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

THREATLOCKER
GOLD PARTNER

Zero Trust, Simplified

Control what runs. Protect what matters. Verify everything.

How SMBs and mid-market organizations can stop cyber threats before they start with ThreatLocker and Net-Tech.

Net-Tech Consulting LLC
6090 Surety Drive El Paso, TX 79905
6565 N MacArthur Blvd #225 Irving, TX 75039
Net-tech.us
marketing@net-tech.us
(877) 449-8324

Contents

I. Introduction: Why Zero Trust Matters Now

Perimeters used to protect us.
Firewalls, antivirus, and detection tools were enough to keep threats outside the network.

But today's reality is different:

- Teams work remotely.
- Vendors access internal systems.
- Apps and data live in the cloud.
- And attackers don't need to break in, they simply log in.

Every assumption of trust becomes a potential vulnerability.
That's why **Zero Trust** is no longer an enterprise-only concept, it's a **foundational mindset for every organization**, large or small.

II. The State of Cybersecurity Today

Recent industry data paints a clear picture:

- Over **80% of breaches** exploit trusted accounts or authorized systems.
- The **average SMB breach cost** now exceeds **$4.45 million (IBM 2024).**
- Most SMBs rely on **4–7 disconnected tools** for protection, and still experience gaps.

In short: **Detection is not enough.**
What organizations need today is *control.*

III. What Zero Trust Really Means

Zero Trust isn't a product or a quick configuration.
It's a strategy built on three core principles:

1. **Never Trust, Always Verify** – Every user, device, and process must earn trust continuously.
2. **Least Privilege Access** – Only the minimum required permissions are granted.
3. **Assume Breach** – Design systems as if they're already compromised.

This philosophy eliminates implicit trust, limits damage, and makes lateral movement nearly impossible.

In practice, Zero Trust creates a controlled ecosystem where every action, from file access to application launch, is authorized, monitored, and logged.

IV. Where ThreatLocker Fits in the Security Stack

Organizations often ask:

"Where does ThreatLocker fit? Is it endpoint protection, EDR, or MDR?"

The answer: **It's the control layer.**
ThreatLocker complements, or replaces, traditional endpoint and detection tools by enforcing a strict Zero-Trust policy at the application, network, and data level.

Key Components:

- **Application Control:** Only approved apps can run.
- **Ringfencing™:** Even trusted apps can't overreach or communicate unexpectedly.
- **Storage Control:** Prevent unauthorized copying or data exfiltration.
- **Network Access Control:** Isolate systems and block lateral spread.
- **Endpoint Control:** Enforce policy baselines, stop drift, and maintain integrity.

ThreatLocker transforms security from *reactive* to *predictive.*

V. The Power of Control Over Detection

Traditional EDR and antivirus systems **detect** anomalies.
ThreatLocker **prevents** unauthorized activity outright.

Here's how the models differ:

	Detection Tools (EDR/MDR)	ThreatLocker (Zero Trust Control)
Timing	After the threat occurs	Before the threat executes
Action	Detects and alerts	Blocks and isolates
User Impact	Reactive, variable response	Controlled, consistent behavior
Visibility	Post-incident	Continuous, preemptive

When combined with Net-Tech's operational management and compliance integration, this shift to control produces measurable outcomes, fewer alerts, faster recovery, and a demonstrably lower attack surface.

VI. How Net-Tech Operationalizes Zero Trust

Technology alone can't deliver Zero Trust, it requires **governance, accountability, and ongoing tuning.**

As a **ThreatLocker Gold Partner**, Net-Tech helps clients implement and sustain Zero Trust through:

- Tailored deployment and policy configuration
- Continuous monitoring and optimization
- Integration with SentinelOne, Datto EDR, Microsoft Defender, and other tools
- Governance alignment through **vGRC** and **vCISO** programs
- Reporting that connects controls directly to business and compliance outcomes

Net-Tech ensures Zero Trust isn't just installed, it's *institutionalized.*

VII. Real-World Use Case: From Reactive to Resilient

Client Snapshot:
A regional healthcare provider with hybrid cloud systems and multiple vendor connections faced repeated phishing and unauthorized software incidents despite an EDR platform.

The Approach:
Net-Tech implemented ThreatLocker with:

- Application Control and Ringfencing™
- Storage Control for patient data protection
- Integration into their compliance program (HIPAA/NIST CSF)

Results:

- 72% reduction in endpoint security alerts
- Zero unauthorized application executions in 90 days
- Compliance audit passed with zero major findings

Control replaced chaos. Security became measurable.

VIII. Your 60-Day Zero Trust Rollout Roadmap

Timeline	Milestone	Outcome
Days 1–15	Deploy ThreatLocker and establish baseline application and storage policies.	Core protection activated.
Days 16–30	Monitor behavior, fine-tune rules, and engage SOC.	Environment learning phase complete.
Days 31–60	Enforce full control and integrate compliance mapping.	Zero Trust becomes operational.

From there, Net-Tech's vCISO oversight maintains continuous optimization, risk reporting, and measurable improvement.

IX. Compliance Alignment: Proving What You Protect

Security and compliance are no longer separate goals.
With Net-Tech's integrated frameworks, every ThreatLocker control maps to recognized standards like:

- **HIPAA** (Healthcare)
- **SOC 2** (Service Providers)
- **PCI-DSS** (Financial)
- **NIST CSF** (General Framework)

The result: your audit trail isn't theoretical, it's embedded in your security controls.

X. Taking the Next Step

Zero Trust isn't about complexity, it's about **clarity and confidence.**

With ThreatLocker and Net-Tech:

- You control what runs.
- You verify every action.
- You protect your data, endpoints, and reputation.

Your perimeter may be gone, but your control doesn't have to be.

Download this whitepaper and take the next step:
Schedule a Zero Trust Walkthrough at net-tech.us/zero-trust