FACTION NETWORKS

GUIDE

OT & IOT SECURITY

Securing OT & IoT with Faction Networks

Protect the connected devices that VPNs and SDNs cannot — and from compromised routers and smart hardware — with a Zero Trust network created and controlled by you. You can't outsource trust, and now you don't have to.

1 The Unspoken Gap in Cybersecurity

Most security tools are built for computers — devices that run software, accept updates, and can defend themselves. But a growing majority of what's connected to networks today can do none of that.

Operational Technology (OT) runs the physical world: the controllers, sensors, and systems behind manufacturing lines, building systems, clinical equipment, and energy and water infrastructure. The Internet of Things (IoT) adds the cameras, meters, and smart devices multiplying across every site. Many are a decade or more old, were never designed to be secured, can't run an agent, and are rarely — if ever — patched.

Worse, these devices are not only undefended — they can be the attacker. A smart device, or even the router controlling your network, can arrive already compromised: a Trojan horse on the inside, implicitly trusted by everything around it. For a small or mid-sized organization — and for the MSP or MSSP that secures it — that is the soft underbelly of the network, and the stakes are not only data but downtime, safety, and physical operations.

> **The hard truth no one wants to say:** if the routers controlling your network — or smart hardware inside of it — is compromised, then all your Zero Trust security software is worthless.

2 Why Current Architectures Are Insufficient

VPNs and firewalls were Generation 1. Cloud ZTNA and SDN were Generation 2. Each was a genuine advance on what came before — and each left the same blind spot: neither was built for devices that can't run software, or for hardware that arrives already compromised.

Generation 1 — VPNs & Firewalls

Generation 1 was built around the perimeter: trust everything inside, and concentrate on keeping attackers out. Firewalls enforced the boundary and VPNs extended it to remote users. The organizing assumption was simple — **inside means trusted** — and for its era it was reasonable. The migration to the cloud demolished it. Once applications, data, and users moved outside the building, there was no clean inside left to defend, and the weaknesses became structural:

- The gateway is a **visible perimeter** — it can be scanned, probed, and targeted from the open internet.
- Access depends on **credentials** that are routinely phished, stolen, or brute-forced.
- A single compromised credential or misconfigured rule can **expose the entire flat interior** behind it.
- **OT and IoT devices sit unprotected** — they can't run VPN agents and remain exposed on the local network.

Generation 2 — Cloud ZTNA & SDN

Generation 2 recognized that the perimeter had dissolved. ZTNA and SDN were built specifically to fix the VPN's flaws — eliminating implicit interior trust and enforcing continuous, identity-based verification. **"Never trust, always verify"** replaced "inside means trusted," and for cloud-first applications it was a necessary step forward. But for most organizations it trades one set of problems for another:

- It relies on **centralized cloud control planes** — servers, certificate authorities, and identity providers become high-value targets, and a breach of the vendor's infrastructure is a breach of every customer on it.
- It is **expensive and complex**, typically priced and staffed for large-enterprise budgets.
- It is **software-only**, and cannot protect OT and IoT devices that can't run agents.
- It creates **metadata exposure** — the provider can observe connection patterns, timing, and topology even when payloads are encrypted.

They leave three gaps

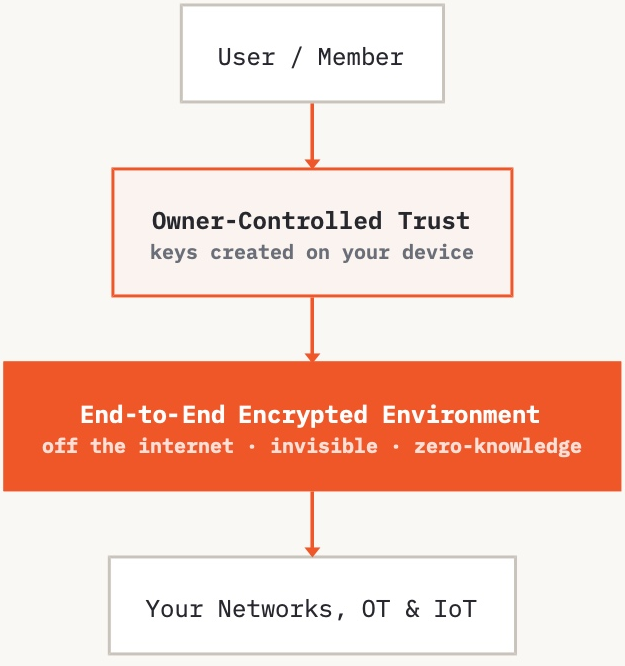
First, SDNs and VPNs depend on their cloud infrastructure to protect yours — and the Cloud is fundamentally indefensible. Second, agentless OT & IoT machines and devices are visible to attackers but outside the scope of these security tools. Finally, and worst, they completely ignore the vulnerability and compromise of routers and smart hardware — the Trojan horse deployed all across our networking infrastructure.

3 Generation 3: Owner-Controlled Trust

Generation 3 extends Zero Trust beyond users and applications to the things current architectures leave exposed — your infrastructure, your OT and IoT devices, your data. More fundamentally, it changes *who holds trust*.

Instead of centralizing trust in a vendor's cloud control plane, Generation 3 returns it to the owner. You create and control your own trust relationships and encryption keys, and Faction routes your encrypted traffic without the ability to read it. For an agentless camera, controller, or sensor, this is the secure place to live it never had — an owner-controlled, invisible network it can attach to without running any software of its own. Its defining properties:

- **Owner-controlled trust** — encryption keys and network identity are created on your device and never stored on Faction's infrastructure. There is no master key, and no vendor holds trust on your behalf.
- **Zero Knowledge Architecture** — the data plane is owner-keyed, so Faction routes your traffic but cannot read it. There is no decryptable content to be compelled or breached for.
- **Invisible by default** — no discoverable gateway, port, or attack surface to scan from the internet, and the OT and IoT devices behind it inherit that same invisibility.
- **Zero Trust for hardware** — we cyber-assure our own hardware and never trust yours; a compromised router or smart device can't reach the network or the internet.



Faction Network

TRUST HELD BY THE OWNER.

Identity and keys originate on the Network Owner's device — distributed only to authorized members through the Faction network. Faction relays encrypted traffic it can never read — the foundation every device attaches to.

GENERATION 3 · CONTINUED

Core Capabilities

Every Faction deployment is built on our Generation 3 foundation that delivers owner-controlled trust by architectural design, not policy.

CAPABILITY	WHAT IT MEANS FOR YOU
Owner-controlled keys	Keys are generated on your device and never stored on Faction's infrastructure. There is no master key.
Invisible by default	Your network can't be discovered, scanned, or probed from the internet. No gateway, no attack surface.
Zero-knowledge infrastructure	Faction routes your encrypted traffic but cannot read it — technically incapable, not just policy-bound.
Cryptographic identity	Every device and user is verified before any access. No passwords to phish or steal.
No anonymous	Every device and IP address is signed with a certificate from the network owner — obfuscation and evasion are impossible.
Two-level human identity	Assure not just what is on your network, but who — biometric 5FA powered by iValt.
Hardware-native OT/IoT	Pods and Portals protect any connected device regardless of age or capability.
Micro-segmentation	Isolate device groups so a problem in one never spreads to the rest.
Made-safe-in-USA hardware	Built in the USA and Cyber Assured, with Independent Cyber Lab inspection and chip-level forensic verification.
Ongoing monitoring	Cyber integrity of network and hardware continuously verified.

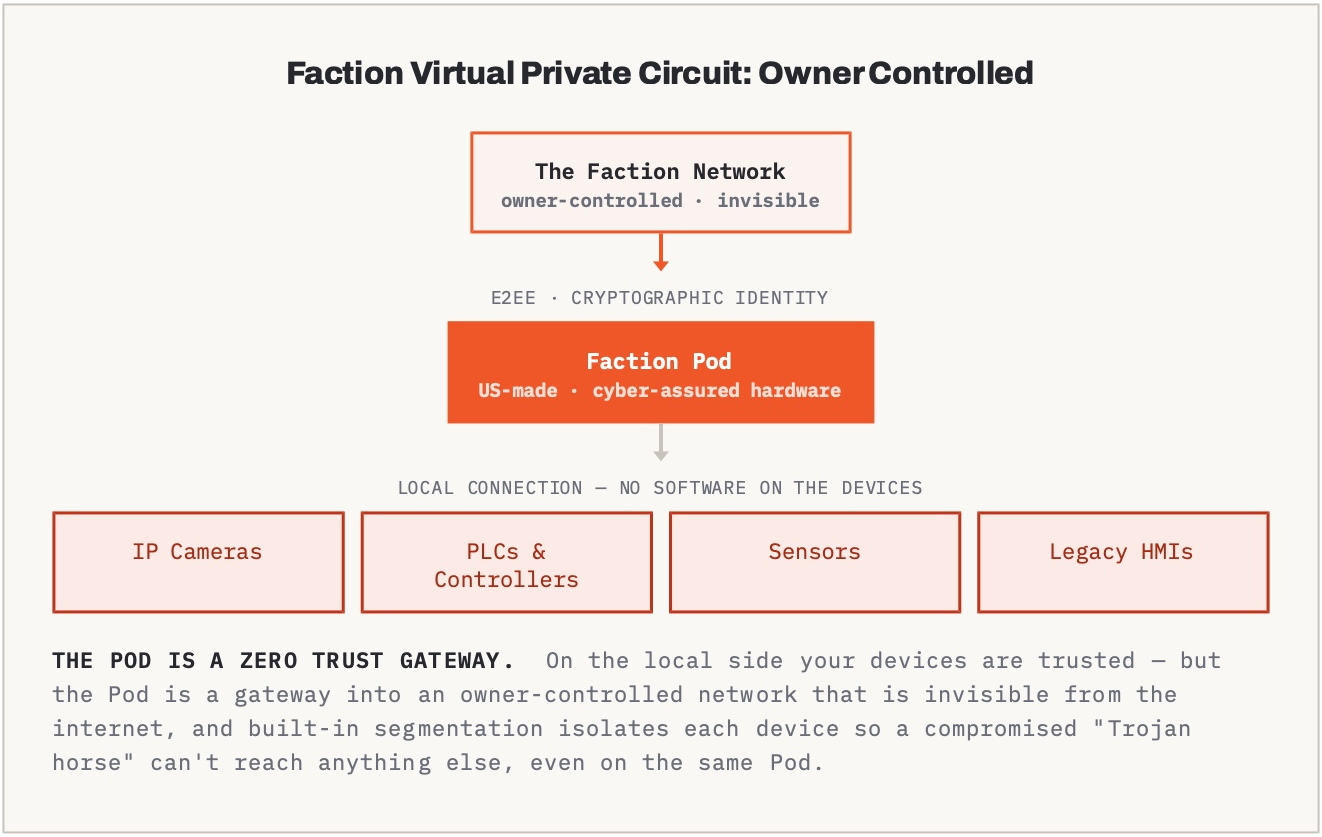
Built for lean teams — low cost and simple to run. The same architecture that protects critical infrastructure deploys without a large IT or security team, and stays manageable by the MSP that serves it.

4 Pods & Portals: Zero Trust for OT & IoT

A Faction Pod is a simple secure networking appliance that is "adopted" into a Faction Network with a simple scan-and-click process — think of it like a Yubikey for your networking. The encryption key is provisioned to the Pod during adoption, and only YOU ever have knowledge of or access to that key, the Faction Network, and the Pod.

The Pod authenticates to the owner with cryptographic identity and, once adopted, cannot be silently moved to another network — only an owner-initiated factory reset returns it to the adoption pool. The OT and IoT devices simply connect to the Pod over the local connection they already use — no agent, no software, no updates, no capability required of the device itself. Everything beyond the Pod is encrypted and owner-controlled. Portals extend the same model to an entire site, bringing a location's devices onto the network at once.

- **Any device, any age** — legacy equipment, IP cameras, industrial sensors, and controllers are all protected regardless of operating system or capability.
- **Hardware-native, US-made** — cyber-assured hardware, supply chain inspected, with independent cyber-lab and chip-level forensic verification.
- **Nothing exposed** — devices behind a Pod inherit the network's invisibility; there is no gateway to scan.



5 Use Cases and Verticals

If it connects to a network, Faction can bring it under owner-controlled trust — across the environments where OT and IoT carry the most risk.

WHAT YOU CAN PROTECT

Industrial control

PLCs, controllers, HMIs, and SCADA endpoints.

Physical security

IP cameras, access control, and building systems.

Sensors & instrumentation

Environmental, industrial, and metering devices.

Legacy & clinical equipment

Older workstations and connected medical devices.

WHERE IT MATTERS MOST

Manufacturing

Robots, PLCs, and HMIs where uptime and safety are non-negotiable.

Healthcare

Connected clinical and imaging devices that can't be patched but must stay protected.

Defense Industrial Base

Suppliers under CMMC and supply-chain scrutiny.

Energy & Critical Infrastructure

SCADA, meters, and remote sites across a wide footprint.

Smart Agriculture

Sensors, controllers, and equipment across remote, unmanned sites.

Smart Cities

Cameras, traffic, and environmental systems in public infrastructure.

WHY YOU SHOULD ACT NOW

Threat environment

Nation-state and ransomware actors increasingly target OT, IoT, and the hardware supply chain — not just users and apps.

Regulatory drivers

CMMC Level 2, sector mandates, and audits increasingly require device-level segmentation and control.

Financial drivers

Cyber-insurance eligibility and premiums increasingly hinge on demonstrable OT/IoT segmentation and controls.

6 Getting Started

You can secure OT and IoT in your owner-controlled Faction Network in days or weeks, not months. No rip-and-replace of existing networking equipment, no software agents to install, no firewalls to configure and maintain. Most importantly of all, no having to trust cloud infrastructure, platforms, and broken promises.

1. **Map what's exposed**
   Inventory the agentless, legacy, OT, and IoT devices sitting unprotected on your networks.
2. **Prioritize**
   Identify the machines and devices most critical to your business.
3. **Stand up a Faction Network**
   Create an owner-controlled, invisible network — keys generated on your device, in minutes.
4. **Deploy Pods & Portals**
   QR-code scan and click. Zero configuration, no change to the devices themselves.
5. **Segment and manage**
   Isolate device groups; manage every site and device from one place with zero cloud exposure.
6. **Connect with control**
   Use our Cloud Connectors to let devices reach required cloud resources — always with security, visibility, and control.

FACTION POD

FACTION PORTAL

Secure Your OT & IoT With Keys Only You Control

We would welcome the chance to show you how Faction puts you in control and secures your critical machines and devices rapidly, with low cost and IT overhead.

FACTION NETWORKS

GET EARLY ACCESS

MSP / MSSP PROGRAM