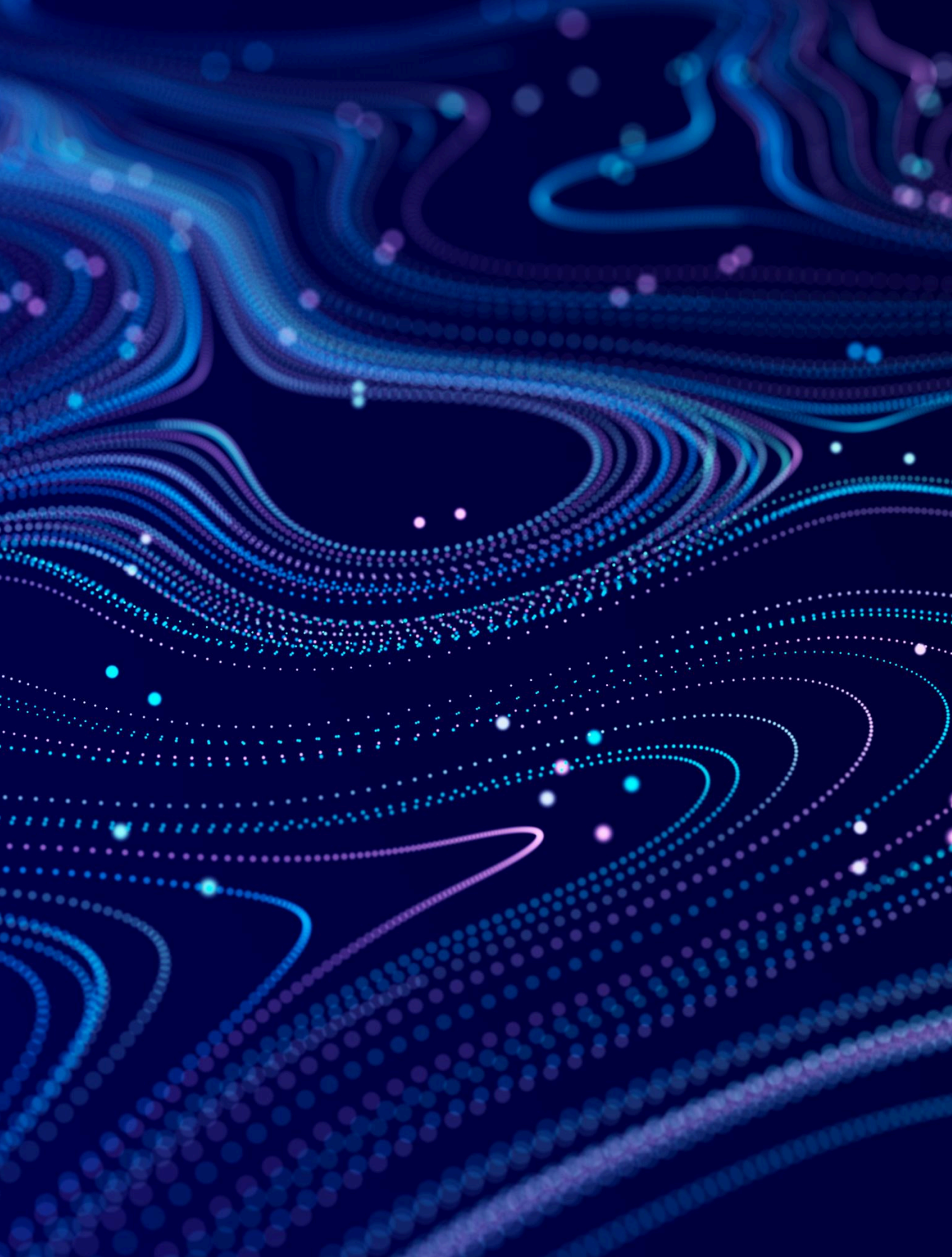


zscaler

Modernizing the Factory Network with the Zero Trust Purdue Model

Every minute of downtime costs millions and undermines your industry investment. As OT, IIoT and other factory devices connect to cloud and AI platforms, the attack surface expands exposing the limits of traditional security controls, and increasing the risk of plant disruptions.

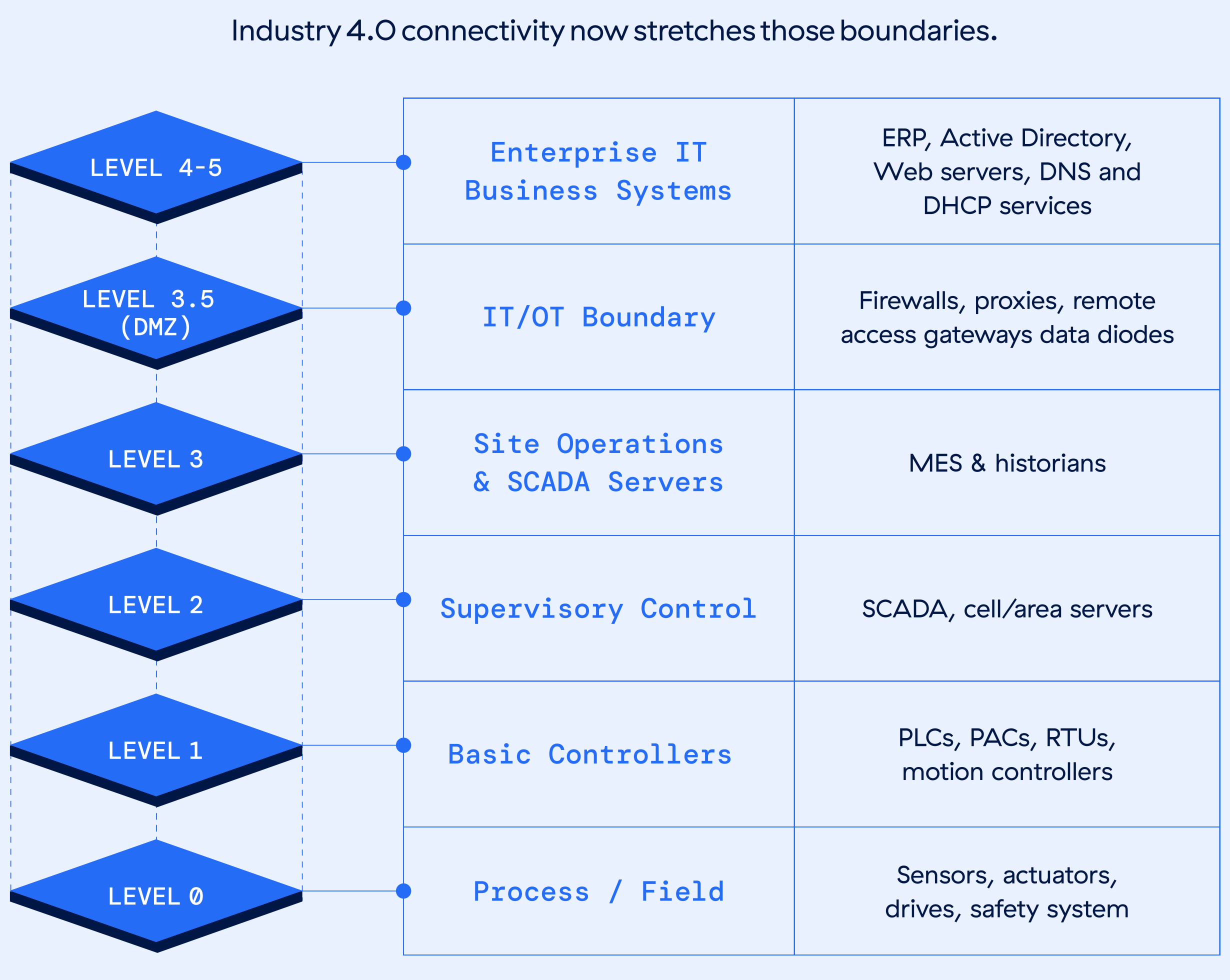
Enable cloud & AI | Stop lateral movement | Enable secure vendor access to OT

Traditional OT security control risks

- VPNs provide broad access
- Flat networks make lateral movement easy
- Cellular and 5G devices used in botnet attacks
- MPLS and SD-WAN extend trust

Classic Purdue Model at a glance

For three decades, the Purdue Model segmented factory networks from Level 0 (process) to Level 5 (enterprise IT). Industry 4.0 connectivity now stretches those boundaries.



LEVEL 4-5	Enterprise IT Business Systems	ERP, Active Directory, Web servers, DNS and DHCP services
LEVEL 3.5 (DMZ)	IT/OT Boundary	Firewalls, proxies, remote access gateways data diodes
LEVEL 3	Site Operations & SCADA Servers	MES & historians
LEVEL 2	Supervisory Control	SCADA, cell/area servers
LEVEL 1	Basic Controllers	PLCs, PACs, RTUs, motion controllers
LEVEL 0	Process / Field	Sensors, actuators, drives, safety system

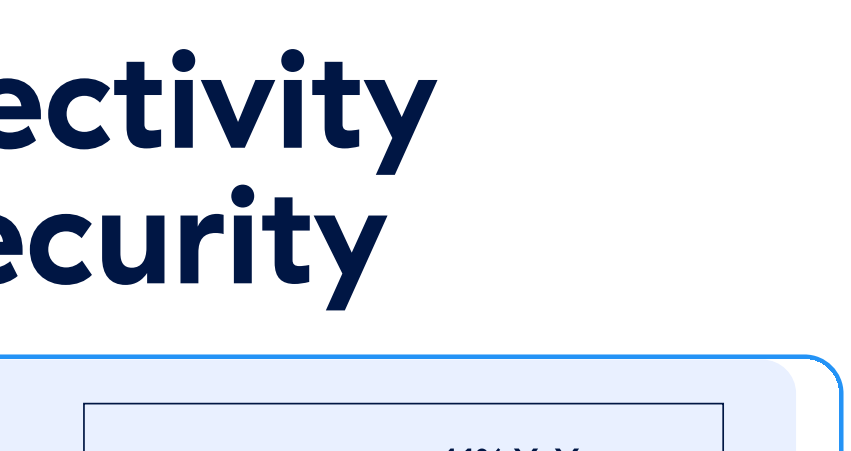
From Level 0 to Level 5 with a hatched DMZ at 3.5. Each level shows typical systems (e.g., PLCs at L1, HMIs at L2, MES/historians at L3, ERP/PLM at L4—5).

Disclaimer: Representation varies by site; shown for shared terminology only.

When connectivity outpaces security

Baseline: Converged OT/IT (Purdue-based) network

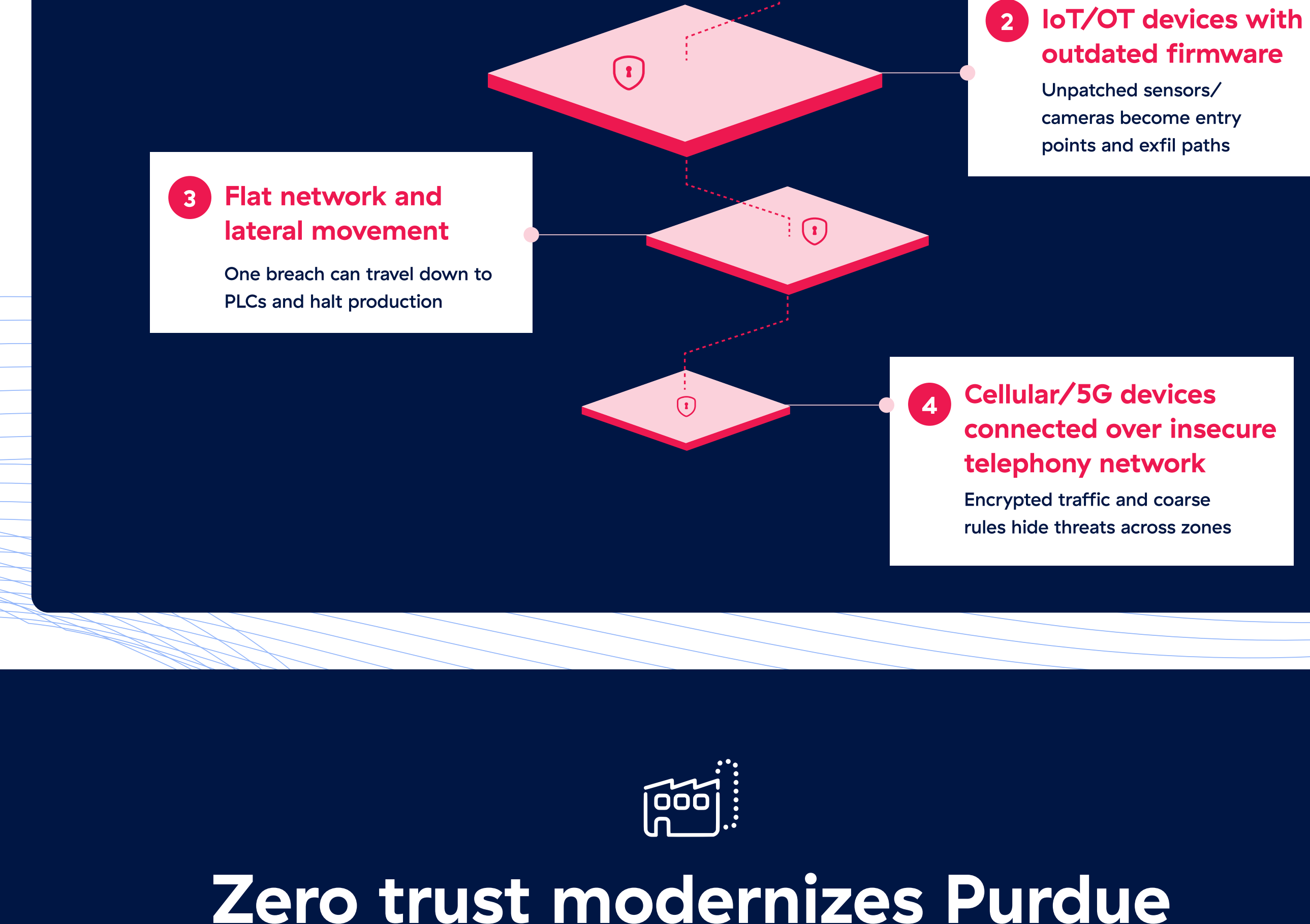
Manufacturing is the #1 most-attacked industry across IoT and mobile



41%

YoY growth in IoT malware targeting factories

Source: Zscaler. Zscaler ThreatLabz 2025 Mobile, IoT & OT Threat Report.



Inspection blind spot (DMZ)

1. **Vendor VPN into L3**
   Third-party devices reach SCADA and HMIs via VPN or jump servers, gaining broad network access
2. **IoT/OT devices with outdated firmware**
   Unpatched sensors/cameras become entry points and exfil paths
3. **Flat network and lateral movement**
   One breach can travel down to PLCs and halt production
4. **Cellular/5G devices connected over insecure telephony network**
   Encrypted traffic and coarse rules hide threats across zones

Zero trust modernizes Purdue Model for Industry 4.0

Identity-based access replaces network trust. Every user, device and app is verified before connection. Outbound-only connectors broker app sessions; microsegmentation prevents east-west spread.

Classic risks	Zero trust corrections
Vendor VPN into L3	**Privileged Remote Access (PRA):** Contractors connect only to approved apps through monitored, time-bound sessions
DMZ/inspection blind spots i.e cellular/5G devices connected over insecure telephony network	**Zscaler Cellular identification and isolation:** Deliver secure connectivity to field OT and cellular devices
Flat segmentation and lateral movement	**OT microsegmentation:** Segment OT systems and enforce business policies without plant disruptions
IoT devices/outdated firmware	**Secure OT connectivity without SD-WAN:** Connect OT to cloud and private apps without extending traditional SD-WAN to factories

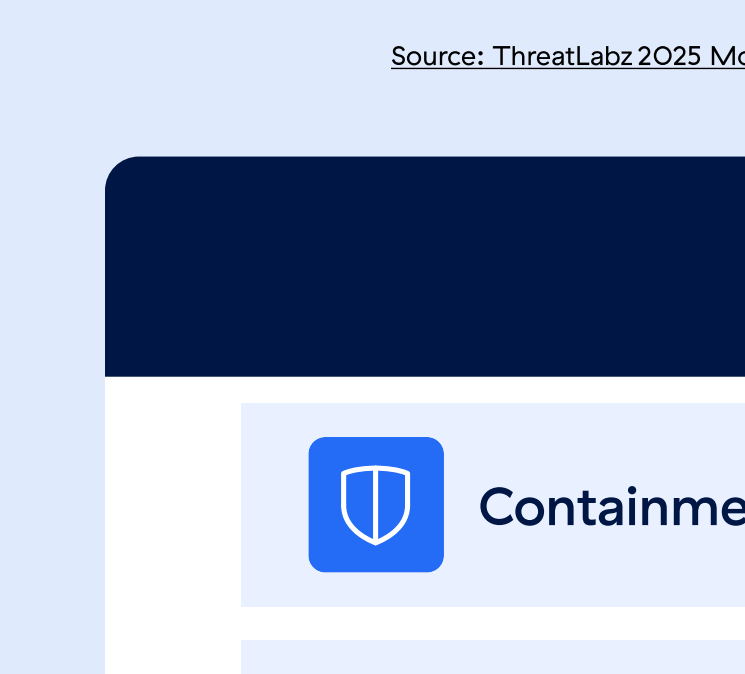
Day-1 actions—Mapped to risks 1 to 4

Start with these four control changes. Each action directly addresses a risk called out earlier.

- ✓ Replace VPN with app-level access
- ✓ Time-bound vendor sessions, recorded
- ✓ Isolate IoT by identity and posture
- ✓ No lateral movement across zones

What manufacturers gain by applying Zero Trust to the Purdue Model

Protect production, IP and safety while safeguarding your Industry 4.0 investment.

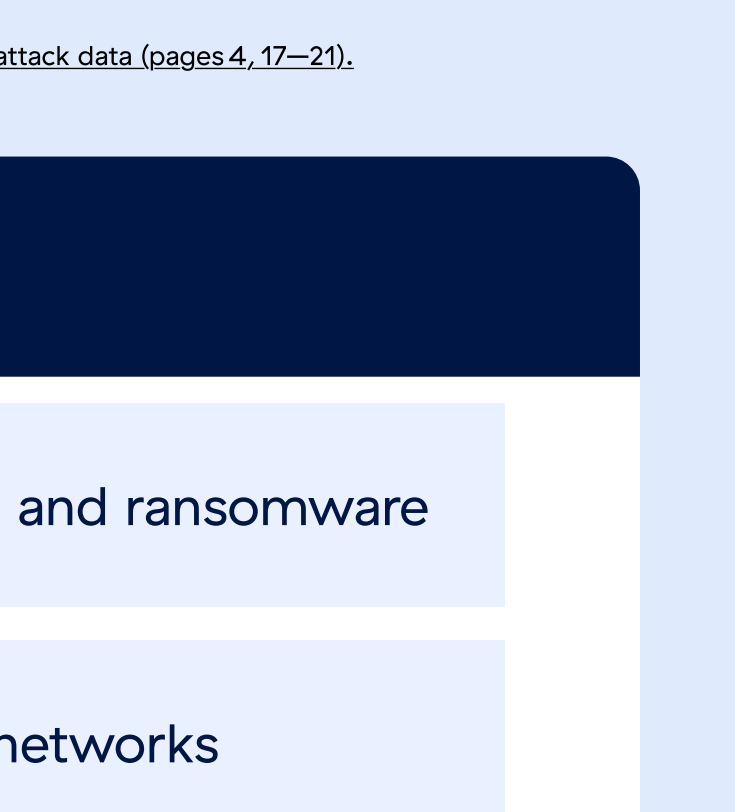


Target SLO with Zero Trust Purdue Model

41% IoT malware growth

0% production loss objective with zero trust

Threats are rising, but downtime doesn't have to



Energy and Oil/Gas IoT attacks up 459% YoY, and manufacturing follows a similar trajectory

Source: ThreatLabz 2025 Mobile, IoT & OT Threat Report (Zscaler, 2025) — used for all threat statistics and attack data (pages 4, 17—21).

Value realized

- **Containment:** Prevent lateral movement of malware and ransomware
- **Lower cost:** Remote maintenance without exposing networks
- **Visibility:** Central monitoring of all connections and sessions
- **Compliance:** Ensure compliance with IEC 62443
- **Efficiency:** Reduce firewall rules and VPN overhead

Protect production, IP and safety, while safeguarding your Industry 4.0 investment

Secure connectivity from enterprise to edge without re-architecting plants

- PRA – App-level access to L3 servers/HMIs (no VPN, no IP exposure)
- ZIA – Inline threat inspection for cloud and vendor traffic
- ZTB – Monitor remote OEM session performance
- ZERO TRUST SERVICE EDGE – Monitor remote OEM session performance
- UNIFIED LOGGING – Map controls to IEC 62443, NIS2 and CMMC

↗ See how Zero Trust modernizes the Purdue Model

zscaler | **Act Fast. Stay Secure.**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange is the company's cloud native platform that protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location.

Distributed across more than 150 data centers globally, Zscaler's SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. It powers all four categories of Zscaler services, including Zscaler Internet Access, which secures connections to the internet and SaaS applications and protects against cyberthreats; Zscaler Private Access, which provides zero trust access to internal applications in the cloud and data center without a VPN; Zscaler Cloud Protection, which secures workloads using microsegmentation and by identifying cloud misconfigurations; and Zscaler Digital Experience, which provides visibility into the complete path between user and app to pinpoint performance issues. Zscaler has been a Leader in the Gartner Magic Quadrant for Secure Web Gateways every year since 2011 and was 2020's only Leader.

With more than 10 years of experience developing, operating, and scaling the cloud, Zscaler serves thousands of enterprise customers around the world, including 500 of the Forbes Global 2000 organizations. In addition to protecting customers from damaging threats, such as ransomware and data exfiltration, it helps them slash costs, reduce complexity, and improve the user experience by eliminating stacks of latency-creating gateway appliances.

Zscaler was founded in 2007 with a mission to make the cloud a safe place to do business and a more enjoyable experience for enterprise users. Zscaler's purpose-built security platform puts a company's defenses and controls where the connections occur—the internet—so that every connection is fast and secure, no matter how or where users connect or where their applications and workloads reside.

Vision statement

Zscaler exists to create a world in which the exchange of information is always secure and seamless.

Mission statement

To anticipate, secure, and simplify the experience of doing business, transforming today and tomorrow.

- ThreatLabz 2025 Mobile, IoT & OT Threat Report (Zscaler, 2025) — used for all threat statistics and attack data (pages 4, 17—21).
- Zero Trust Purdue Model for OT/ICS Reference Architecture (Zscaler, 2025) — used for all architectural and compliance references (pages 12—18).

All quantitative metrics and Zero Trust technical descriptions in this infographic are derived directly from these Zscaler primary sources.

© 2026 Zscaler, Inc. All rights reserved.

Zscaler.com