Zscaler IoT/OT Security

Delivering the necessary technical architecture to protect complex systems from advanced cyber threats

Traditional IT security frameworks are increasingly inadequate to address the growing risks posed by Internet of Things (IoT) and operating technology (OT) environments.

Legacy technologies with outdated software, devices not originally designed for network connectivity, and IoT controllers or sensors that lack robust patching and update mechanisms create gaps for hackers and other malicious parties to exploit. A *single compromised vulnerability* in an exposed device can allow threat actors to move laterally across networks and gain access to mission-critical assets. These attacks can escalate quickly, resulting in unauthorized control over physical systems and infrastructure.

Potential results include disruption to your organization or public service, substantial financial losses, steep penalties for noncompliance, damage to industrial equipment, and risks to employee safety and even the environment.

Securing these interconnected environments requires a shift from traditional defenses toward an identity-centric security model that is more agile and resilient.

Why Zero Trust matters

Zscaler's cloud-native Zero Trust Exchange (ZTE) architecture delivers real-time monitoring, segmentation, and policy-based access controls to secure complex environments.

A successful OT breach can have **severe consequences**–from halted manufacturing operations and disruption of essential public services (e.g., electricity, water) to damage of industrial equipment and even risks to **employee safety** and the **environment**. Beyond operational impacts, such incidents can lead to substantial **financial losses**, including penalties due to **regulatory non-compliance**.

In environments where agents cannot be deployed (legacy OT systems, specialized factory equipment), organizations can utilize Zscaler to establish secure, policy-driven communication channels among office locations, data centers, and industrial sites.

Zscaler's ZTE helps ensure that every device, user, and application communicates securely, regardless of location or method of connectivity.

Zscaler capabilities for IoT/OT

The ZTE platform is engineered to reduce, minimize or something that is not a guarantee implicit trust and enforce strict, identity-centric access controls across the full spectrum of OT devices and systems. Built for scalability and distributed environments, Zscaler's Zero Trust approach is particularly well-suited to securing the diverse and geographically dispersed nature of IoT and OT deployments by:

Microsegmentation and least privilege access: Implements granular segmentation by device identity, context, and authorized function, minimizing the risk of lateral movement within the network.

Policy-based access control: Enforces dynamic, context-aware policies so only authorized users, devices, and applications can access critical OT systems.

Continuous monitoring and anomaly detection: Delivers real-time inspection and behavioral analytics across connected IoT and OT devices.

Threat detection and response: Provides inline inspection of traffic, including encrypted communications, to detect and mitigate known and unknown threats, malware, and sophisticated attacks targeting IoT/OT protocols.

Seamless integration with existing infrastructure: Supports complex hybrid environments across cloud and on-premises systems, including SCADA and ICS networks, enables consistent security without disrupting operations.

The KPMG advantage

KPMG offers strategic consulting, implementation services, and governance frameworks to help organizations integrate Zscaler into broader security programs and build operational resilience.

KPMG leverages extensive industry experience to guide organizations in securing their IoT/OT environments. Our tailored approach is designed to align cybersecurity initiatives with overarching business objectives and critical regulatory requirements, fostering long-term resilience and sustainable operational continuity. We begin with a thorough assessment of the client's IoT/OT landscape, focusing on critical asset identification, vulnerability analysis, and the obligation to adhere to regulatory requirements.

Our methodology is structured around several key pillars:

- **Cybersecurity risk and maturity assessment:** KPMG conducts in-depth evaluations of current IoT/OT security posture, identifying critical gaps, emerging threats, and areas for improvement.
- **Secure architecture design and modernization:** KPMG designs resilient security architectures that integrate zero trust principles, tailored to unique OT profiles and industry-specific needs.
- **Governance, risk, and compliance frameworks:** KPMG helps organizations establish thorough policies, procedures, and controls for the lifecycle of IoT/OT devices.
- **Regulatory alignment and compliance enablement:** KPMG maps the organization's security controls to relevant industry standards and regulatory bodies. This helps ensure that security investments not only mitigate risk but also contribute to compliance requirements.

How KPMG implements Zscaler IoT/OT

Our strategic implementation for integrating Zscaler's IoT/OT security capabilities is structured as a phased and iterative process, designed to minimize disruption while maximizing security posture uplift. It follows four phases:

1. **Assessment and strategic planning:** KPMG conducts in-depth workshops with key stakeholders across IT, OT, and business units. KPMG also performs detailed analysis of device inventory, network architecture, communication protocols, and existing security controls.

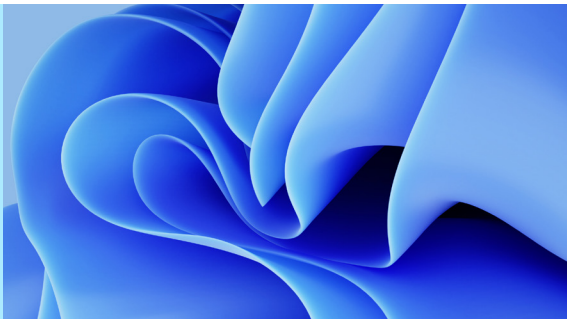
2. **Sandbox deployment and validation:** KPMG selects high-risk use cases and deploys Zscaler microsegmentation, policy-based access, and threat detection mechanisms. Additional design and testing of security policies, system performance, and integration points are gathered for feedback on production usage.

3. **Enterprise-wide rollout and operational integration:** KPMG expands Zscaler deployments across identified IoT/OT domains, via insights obtained from the Sandbox deployment. Zscaler telemetry and alerts are then implemented with Security Information and Event Management platforms and Security Orchestration, Automation, and Response systems.

4. **Continuous optimization and threat intelligence integration:** KPMG establishes key performance indicators and dashboards to continuously monitor system performance, threat detection, policy compliance, and operational impacts. Regular policy reviews are performed with adjustments based on threat intelligence and operational changes.

Gain control of your security

Zscaler's cloud-native infrastructure delivers scalable protection without the reliance on traditional on-premises hardware, offering a highly resilient and secure solution for IoT and OT systems. Combined with the strategic guidance and implementation experience of KPMG, Zscaler's platform helps organizations proactively mitigate risk; achieve regulatory compliance; and build resilient, future-ready operations.



Contact us

Sai Gadia
Partner, KPMG LLP
E: sgadia@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**