FACTION NETWORKS

PUBLIC DISTRIBUTION

GUIDE · GENERATION 3 ZERO TRUST

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.

CONTROL. PEACE OF MIND.

Faction Networks
Generation 3 Zero Trust

Published 2026
Revision 1.0

factionnetworks.com
Made in the USA

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 — and each left the same blind spot: none was built for devices that can't run software, or for hardware that arrives already compromised.

Generation 1 — VPNs & firewalls

Protect a perimeter. Once a device is inside, it is implicitly trusted — and the agentless camera or controller on the local network sits fully exposed to anything else that gets in. Firewalls themselves are riddled with vulnerabilities and plagued with configuration errors.

Generation 2 — SDN & software ZTNA

Verifies identity well, but requires an agent installed on the device — and the devices that most need protection are precisely the ones that can't run one. It also does nothing about a compromised router or a smart device that arrives as a Trojan horse inside the network; that hardware is simply trusted and never inspected.

Both leave critical 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.

THE OT & IOT GAP

3 Securing the Foundation

For an agentless device to be protected, it needs a secure place to live. That is the Faction Network — an owner-controlled, invisible, zero-knowledge private network. You don't need a firewall or an agent because they have been moved OFF the internet into a cryptographically isolated environment that only you can access.

Owner-controlled trust

Encryption keys and network identity are created on the owner's device and never transmitted to or stored on Faction's infrastructure. The owner — not a vendor — holds trust.

Invisible by default

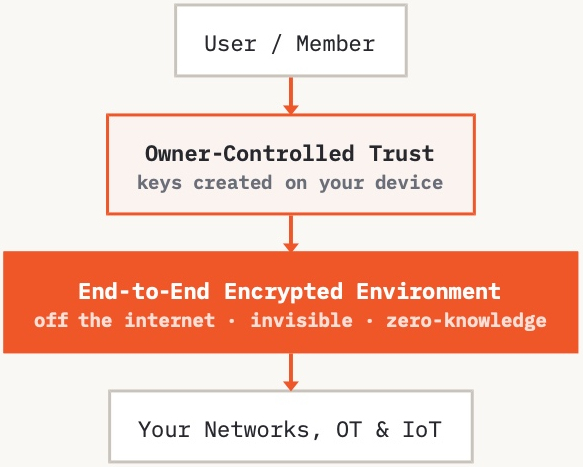
The network cannot be discovered, scanned, or probed from the internet. There is no visible gateway and no attack surface; unauthorized parties cannot even attempt a connection.

Zero Trust for hardware

We cyber-assure our own hardware — and we never trust yours. A compromised router or smart device can't reach the network or the internet, because everything has been moved into an isolated environment only you control.

Zero Knowledge

Faction routes your encrypted traffic but cannot read it — technically incapable, not merely bound by policy. With no keys and no decryptable content on our infrastructure, there is nothing to compel, leak, or breach.



Faction Network

TRUST HELD BY THE OWNER.

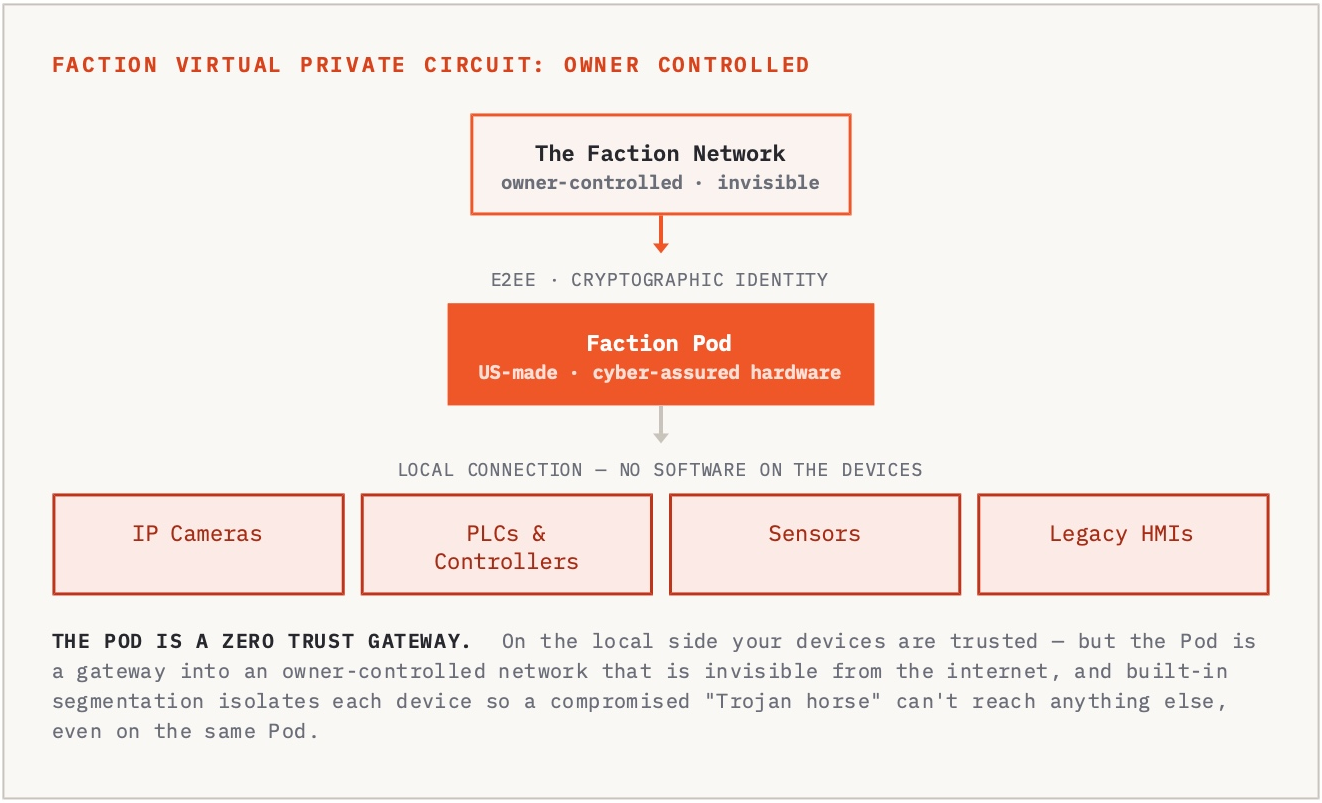
Identity and keys originate on your device and never leave it. Faction relays encrypted traffic it can never read — the foundation every device attaches to.

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 Pod gets your encryption key in a direct, out-of-band transmission. Only YOU have knowledge or access to that key, the Faction Network, and the Pod.

The Pod authenticates to the owner with cryptographic identity and, once adopted, can never be joined to another network. 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.



THE POD IS A ZERO TRUST GATEWAY. On the local side your devices are trusted — but the Pod is a gateway into an owner-controlled network that is invisible from the internet, and built-in segmentation isolates each device so a compromised "Trojan horse" can't reach anything else, even on the same Pod.

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 NOW — THE DRIVERS

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 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.

7 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

Take control and get peace of mind

Faction delivers Generation 3 Zero Trust for OT and IoT: owner-controlled, invisible, hardware-embedded. Our Zero Knowledge architecture ensures that you stay in control.

FACTION NETWORKS

CONTACT US

SCAN HERE

info@factionnetworks.com
o. (680) 778-8702