Leaders in many specialized fields secure their operations with TXOne's OT Zero Trust, including 5 of the top 10 pharmaceutical companies, 4 of the top 10 semiconductor fabricators, and 4 of the top 10 aviation companies.

5 Pharmaceutical

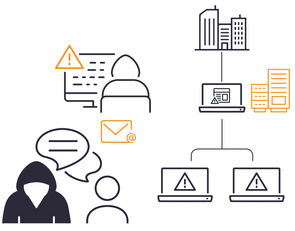
4 Semiconductor Fabrication

4 Aviation

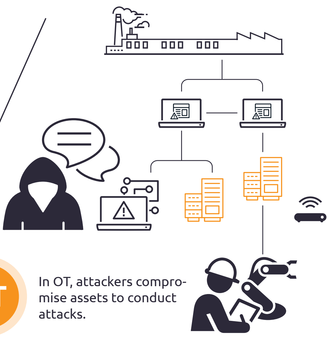
OT Zero Trust

Keep the operation running. Secure assets for high availability.

IT Zero Trust vs. OT Zero Trust



IT In IT, malicious actors compromise user accounts to conduct attacks.



OT In OT, attackers compromise assets to conduct attacks.

Attackers take control of assets by:

- Exploiting unpatched vulnerabilities
- Deploying malware
- Hiding malware in updates or newly-acquired devices

OT Zero Trust stops these behaviors with one simple rule:

Never Trust, Always Verify

The Four Cornerstones of OT Zero Trust

Inspect

Scan all inbound devices brought on site by personnel to stop insider threat, and scan assets before onboarding to prevent supply chain attacks.

90 days

TXOne's threat specialists recommend keeping scan logs for a general minimum of 90 days, and for mission critical assets a minimum of 180 days.

Lock Down

Trust lists secure endpoints and networks alike by specifying what is allowed and blocking everything else.

Segment

Network segmentation groups vulnerable assets into operations-friendly safe zones, preventing attackers from moving and malware from spreading.

80 sec.

Malware can strike as fast as it can appear - after file landing, the REvil ransomware only needs 80 seconds to encrypt a typical Windows system and post a ransom note.

Reinforce

Shield assets at a network level to secure vulnerabilities in legacy and other unpatched assets without interrupting their work.

28.3% Vulnerabilities that OT security experts must address are appearing at a faster and faster rate - 28.3% of all ICS vulnerabilities ever discovered were discovered in 2021.

1,500 organizations affected

It's hard to stop malware when it's hidden in a trustworthy-seeming update from a vendor, as nearly 1500 companies learned in the Kaseya VSA supply chain attack of 2021. With an application trust list, updates can't run on your systems until an administrator has scanned, approved, and scheduled them.

OT-NATIVE

The OT-native IPSes and firewalls that make OT zero trust possible were created with rule sets that repel attacks without disrupting operations. This means no forcing endpoints to conduct an update, no forced system reboots, and most importantly no production downtime. Through network segmentation and asset shielding, engineers can keep assets operational and secure while they test, schedule, and deploy the patch.

Keep the Operation Running with the OT Zero Trust Approach

OT Zero Trust Secures High Availability

IT Zero Trust is based on

#1 Confidentiality #2 Integrity #3 Availability

OT Zero Trust is based on "AIC"

The philosophy of OT zero trust was developed as an answer to the problems traditional cyber defenses create in OT environments. IT cybersecurity uses a priority system called "CIA" - confidentiality first, integrity second, and availability third. OT network security, on the other hand, is based on asset activity so that productivity can always be the highest priority. This requires a different model, "AIC" - availability is #1, integrity is #2, and confidentiality is #3. The OT Zero Trust approach prepares cyber defenses to never make assumptions about credibility and to continually evaluate trust on the network.

OT Zero Trust is based on

OT Zero Trust-based solutions always prioritize availability

txone.com