

Zscaler for Manufacturing

Bring Zero Trust to the Purdue Model

SOLUTION BRIEF

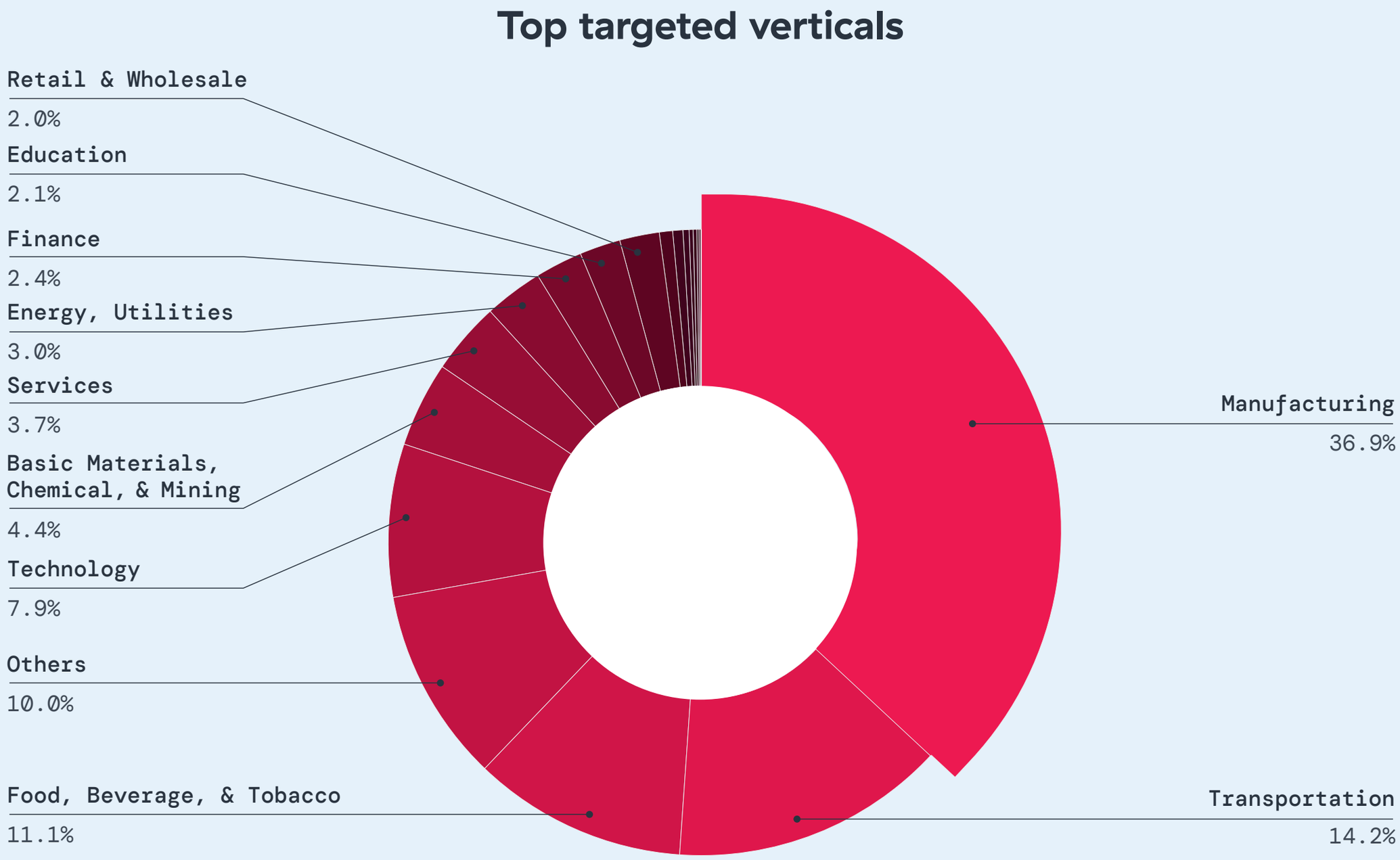
©2025 Zscaler, Inc. All rights reserved.

Factories need a fresh take to secure OT systems

Global manufacturing organizations have set out to improve their production lines, adding smart robots, IoT sensors on every machine, cloud-based analytics, and a digital twin of the entire plant floor. The goal is simple: higher output, lower downtime, and predictive maintenance that enable 24/7 production.

But many organizations have recognized a different reality. Each new connection expands the OT attack surface. And, once the attackers get in, the risk of impact is much greater due to outdated OS, flat networks, and limited OT visibility. To continue factory transformation, factories need to rethink their security architecture.

In the latest Zscaler, Threatlabz IoT/OT report, manufacturing was hit the hardest accounting for 36% of IoT malware blocks.



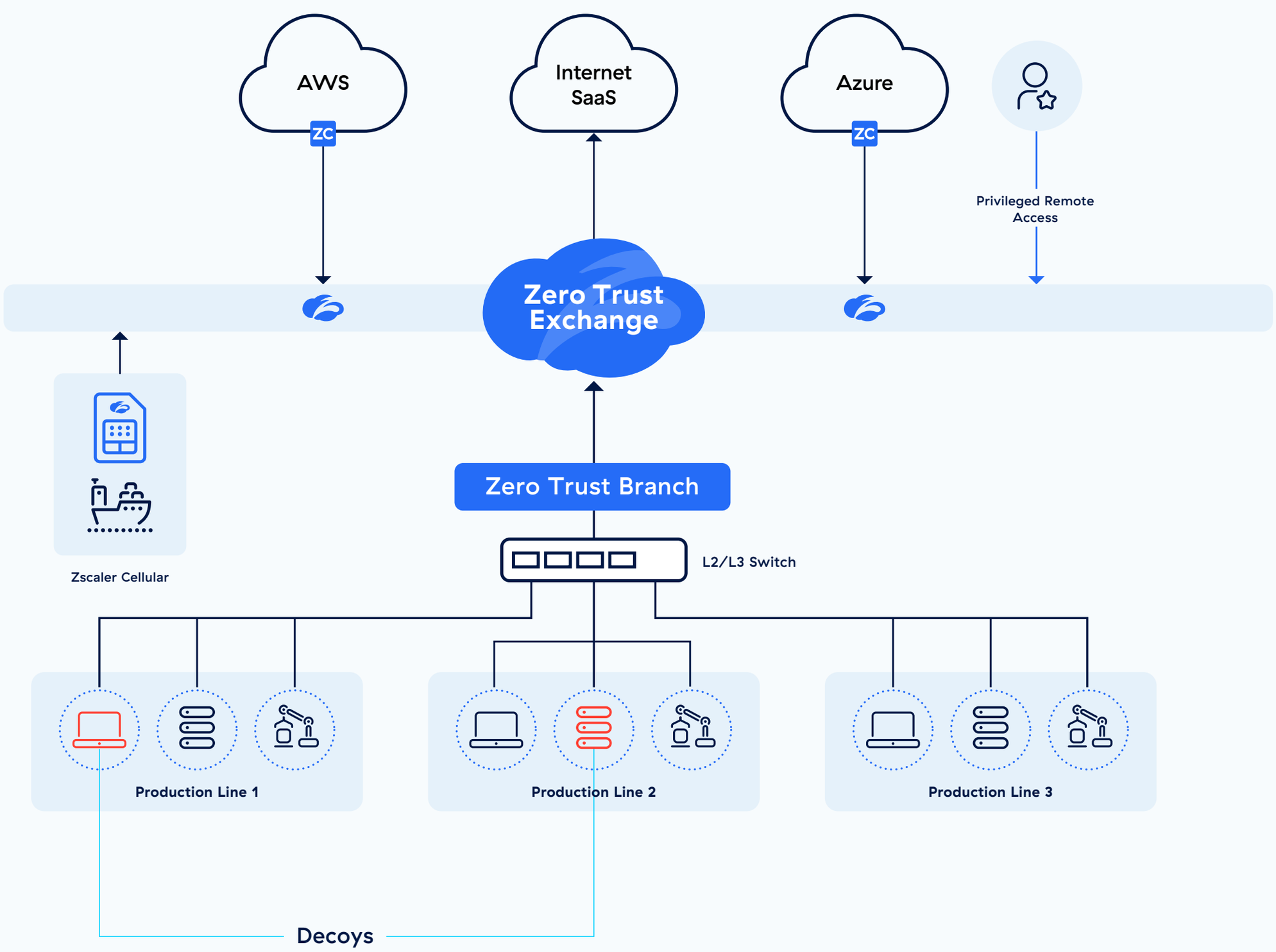
Distribution of the most targeted industries

©2025 Zscaler, Inc. All rights reserved.

Extend Zero Trust to every user and device, inside and outside your factories

To secure manufacturing and industrial environments, security teams need to ensure every user and device interaction is inspected and enforced according to least-privileged policies. Our Zero Trust approach is purpose-built for OT, enabling secure access, segmentation, and connectivity across your factory operations.

- Give technicians and third parties access to critical OT systems without VPNs
- Enforce granular east-west segmentation to prevent lateral movement of threats
- Securely connect OT systems to the cloud and data center for analytics
- Extend zero trust to cellular OT systems like trucks, kiosks, and POS scanners
- Detect attackers early and prevent them from escalating privileges



Zero Trust Factory Architecture

©2025 Zscaler, Inc. All rights reserved.

Zscaler Solution Components

Privileged Remote Access

Enable third-parties and remote technicians to securely connect to RDP/SSH/VNC targets through any browser without agents.

KEY CAPABILITIES

Clipboard Controls Limit copy/paste capabilities based on zero trust policies to protect sensitive data.	**Audit and Governance Controls** Reduce third-party risk with session recording, session sharing, and ushered access.
Credential Vault and Mapping Store credentials to target systems in a cloud vault and share access through mapping policies.	**Time-Bound and Just-in-Time Access** Allot maintenance windows and provision JIT access for emergency maintenance.

Zero Trust Segmentation

Microsegment OT systems and enforce policies to ensure only authorized communications between your OT systems and OT-IT systems.

Granular Microsegmentation Isolate supported OT systems into a segment of one (using /32).	**Device Discovery and Classification** Automatically discover and classify OT devices.
Ransomware Kill Switch Automate incident response by using preset policies to progressively lock down OT systems.	**Policy Enforcement** Group devices automatically and enforce policies for east-west traffic based on device type/tags.

©2025 Zscaler, Inc. All rights reserved.

Secure OT access

Enable cameras, sensors, monitors, kiosks and other OT systems to securely connect to the cloud applications and internet. Prevent communication with risky or malicious apps and URLs.

Zero Touch Provisioning Leverage fully automated zero touch deployment with predefined templates.	**Unified Zero Trust Policies** Inspect and enforce policies for IoT/OT to private apps and the internet.
Granular Policy Enforcement Enforce policies based on user/device geo, location, URLs accessed, sensitive data etc	**Zero Trust Cellular** Easily easily Zero Trust to connect cellular devices such as trucks, kiosks, rigs etc

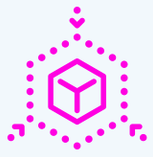
Zscaler Deception

Use decoys to detect OT threats that have bypassed existing defenses. Detect compromised users, stop lateral movement, and defend against ransomware and malicious insiders.

Lateral Movement Detection Deploy decoy PLCs and SCADA systems to detect attackers attempting to move laterally.	**Pre-Breach Detection** Get accurate alerts when threat actors are scoping out your environment before an attack.
Cloud Native Deployment Integrates with Zscaler Private Access (ZPA) to create, host, and distribute decoys.	**Zero Network Configuration** Say goodbye to VLAN trunking, SPAN ports, and GRE tunnels to route traffic to decoys.

©2025 Zscaler, Inc. All rights reserved.

Zscaler differentiators



ELIMINATE SECURITY GAPS

Enforce consistent Zero Trust policies across all environments inside and outside your factories.



REDUCE DOWNTIME

Enforce Zero Trust segmentation with minimal disruption to your existing OT environment, reducing the risk of downtime due to lateral movement.



REDUCE COST AND COMPLEXITY

Reduce or consolidate firewall, NAC, VPNs, VDIs, and microsegmentation tools with a simpler Purdue Model security architecture inside your factories.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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

zscaler™

Zero Trust Everywhere