FACTION NETWORKS

WHITE PAPER

HARDWARE TRUST

Hardware Trust & Supply Chain Security

Software-only Zero Trust leaves hardware unexamined. Why the trust assumption must extend to the physical layer — and what Faction does about it.

Faction Networks
Generation 3 Zero Trust

June 2026
Revision 1.0

factionnetworks.com

1 The Hardware Trust Assumption

Zero Trust has always been understood as a software problem. Verify every user. Verify every device. Enforce policy at the application layer. Trust nothing implicitly.

But Zero Trust architectures have a blind spot: they typically trust the hardware they run on.

When an organization deploys a router, a switch, or an IoT device, it generally assumes the hardware does what it claims to do and nothing else. The firmware is presumed to be what the manufacturer shipped. The chips are presumed to be unmodified. The supply chain is presumed intact.

These assumptions are no longer safe to make. The risk has two faces. The first is the network gear itself — the routers, switches, and access points that move every packet. The second is the **Trojan horse**: vulnerable or compromised smart hardware — cameras, sensors, building controls, printers, network-attached storage — placed inside an otherwise secure network, where it is trusted implicitly the moment it is connected. Either can arrive already compromised at the firmware or chip level, carrying a backdoor that survives patching, reimaging, and conventional inspection.

> **The hard truth:** if the routers that move your traffic — or the smart hardware sitting inside your network — are compromised, the Zero Trust software running above them is worth very little. The attacker is already inside, wearing trusted hardware as a disguise.

The hardware already inside ordinary networks — offices, factories, hospitals, substations — may already be compromised. And most Zero Trust architectures have nothing to say about that.

Targeting Goes Far Beyond Critical Infrastructure

The instinct is to treat hardware supply chain security as a concern only for defense contractors and major operators of critical infrastructure. It is not. The same foreign-manufactured routers flagged by the FCC are present in ordinary offices, SMB networks, schools, and healthcare facilities. The threat is not targeted — it is pervasive. Any organization running routers, networking gear and smart hardware that is manufactured or has key components made in China or nations within its sphere of espionage is operating with an unexamined and dubious trust assumption at the physical layer of its network.

2 The Threat Is Documented

This is not theoretical. The U.S. government, the intelligence community, and independent researchers have documented the threat at every level — from the routers on the FCC's Covered List to nation-state campaigns living inside ordinary network hardware.

> **FCC ROUTER MANDATE · COVERED LIST**
>
> The Federal Communications Commission has determined that equipment from certain foreign manufacturers poses an unacceptable national-security risk, placing it on the Covered List and moving to prohibit its use in U.S. networks. The same devices are already installed across ordinary offices, SMB networks, schools, and healthcare facilities.

> **ROB JOYCE · FORMER NSA DIRECTOR OF CYBERSECURITY · HOUSE SELECT COMMITTEE ON THE CCP, MARCH 2025**
>
> Joyce testified that PRC state hackers have *"prepositioned malware within our power grids, pipelines, water treatment plants, and other critical infrastructure,"* and that one foreign router maker — now holding the majority of the U.S. retail Wi-Fi market — had devices *"among the various brands exploited"* in the Volt, Flax, and Salt Typhoon campaigns. His recommendation was blunt: eliminate that footprint.

Volt, Salt, and Flax Typhoon

These campaigns are documented by CISA, the FBI, and the NSA. Volt Typhoon pre-positioned inside U.S. critical-infrastructure networks, living off the land to evade detection. Salt Typhoon penetrated major U.S. telecommunications carriers. Flax Typhoon assembled a botnet from compromised IoT and small-office routers. In each, the foothold was trusted network hardware — the layer software Zero Trust leaves unexamined.

3 What Hardware Trust Requires

Addressing hardware trust requires going deeper than software. It requires independent verification at every layer of the physical stack — from the chip to the supply chain to ongoing field monitoring.

1. **Chip-level forensic inspection**
   Physical analysis — chip-off and motherboard examination — to verify components are what they claim to be and have not been tampered with in manufacturing or transit.

2. **Supply chain verification**
   Independent tracing of every component from manufacture through delivery, with certification that the chain of custody is intact.

3. **Source code review**
   Independent review of firmware and embedded software to verify it matches the claimed specification and contains no undisclosed functions.

4. **Protocol analysis**
   Examination of the device's network behavior to confirm it communicates only as advertised and does not exfiltrate data or accept unauthorized commands.

5. **Red-team OT/IoT testing**
   Adversarial testing in operational environments to identify vulnerabilities that conventional testing misses.

6. **Ongoing monitoring**
   Continuous verification after deployment — hardware integrity is not a one-time question.

4 Cyber-Assured & Made-Safe in the USA

Faction addresses hardware trust at two moments: at the source, before a device is ever deployed — and continuously, for as long as it operates in your network. Pods and Portals are independently certified, then independently and continuously verified.

Certified at the source — ORION

Faction's Pods and Portals are certified through ORION's Cyber-Assured and Made-Safe in the USA programs, which apply the disciplines above: chip-off and motherboard forensics, supply-chain tracing from manufacture through delivery, independent source-code review, protocol analysis, and OT/IoT red-team lab testing — independent confirmation that the device is what it claims to be before it carries a single packet.

Verified continuously in the field — OSec

Certification is a starting point, not a finish line. Through a partnership with OSec — an offensive-security firm whose Incenter platform continuously tests millions of systems, applications, and endpoints — Faction extends hardware trust into ongoing operation:

- **External verification**
  Incenter continuously tests that the devices and users behind your Pods and Portals remain invisible and unreachable from the public Internet — confirmed, not assumed.
- **Vulnerability assurance**
  Ongoing, AI-assisted research against Faction's platform and its components — such as OpenWRT and WireGuard — surfaces new vulnerabilities so they can be remediated, wherever possible before they ever become public.
- **Owner-controlled verification**
  A secure channel Faction itself cannot access lets you independently confirm the inventory of users and devices you protect, and alerts you to new exposure — preserving the zero-knowledge principle even in monitoring.

Cyber-Assured · ORION	Supply Chain Verified · ORION	Continuously Monitored · OSec
Source-code review, protocol analysis, and OT/IoT red-team lab testing confirm the device is what it claims to be.	Every component traced from manufacture through delivery via chip-off and motherboard forensic analysis.	Hardware and network integrity verified on an ongoing basis after deployment — assurance does not stop at certification.

5 Supply Chain Security & Sovereignty

Verifying and containing the hardware in front of you treats the symptom. The deeper exposure is the supply chain beneath it — the silicon, firmware, and manufacturing that no buyer can see and few can control, and that federal action has not yet reached.

The FCC's 2026 ban on foreign-made routers was a necessary step, but it addressed the finished good while leaving the silicon supply chain untouched. The CHIPS Act mobilized advanced semiconductors for AI and defense, yet skipped the commodity components — memory, microcontrollers, wireless chipsets — in every router, camera, OT controller, and drone. Regulation has reached the device level and stopped at the component level.

> **You cannot outsource trust.** Control of the means of production — the fab, the firmware-signing environment, the manufacturing floor — is a prerequisite for provable end-to-end security. Manufacturing in the United States is necessary but not sufficient; cyber assurance — the continuous, independent verification of hardware from silicon to software — is the standard that must be required.

This is, ultimately, a question of sovereignty. Most networking and smart hardware depends on silicon from China, Taiwan, and the South China Sea corridor. A confrontation over Taiwan would not merely risk cyber disruption — it would sever the supply of chips and devices that government, military, and critical infrastructure depend on. The South China Sea is the digital Strait of Hormuz.

Unlike rare-earth minerals, this problem is tractable — the capability already exists in American industry and among close allies. Chip designers such as Qualcomm design the components; US fabricators such as GlobalFoundries and Micron can produce the commodity silicon networking hardware requires; the GO SEMI Alliance and CHIPS Act already have a mandate for domestic packaging; and US contract manufacturers and ODMs are widespread. What is missing is not capability but coordination, incentives, and procurement requirements. Faction has mapped a three-phase roadmap to 100% US-manufactured, cyber-assured networking hardware:

Phase 1 · 2026 — US Cyber-Assured	Phase 2 · 2027 — US-Manufactured & Sovereign Supply Chain	Phase 3 · 2028 — Zero Trust to Silicon
Forensic inspection of every component, cyber-assurance validation (ORION, AIS), and security-by-design: secure boot, signed firmware, device identity.	Key components shifted to US sources under audited controls — traceability, tamper controls, and chain-of-custody (Z-Axis and others).	Zero Trust embedded at the silicon level, quantum-validation readiness, and a full sovereign supply chain verified end-to-end.

6 Containing the Threat Already Inside

Foreign-made hardware flagged by the FCC — and the compromised smart devices already operating beside it — cannot be ripped out and replaced overnight. There is too much of it, in too many networks, on budgets never built for a wholesale refresh. The real question is not how fast you can replace it, but how fast you can contain it.

For the highest-risk systems, replacement remains the right answer over time. But a full hardware swap is slow, costly, and disruptive — and it does nothing for the months or years in between. A credible strategy has to contain the threat that is already inside while trusted hardware is phased in on a realistic timeline and budget.

This is where Faction is built to act — rapidly and at low cost. Pods and Portals do not replace your routers; they sit behind your existing infrastructure and contain the threat. Anything connected behind them is placed inside an owner-controlled network that is invisible and unreachable from the public Internet, with every packet encrypted under keys only you control. A compromised router or smart device can no longer reach, observe, or exfiltrate the traffic that matters — its ability to do harm is mitigated without changing a single piece of existing hardware, and OSec's continuous monitoring verifies that it stays that way. Faction's *Securing OT & IoT* and *Virtual Private Circuit* guides detail how this is deployed.

The lesson of every supply chain attack is the same: trust cannot be assumed at any layer of the stack. Software Zero Trust is necessary but not sufficient — the hardware it runs on must be verified at the source and contained in the field. Faction's Cyber-Assured Pods and Portals, certified by ORION and monitored by OSec, bring that discipline to the physical layer and let you act on the threat already inside your network now — not after the next budget cycle.