DATA SHEET · GENERATION 3 ZERO TRUST

FACTION NETWORKS × iVALT

HUMAN IDENTITY

Human Identity with iVALT + Faction

PROVABLE HUMAN AUTHORITY FOR EVERY ACTION

Zero Trust secures connections — it verifies that an approved device reached an approved resource over an approved path. What it cannot verify is that a trusted human is actually behind the action. **Faction and iVALT close that gap.** The integration adds passwordless, biometric, AI-resistant human identity verification to a Generation 3 Zero Trust network — securing every action, not just every connection.

WHAT IT IS

Faction + iVALT integrates iVALT's passwordless, biometric Digital Trust platform directly into Faction's owner-controlled Generation 3 Zero Trust architecture. The result is a complete human identity layer: it establishes not just that an approved device connected, but that **provable human authority — or an AI agent acting under one — stands behind every action.**

iVALT authentication is accessible only through Faction — not from the public internet — so there is no internet-facing identity service to attack. Human identity verification is **in implementation and ships in the v1 launch**; identity-bound governance for AI agents is on the roadmap.

WHY IT'S DIFFERENT

Most identity systems verify a **credential, not a person** — and credentials are the most exploited attack vector in cybersecurity. Passwords are phished, tokens are stolen, MFA codes are intercepted, and AI deepfakes now defeat visual and voice checks.

iVALT's **Human-Bound Identity™** delivers provable human authority before execution — with a single tap. There is no shared secret to phish, replay, or hand to an AI agent. And because cloud IAM and hosted Certificate Authorities are themselves internet-exposed targets, securing all connectivity and communications for iVALT authentication through a Faction Network removes that entire class of vulnerability.

HOW IT WORKS

CORE CAPABILITIES

- **Provable human authority** — human-bound authority verified before execution, not just a credential presented.
- **Passwordless & AI-resistant** — biometrics bound to device PKI; no shared password or token to steal.
- **Cryptographic, real-time human-in-the-loop** — step-up that re-verifies the person, not a stolen credential or hijacked token.
- **Presence verified at authorization** — confirmed at the moment of approval, then cryptographically maintained — not assumed from a session.
- **Not internet-accessible** — iVALT authentication is reachable only through Faction; no internet-facing identity service to attack.
- **Step-up only when it matters** — verification fires at the thresholds you define; invisible when not needed, enforced when it is.
- **Signed & auditable** — every action tied to this person, this action, this moment — a tamper-evident record.
- **No rip-and-replace** — deploys as a layer on your Generation 3 Zero Trust network, alongside existing infrastructure.

HUMAN-IN-THE-LOOP VERIFICATION

At defined risk thresholds, the combined system steps up to confirm provable human authority before execution. At its core are **biometrics bound to device PKI** — the cryptographic proof of the responsible human — with **contextual attributes such as GPS and time** layered on to further reduce the attack surface.

HUMAN-BOUND IDENTITY™ (FACTORS) — VERIFIED WITH ONE TAP ON YOUR MOBILE PHONE

WHAT EACH STEP-UP CONFIRMS

- **Verified human presence** — a live person, not a bot or a replayed credential.
- **Re-verified at approval** — presence confirmed at authorization, closing the session-hijacking gap.
- **Per-action authorization** — this specific action, not a carried-forward session.
- **Signed & auditable** — tied to this person, this action, this moment.

WHERE STEP-UP APPLIES

You decide where a verified human is required. Administrators define step-up policy from a central dashboard — and can invoke it from a policy rule, an execution checkpoint, or a simple API call. **Optional presets map common risk profiles to recommended thresholds**, so teams start from a sensible baseline and tune from there. When a qualifying action occurs, iVALT's patented Loop Back redirects it to the responsible person, who must authorize it before it can proceed.

Baseline EVERYDAY

Step-up reserved for privileged and administrative access and irreversible operations.

Elevated SENSITIVE · REGULATED

Adds sensitive-data access, configuration changes, and high-value transactions.

Maximum CROWN-JEWEL

Every action you designate high-risk requires a present, verified human before it runs.

Common triggers organizations configure for step-up:

PRIVILEGED & ADMIN ACCESS | IRREVERSIBLE OPERATIONS | HIGH-VALUE TRANSACTIONS | SENSITIVE DATA ACCESS | WIRE & PAYMENT AUTHORIZATION | THIRD-PARTY APPROVALS | AI AGENT GOVERNANCE | INCIDENT RESPONSE & RECOVERY | MULTI-PARTY APPROVAL WORKFLOWS

Because verification is invoked only at these moments, security scales with risk instead of friction — everyday work is untouched, while the highest-stakes actions get a present, verified human and a signed, auditable record. Triggers and thresholds can be tuned at any time as your risk profile changes.

PROVABLE HUMAN IDENTITY | PASSWORDLESS & AI-RESISTANT | AUTHORITY-IN-THE-LOOP

Secure Your Network With Human-Verified Trust

We would welcome the chance to show you how Faction and iVALT put you in control of who — and what — acts on your network, and holds them accountable.

FACTION NETWORKS

GET EARLY ACCESS | MSP / MSSP PROGRAM