

FIVE OT CYBERSECURITY PREDICTIONS 2026

AXITE SECURITY TOOLS ANALYST PREDICTIONS 2026

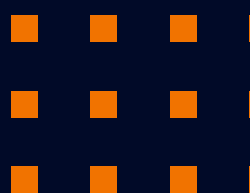


GEOPOLITICAL PRESSURE



Rising geopolitical tension will drive more digital attacks on critical infrastructure.

State-aligned groups increasingly target energy, water, transport, and manufacturing — a trend already underway and expected to accelerate in 2026.

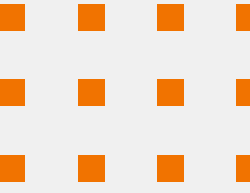




AI will accelerate OT reconnaissance — for both attackers and defenders.

Attackers use AI to map networks and find vulnerabilities faster. Defense shifts to anomaly-first detection and predictive analytics.

AI-DRIVEN RECONNAISSANCE



IT and OT will merge into one ecosystem

OT increasingly moves into IT and cloud environments, expanding the attack surface.

Zero-trust becomes essential as traditional boundaries disappear.

IT/OT CONVERGENCE





LEGACY OT AS AN INSURANCE RISK

Cyber insurers will tighten requirements:

- ➔ higher premiums
- ➔ stricter audits
- ➔ mandatory segmentation & monitored access

Unmitigated legacy systems become financially unsustainable.

FROM PERIMETER SECURITY TO VENDOR / SUPPLY CHAIN RISK

OT security shifts from "secure the perimeter" to managing vendor and supply chain risk

Third-party technicians, integrators, and external suppliers become the biggest entry point for OT incidents.

Organizations move toward strict vendor governance: session approval, full auditing, and block-by-default remote access.





PIONEERING OT SECURITY SOLUTIONS

**WANT TO STRENGTHEN YOUR OT ENVIRONMENT IN 2026?
LET'S TALK.**