compucom
Technology Driven.
People Powered.

ASSESSMENT:
Zero Trust Readiness

GET CYBER RESILIENT. SHRINK THE ATTACK SURFACE.

The Challenge

Enterprise security challenges have fundamentally shifted. With today's remote workforces and applications in the cloud, the traditional network perimeter is gone. Firewalls can't protect assets that no longer sit behind them. Breaches are increasingly inevitable — most commonly from phishing and credential theft, followed by unchecked lateral movement once attackers gain access.

The Solution: Zero Trust – Verify Everything. Trust Nothing

Zero Trust Architecture (ZTA) is a cybersecurity model based on the principle of *"never trust, always verify."* It requires continuous authentication, authorization, and validation of users, devices, and applications before granting access to resources. ZTA helps your organization:

- **Protect identities, devices, applications, and data —** no matter where they reside
- **Limit blast radius** by enforcing least privilege, continuous authentication, and micro-segmentation
- **Meet increasing compliance and cyber insurance requirements –** frameworks such as NIST 800-207, CISA's Zero Trust Maturity Model, and many industry regulations require it
- **Reduce security cost and complexity** by consolidating identity, access, and security controls, resulting in fewer tools and less overhead

However, jumping into Zero Trust Architecture without a plan is like renovating a house without an inspection. You risk missing critical structural issues and wasting money.

The Benefits of Our ZTA Assessment

Our Zero Trust Assessment delivers a practical, actionable plan, along with these key benefits:

1. **Identify your current maturity.** Most organizations have elements of Zero Trust in place, such as identity management, MFA, and endpoint controls. Our assessment maps what you have, what's missing, and what's misconfigured.
2. **Prioritize what matters most.** We help you focus first on high-impact areas first, including identity protection, micro-segmentation, device compliance, and data classification.
3. **Align Zero Trust with your business goals.** Security shouldn't slow your business down. We tie Zero Trust outcomes to productivity, risk reduction, compliance, and cloud strategy – driving leadership buy-in.

“Never trust, always verify.”

– John Kindervag, creator of Zero Trust

Assessment Details:

(Three Week Fast-Track)

Week 1 – Discovery	• Stakeholder interviews • Architecture and policy review • Inventory of tools, configurations, and controls
Week 2 – Analysis	• Review the six core Zero Trust pillars: 1. **Identity:** MFA, authorization policies, privileged access, identity lifecycle 2. **Devices:** Managed/unmanaged devices, compliance, BYOD, patching 3. **Network:** Segmentation, NAC, east-west visibility, Zero Trust access 4. **Applications & Workloads:** Authentication methods, API security, cloud workloads, legacy applications 5. **Data:** Classification, DLP, encryption, access governance 6. **Governance & Operations:** Policies, monitoring, incident response, tool rationalization • Generate Maturity scoring • Perform Gap identification • Risk prioritization
Week 3 –Roadmap and Recommendations	• Quick wins (30–90 days) • Strategic initiatives (12–36 months) • Cost and resource considerations • Executive presentation

Assessment Deliverables

We deliver a phased implementation roadmap that takes you from your current state to your target security maturity. Instead of vague advice, the roadmap provides concrete cost estimates, prioritized technology recommendations, and a clear breakdown of quick wins versus longer term strategic investments.

Benchmark your maturity.
Improve your security posture.

Contact us to schedule your Zero Trust Readiness Assessment.

compucom®
Technology Driven.
People Powered.