FACTION NETWORKS

WHITE PAPER

PUBLIC DISTRIBUTION

The Next Generation of Zero Trust

How network security has evolved from perimeter defense to cloud-centralized identity — and why the next generation of owner-controlled trust is required to meet the challenges of the new era.

Faction Networks
Generation 3 Zero Trust

May 2026
Revision 1.0

factionnetworks.com

1 Executive Summary

Every major evolution in cybersecurity has followed a shift in infrastructure. Generation 1 protected trusted internal networks with firewalls and VPNs. Generation 2 recognized that the perimeter had dissolved and centralized trust in cloud-managed control planes. Both were genuine advances in their time.

Neither was designed for the environment organizations operate in today — one where infrastructure, devices, supply chains, and AI systems all influence security outcomes, and where the very platforms that manage trust have themselves become high-value targets.

This paper traces that evolution and introduces **Generation 3 Zero Trust**: a model in which organizations own and control the trust relationships that govern their networks, devices, data, and AI. The shift is not simply stronger authentication. It is ownership and control of trust itself.

> **Control. Peace of Mind.** Security built so trust is owned and controlled by you — delivered and verified by architecture, not promised by policy.

2 Why Trust Models Are Breaking Down

Modern organizations operate in environments where users, devices, infrastructure, supply chains, and AI systems all influence security outcomes. The challenge is no longer simply keeping attackers out. The challenge is maintaining control.

Cyber Criminal & Nation-State Threats

Criminal and nation-state actors increasingly target infrastructure, devices, and supply chains — not only users and applications. Security must extend beyond traditional perimeter and endpoint models.

AI Disruption

Organizations are deploying AI systems faster than governance frameworks are evolving. Identity, authorization, and accountability become critical as AI assumes greater operational responsibility. At the same time, AI is being leveraged by bad actors to exponentially increase their capabilities to discover and exploit vulnerabilities.

Hardware & Supply Chain Exposure

Trust assumptions now extend beyond software into manufacturing, sourcing, and connected devices. Organizations need visibility into the trust relationships that underpin their environments.

OT & IoT Expansion

Industrial systems, medical devices, sensors, cameras, and connected infrastructure keep expanding the attack surface while operating outside traditional endpoint security models.

3 Generation 1: VPNs & Firewalls

Generation 1 was built around the perimeter. Organizations trusted everything inside the network and concentrated on keeping attackers out. Firewalls enforced a boundary; VPNs extended it to remote users.

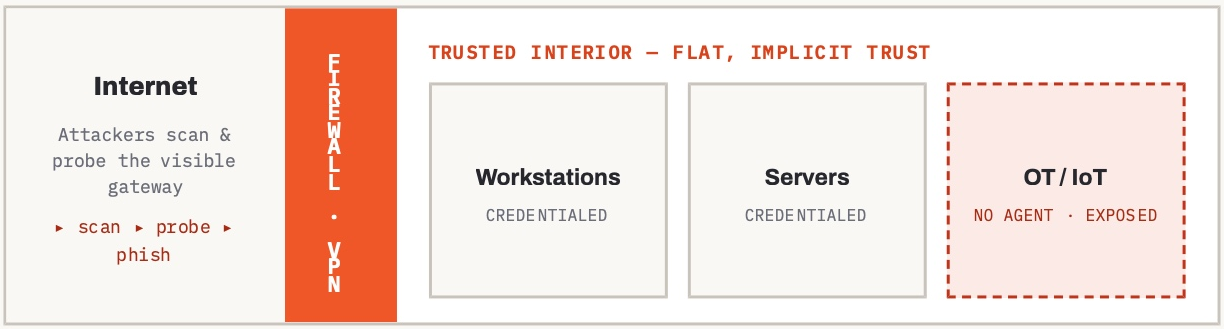
The model worked when users, devices, and applications largely operated inside a single controlled environment. Its organizing assumption was simple — **inside means trusted** — and for its era, that assumption was reasonable.

But the explosive evolution and migration to the cloud demolished that assumption. As applications, data, and users moved outside the building, the perimeter dissolved — there was no longer a clean inside to defend or a single edge to guard. The model's deepest weaknesses became structural:

- The gateway is a **visible perimeter** that attackers can scan, probe, and target from the open internet.
- Access depends on **credentials** — usernames and passwords that are routinely phished, stolen, or brute-forced.
- A single compromised credential or misconfigured rule can **expose the entire network** behind it.
- **OT and IoT devices sit unprotected** — they cannot run VPN agents and remain exposed on the local network.

Perimeter-based architecture had become incurably vulnerable in a cloud-connected world — which is precisely what drove the development of Zero Trust. Yet VPNs and firewalls remain the most widely used security tools for small and mid-sized organizations today.

FIGURE 1 · THE PERIMETER MODEL



THE FLAW IS STRUCTURAL. One breach of the gateway — or one phished credential — exposes a flat interior where everything is implicitly trusted, and devices that can't run agents go unprotected.

4 Generation 2: Cloud ZTNA & SDN

Generation 2 recognized that the perimeter had dissolved. Zero Trust Network Access (ZTNA) and Software-Defined Networking (SDN) were developed specifically to address the vulnerabilities of VPNs, and they represent a genuine advance.

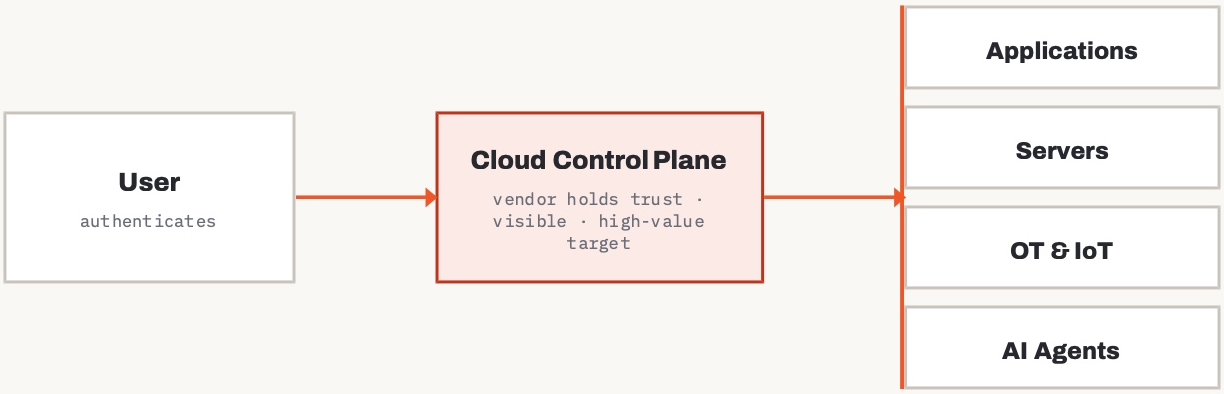
Enterprise platforms — Zscaler, Fortinet, Palo Alto Networks and others — eliminated perimeter-based trust, enforced continuous authentication tied to identity verification, and enabled fine-grained access control. "Never trust, always verify" replaced implicit interior trust, and for cloud-first applications it was a necessary step forward.

But for the majority of organizations, Generation 2 trades one set of problems for another. Its advances are real; so is the new dependency it creates:

- It relies on **centralized cloud control planes.** Servers, certificate authorities, and identity providers become high-value targets — a compromise of the vendor's infrastructure is a compromise of every customer on the platform.
- 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** — cloud providers can observe connection patterns, timing, and topology even when payload content is encrypted.

Trust still rests with a third party — now the cloud provider rather than the network perimeter. The organization verifies more, but it controls less and outsources trust entirely.

FIGURE 2 · CLOUD ZTNA — TRUST BROKERED BY THE VENDOR



TRUST MOVES TO THE CLOUD. Every connection is brokered through a control plane the vendor owns and operates — a single, visible point of dependency and a high-value target shared across every customer.

5 Generation 3: Owner-Controlled Trust

Generation 3 extends Zero Trust beyond users and applications to include infrastructure, OT/IoT devices, data, and AI-enabled operations. More fundamentally, it changes *who holds trust*.

Instead of centralizing trust in a vendor's control plane, Generation 3 returns it to the owner. The organization creates and controls its own trust relationships and encryption keys, and the platform routes encrypted traffic without the ability to read it. Its defining properties:

- **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. *Faction can't see what you protect.*
- **Owner-controlled trust** — keys and trust relationships are created and governed by the organization, not the vendor.
- **No Anonymous.** Every device authenticates with a certificate from the network owner — no anonymous or unsigned connections are accepted.
- **Invisible by default** — no discoverable gateway, port, or attack surface to scan from the internet.
- **Hardware-native protection** — Pods and Portals extend Zero Trust to OT and IoT devices that cannot run software agents.
- **Identity-bound AI governance** — every agent is cryptographically bound to a verified identity and accountable beneath the application layer.

Together these properties remove the weaknesses of the first two generations: no perimeter to breach, no control plane to compromise, and no anonymous foothold inside.

FIGURE 3 · FACTION — TRUST HELD BY THE OWNER

TRUST CONTROLLED BY YOU, NOT BY US. The owner possesses the encryption keys for the Faction data plane. Faction does not and therefore cannot yield access to your network's traffic.

6 Three Generations at a Glance

Each generation of network security is defined by one question: where does trust live? Here is how Faction's owner-controlled model contrasts with — and closes the structural gaps of — the two generations that came before it.

Generation 1 placed trust in the perimeter and proved architecturally vulnerable once the cloud dissolved the perimeter entirely. Generation 2 moved trust to a cloud control plane — a real advance, but one that made the vendor's infrastructure a single high-value target shared across every customer. Generation 3 removes the dependency altogether: a zero-knowledge architecture that routes encrypted traffic but cannot read it, with keys and trust held only by the owner. Seen side by side, the trajectory is clear — from defending a boundary, to verifying identity, to owning trust.

	GEN 1 — VPNS & FIREWALLS	GEN 2 — CLOUD ZTNA / SDN	GEN 3 — FACTION
Architecture	Perimeter gateway	Cloud control plane	Zero Knowledge, no control plane
Network visibility	Exposed, scannable	Cloud broker visible	Invisible by default
Authentication	Credentials (phishable)	Cloud IAM + 2FA	Out-of-band cryptographic key
OT / IoT devices	Unprotected	Software only	Pods, Portals, Modules
AI agent control	None	Cloud IAM (vulnerable)	Identity-bound governance
Data encryption	In transit only	In transit only	In transit and at rest
Cloud Vulnerability	High	Better, but still centralized	Zero — owner holds the keys

> The next evolution of Zero Trust is not simply stronger authentication. **It is ownership and control of trust itself.**

7 What Generation 3 Means in Practice

One platform applies owner-controlled trust across the four domains where modern organizations carry the most risk.

Networking

Secure networking built around owner-controlled trust and reduced dependence on centralized control infrastructure. The network is invisible from the internet and reachable only from inside.

OT & IoT

Protection for the devices traditional, software-only models struggle to secure — extended through Pods, Portals, and embedded capabilities regardless of operating system, age, or capability.

Data

Encryption and trust governed by the organization rather than third-party vendors. Data is protected in transit and at rest, with keys that never leave the owner's devices.

AI

Identity-bound governance, accountability, and policy enforcement for AI-enabled operations — every agent cryptographically bound to a verified human identity.

How it works

- **Deploy alongside or *Factionize* existing infrastructure.** No rip-and-replace.
- **Create owner-controlled trust.** Trust relationships and encryption keys originate with the organization, not the vendor.
- **Authenticate with cryptographic identity.** Users and devices are verified out-of-band, impervious to phishing and credential theft.
- **Extend protection to OT & IoT.** Reach the devices software-only models can't, using Pods, Portals, and embedded capabilities.
- **Keep operating on your terms.** Trust does not depend on a vendor's cloud staying available.
- **Human Identity Verification and Authorization.** When needed, escalate to native device biometrics or iValt 5-Factor Verification to keep a human in the loop — confirming a responsible person authorized the access or action, and remains accountable for it. Especially important for AI agents.

8 The Inflection Point

Each generation of security solved the problem its era presented. Generation 3 answers a question the first two could not.

Not *how do we keep attackers out*, or *how do we verify identity*, but **who controls trust.** For modern infrastructure, the answer must be the owner. When trust is owned and controlled by the organization, security stops depending on the integrity of a third party — and becomes an architectural property rather than a vendor policy.

This is also why the shift is durable. A Generation 2 platform cannot simply adopt owner-controlled trust without dismantling the centralized control plane its business depends on. Generation 3 is not a feature added to the previous model — it is a different architecture, built from the cryptographic identity and zero-knowledge foundations up. For the organization, the practical consequence is straightforward: less dependence on actors you cannot verify, a smaller attack surface, and protection that finally extends to the networks, data, OT, IoT, and AI systems that earlier generations left exposed — with human-in-the-loop control, authorization, and accountability enforced where actions carry real risk.

That is the shift Generation 3 represents, and the foundation Faction is built on.

> **The question is no longer whether you can keep attackers out, or verify who is inside. It is whether you own and control the trust your organization runs on.**