NET-TECH CONSULTING

Real People, Real Protection, Right Now

# Zero Trust Security + Risk Readiness

THREATLOCKER GOLD PARTNER

ThreatLocker Gold Partner implementation + managed operations with risk assessments + tabletop exercises (optional).

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Why Zero Trust + risk readiness matters now

Control reduces your attack surface. Evidence reduces audit and insurance drag.

## Trust assumptions break first

Most incidents start with something trusted: a signed app, a vendor login, or a “normal” script. Zero Trust removes implicit trust and forces continuous verification.

## Control beats tool sprawl

ThreatLocker adds the control layer—what can run, what can talk, and where data can move—without requiring you to rip and replace your existing stack.

## Audits ask for proof

Policies and MFA aren’t enough if you can’t show evidence on demand (access reviews, logs, approvals, and exceptions) when an auditor, customer, or insurer asks.

## Incidents require rehearsal

Tabletop exercises turn “we have a plan” into practiced response, gaps, and owners—before a real incident forces the issue.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# What this program is

A managed-services operating model with Zero Trust as the control backbone.

### Net-Tech operationalizes Zero Trust with clear outcomes:

- ThreatLocker deployment + policy baseline (allowlisting, Ringfencing™, Storage Control, Network Control)
- Ongoing tuning and exception handling so controls don't drift
- Risk assessment (20/30 control scorecard) + a prioritized remediation roadmap
- Tabletop exercise facilitation + after-action report (owners, gaps, next actions)
- Leadership-ready reporting: what changed, what's enforced, and what evidence exists

## Operator-built, right-sized for mid-market teams

### Practical rollout

Start with baseline policies, then tighten based on real behavior—no "big bang" surprises.

### Minimal lift

We do the structure, tuning, and documentation. Your team provides input and approvals where needed.

### Evidence-first

Controls are paired with proof artifacts so you can answer audits, insurers, and customer reviews faster.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# What you walk away with

Concrete artifacts you can execute against—and reuse for audits and renewals.

### Core deliverables

- Zero Trust baseline + enforcement plan (ThreatLocker policies + rollout sequencing)
- Risk scorecard (20/30 controls) + prioritized remediation roadmap
- Vendor access + admin access review notes (who has access to what, and why)
- Evidence pack pointers (logs/exports, approvals, exceptions, retention notes)
- Incident readiness tabletop + after-action report (gaps, owners, due dates)

### Optional add-ons (if useful)

- vRC / vCISO governance cadence (quarterly risk reporting + evidence refresh)
- Fast-Track Remediation (close top 2–3 gaps and package audit-ready proof)
- AI & data governance (when AI becomes operational dependency)
- Cloud managed services and modernization support

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# How it works

Stage-gated flow: assess → control → prove → operate.

### Stage 0: Discovery

60–90 min workshop
Scope, priorities, access paths

### Stage 1: Baseline

Risk scorecard (20/30)
Immediate top gaps

### Stage 2: Zero Trust

ThreatLocker deployment
Policy + tuning cycle

### Stage 3: Operate

Evidence + reporting
Tabletop + quarterly cadence

## Typical engagement cadence (fast and structured)

- Discovery workshop → confirm scope and the “must-control” surfaces (apps, vendors, data paths)
- Baseline risk scorecard → identify top gaps and required evidence
- Zero Trust rollout → deploy ThreatLocker, tune policies, move from monitor → enforce
- Tabletop + evidence pack → validate response and package proof for audits/renewals

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Zero Trust routes you into the right control focus

Pick the guardrails that match your access paths and data sensitivity.

## Path A — Application control

Allow what you need. Block everything else. Pair with Ringfencing™ to limit what approved apps can do.

## Path B — Network control

Granular control over endpoint network traffic to reduce lateral movement and lock down vendor/service access paths.

## Path C — Storage control

Stop risky data movement (USB, unapproved copy/exfiltration patterns) and enforce where sensitive data can go.

## Path D — Elevation & admin discipline

Standardize privilege: approvals, elevation rules, and evidence that the right people have the right access—nothing more.

Rule: treat each environment boundary separately (endpoints, servers, privileged access, vendor pathways) so controls and evidence stay clean—and scope doesn't drift.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Mandatory gates (operational rules)

Three checks that prevent “risky by default” environments.

### 1) Control gate (default deny)

If an app/script/process isn’t approved, it doesn’t run. Exceptions are documented and time-bounded.

### 2) Access gate (vendor + admin)

Privileged access is least-privilege, reviewed, and provable (MFA, admin roles, vendor access paths and owners).

### 3) Auditability gate (proof exists)

If we can’t produce baseline logs/exports for approvals, access, and changes—controls don’t count. Proof matters for audits, customers, and insurance.

**Outcome: controlled-by-default operations with evidence you can export.**

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Evidence model (audit / insurance / customer friendly)

We don’t just configure controls—we define the proof.

| Control area | Typical evidence artifacts |
|---|---|
| Identity + access | SSO/MFA/RBAC settings, admin roles, access review notes, audit logs + retention |
| Application control | Allowlist policy exports, approval history, exception list + rationale |
| Network + vendor access | Vendor access map, segmentation notes, network control policies, remote access evidence |
| Data movement | Storage control policies, USB rules, data handling notes, alerts/incidents (if any) |
| Incident readiness | Tabletop agenda/notes, after-action report, follow-up actions + owners |

**Result: evidence that travels — leadership-ready, auditor-ready, and usable for customer security reviews.**

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# What we need from your team

Minimal lift—just enough input to bound scope and validate controls.

## People + context

- Primary IT/Security owner + an exec sponsor
- Any compliance/audit drivers (GLBA, PCI, SOC 2, customer questionnaires)
- Known pain points: vendor access, ransomware exposure, or tool sprawl

## Tools + environment

- Endpoint/server inventory + identity provider details (SSO/MFA/RBAC)
- Current endpoint security stack (EDR/MDR, M365, backups)
- List of key vendors with access paths (VPN, RMM, admin accounts)

We can start even if parts are unknown—the first workshop is designed to surface and bound the unknowns.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Workshop format to get started

Goal: align on priorities, control focus, and evidence expectations.

### 1) Confirm operational priorities

What has to stay up? What can't be disrupted? Identify critical apps, users, and workflows.

### 2) Map access paths

Vendor access, admin accounts, remote access methods, and where sensitive data enters/exits.

### 3) Select Zero Trust control focus

Pick the first enforcement targets (apps, network paths, storage rules, elevation discipline).

### 4) Lock next steps + evidence

Owners, sequencing, approval path, and what proof you need (audit/insurance/customer).

### Pre-work (optional)

If you can share a vendor list + current security stack before the workshop, we'll come in with a draft access map and a recommended "first enforcement" plan.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Where MSP services and Zero Trust fit

Governance sets the rules. Controls enforce them. Operations keep them from drifting.

### Layer 1 — Risk & compliance readiness (vRC / vCISO)

Risk scorecards, policies, evidence cadence, and leadership-ready reporting aligned to business goals and regulatory/insurer pressure.

### Layer 2 — Zero Trust controls (ThreatLocker)

Default-deny application control, Ringfencing™, Network/Storage Control, and elevation/admin discipline—implemented and managed by Net-Tech.

### Layer 3 — MSP operations (support + monitoring + cloud)

Keep controls tuned, reduce drift, and maintain stability across endpoints, identity, and backups—day to day.

Adjacent: AI & Data Governance can layer in when AI becomes an operational dependency (policies, boundaries, evidence).

NET-TECH CONSULTING
Real People, Real Protection, Right Now

# Next steps

We'll keep this momentum and make the first workshop decision-ready.

### Checklist

- Confirm attendees (IT/Security + an executive sponsor)
- Share vendor list + remote access methods (VPN/RMM/admin accounts)
- Identify highest data sensitivity in scope (Public / Internal / Confidential / Regulated)
- Confirm current endpoint + identity stack (EDR/MDR, M365, MFA/SSO)
- Align on success criteria and the evidence format needed for audits/insurers/customers

Contact: Zachary Kinder | Partner | zachary.kinder@net-tech.us | 877-449-8324