Zero Trust Blueprint 2025

A practical security build order for contractors & small teams (Protocol 4 Pro).

Executive Summary

Zero Trust is not a product. It’s a policy-driven system for deciding what is allowed to talk to what, when, and under what conditions — and proving it.

This blueprint gives you a practical build order that works for small teams and contractors without enterprise overhead.

- Default deny: nothing is trusted by network location.
- Verify explicitly: identity + device + context.
- Assume breach: segment and log as if compromise is normal.

Build Order (Do This in Order)

If you skip the order, you create expensive security theater. This sequence creates real control fast.

Step	Outcome	Tools / Notes
1. Inventory	Know what exists	Domains, apps, endpoints, admin accounts, vendors
2. Identity hardening	Stop easy takeovers	MFA, admin separation, password manager, least privilege
3. Device trust	Only clean devices access	OS updates, disk encryption, endpoint protection
4. Network segmentation	Blast radius reduced	Separate admin, prod, user, IoT; block lateral movement
5. Access policy	Rules enforceable	Conditional access by role, geo, risk, device
6. Logging + alerts	Proof + detection	Central logs, auth alerts, admin changes, data exfil signals
7. Backup & recovery	Survive ransomware	3-2-1 backups, immutable snapshots, restore drills

Minimum Policy Set (Copy/Paste)

These are the minimum policies that prevent 80% of real-world incidents.

- Admin accounts are separate from daily-use accounts (no email + admin in same identity).
- MFA required for all accounts; phishing-resistant MFA required for admins.

- No shared logins. Vendor access is time-boxed and audited.
- Default deny inbound. Only expose what must be public, behind WAF when possible.
- All production changes require logged approval (even if it’s you).
- Backups are tested monthly with a real restore.

Quick Audit Checklist (30 Minutes)

Use this checklist before you claim 'secure'. If you fail any item, the system is not secure yet.

- Do you have a list of all domains, logins, and who owns them?
- Can you see who logged in as admin in the last 7 days?
- If a laptop is stolen today, can that device access anything without MFA?
- Are backups offline/immutable and can you restore within 24 hours?
- Can a compromised user account reach admin panels or production dashboards?

Proof Artifacts (What to Show Clients)

Security is credibility. These artifacts turn security into trust and closing power.

- Access policy screenshot (conditional access rules).
- Admin account separation evidence.
- Backup policy + last restore test record.
- Logging dashboard showing auth events and alerts.
- Network segmentation diagram (high level).