Zero Trust

The secure SIM for IoT.

IXT Zero Trust eliminates the attack surface on your cellular-connected IoT and OT devices. It replaces VPN complexity with device-initiated access, real-time traffic inspection, and full visibility into what every device communicates with. No VPN clients. No exposed ports. No software agents on endpoints. Security is enforced at the SIM and network level.

The first solution to extend Zero Trust to OT and IoT endpoints over cellular. Built on the same architecture Zscaler delivers to Fortune 500 enterprises, adapted for connected devices.

Zero Trust Connectivity

Powered by Zscaler ZTNA

Secure endpoint-to-application access with full traffic inspection. Eliminates VPN dependencies and removes exposed ports from your infrastructure.

- SASE/ZTNA: Zero exposed ports on datacenter or cloud side
- Privileged Remote Access: Browser-based SSH, VNC, RDP for service technicians and third parties
- Dynamic firewall inspection with real-time policy enforcement
- Malware scanning and sandboxing on all file transfers
- Time-limited, recorded sessions. No VPN client distribution.

Zero Trust Visibility

Powered by Illumio

See every connection your IoT devices make. Detect threats the moment they appear. Control what is allowed across your entire device fleet.

- Traffic flow extraction: All communications through the mobile gateway are captured
- Visual traffic mapping: See which devices talk to which endpoints in real time
- Automatic anomaly detection with immediate alerting
- Policy-based segmentation across any device type
- Works for both intelligent and unintelligent devices, including headless endpoints

Zero Trust

How Zero Trust compares to VPN and APN

	VPN	APN ONLY	IXT ZERO TRUST
Attack surface	Exposed ports, full network access	Isolated, trust assumed inside	Zero exposed ports. Device-initiated only.
Visibility	Tunnel status only	No device behavior insight	Visual traffic map. Anomaly alerts.
3rd party access	Full network via VPN client	Not addressed	Browser-based, timelimited, recorded
Client software	Required on every device	None	None. Security at SIM level.
NIS2 compliance	Encryption only	Limited audit trail	Full audit trail + segmentation
Built for	Laptops and users	Basic IoT isolation	IoT/OT, incl. headless devices

Zero Trust

How it works

IXT Global SIM

Your device connects through IXT's cellular network. 600+ networks in 190+ countries.

1

Private Network

SIMs are registered to your account with full lifecycle management. Apply custom labels and organize by region, project, or device type.

2

Zscaler Exchange

Traffic is inspected and policy-enforced through the Zero Trust Exchange.

3

Illumio Mapping

Every device connection is mapped, monitored, and checked against expected behavior.

4

Secure Access

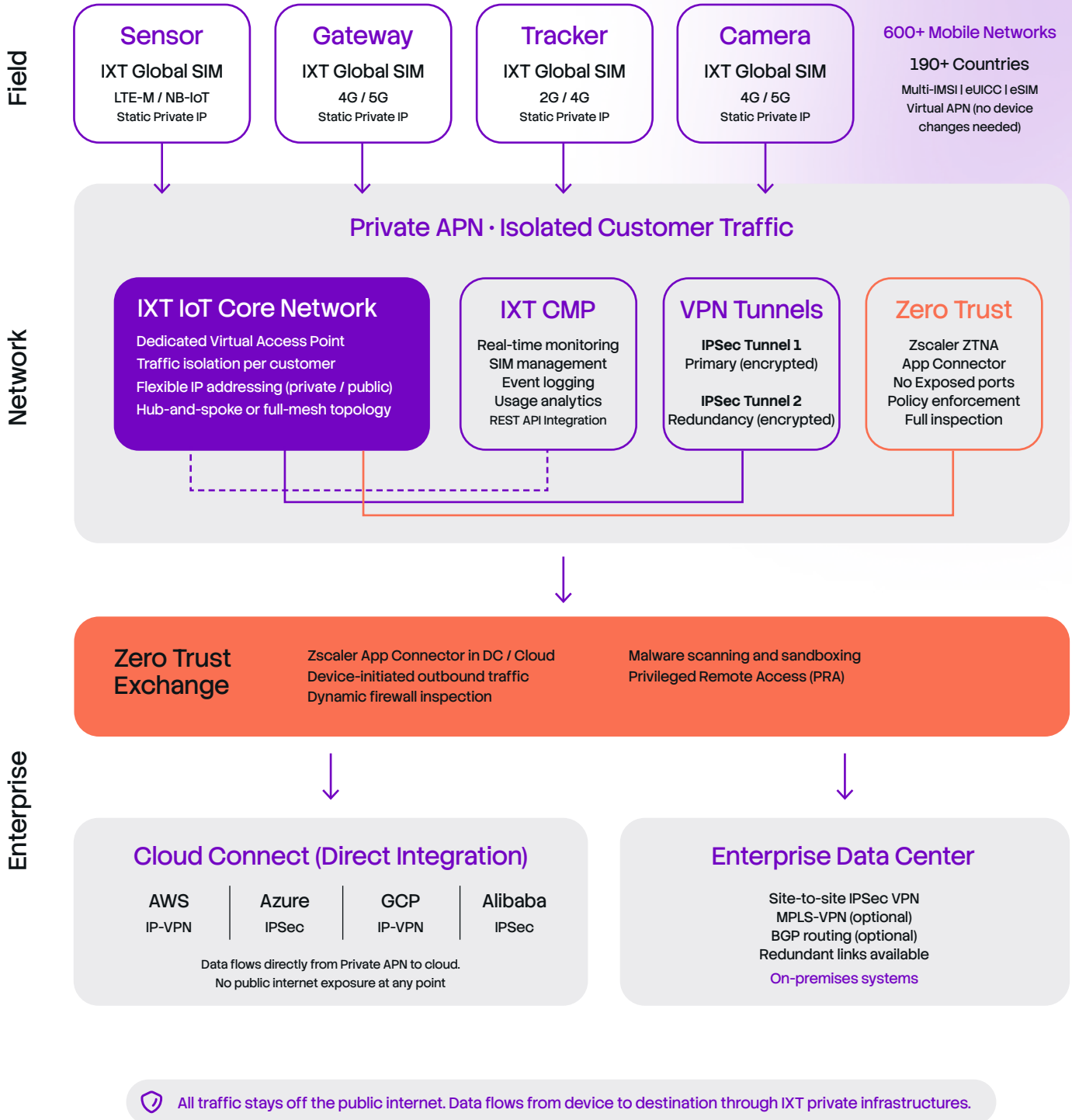
Traffic reaches only authorized applications. Third parties connect via recorded sessions.

5

Zero Trust

Security Architecture

Private networking for IoT. Keep your data off the public internet.



All traffic stays off the public internet. Data flows from device to destination through IXT private infrastructures.

Industry applications

Industrial Automation

Vendors connect to your machinery via VPN with broad network access. Privileged Remote Access gives them browser-only access to specific machines. Every session is time-limited and recorded.

Security and Surveillance

Compromised cameras and access control systems become network entry points. Traffic mapping shows all device communications. Anomaly detection alerts you when a device contacts an unexpected destination.

Tracking and Logistics

Location and cargo data crosses borders over public networks. Private infrastructure keeps commercially sensitive data off the public internet. Segmentation controls who sees what.

EV Charging

Payment data and grid communication share the same infrastructure. Segmentation separates payment processing from grid management. Remote service access through recorded browser sessions replaces VPN distribution.

Deployment and specifications

Client software	None required on devices
Device types	Intelligent and unintelligent endpoints
Network support	2G, 3G, 4G, 5G, LTE-M, NB-IoT
Coverage	600+ networks across 190+ countries
Cloud integrations	AWS, Azure, GCP, Alibaba Cloud
Management	IXT CMP + Zscaler Portal + Illumio Console
Infrastructure	Managed by IXT and Shift Security
Hardware on your side	None

Zero Trust

Zero Trust vs. SecureNet-only

IXT Zero Trust is the full security offering for IoT connectivity. SecureNet-only is available for deployments where private networking meets your requirements without Zero Trust capabilities.

Capability	Zero Trust	SecureNet-only
Global cellular connectivity (600+ networks)	✓	✓
Private APN and direct cloud connect	✓	✓
VPN tunnels (IPSec)	✓	✓
Zscaler ZTNA (zero attack surface)	✓	–
Privileged Remote Access (browser-based)	✓	–
Illumio traffic mapping and anomaly detection	✓	–
Policy-based device segmentation	✓	–
Malware scanning and sandboxing	✓	–