Zero Trust Security Assessment & Implementation

Accelerating Enterprise Protection with Microsoft Security Ecosystem Integration

Security & DevSecOps | 2026

60–70%	3–5x	60–80%
Reduction in Manual Effort	Faster Incident Response Times	Reduction in Breach Likelihood

Introduction

Your attack surface is expanding beyond traditional boundaries to include AI agents, copilots, and distributed data — not just users. Evoke Technologies deploys Zero Trust Architecture across cloud, data, and AI ecosystems so every access request is verified, every AI action governed, and every data interaction is protected.

Since most breaches involve stolen credentials or inside access, a new foundation of security is essential to protect your enterprise.

The Challenge: Why Traditional Security Fails

Traditional Security Relies On	This Approach Results In
Strong perimeter walls that operate like a castle defence	Modern attacks bypassing perimeters using stolen passwords, phishing, or compromised vendors
Implicit trust for anyone or any device once inside the network	Attackers gaining unrestricted access once they breach the initial defence
A defined perimeter that ignores remote work and dozens of SaaS apps	Growing compliance risk as frameworks like the EU AI Act and NIST demand strict accountability for autonomous systems
High manual overhead for compliance audits	Slower, costlier, and more error-prone audit cycles

Because 95% of breaches involve stolen credentials or inside access, perimeter security is no longer sufficient. A Zero Trust architecture is essential.

The Solution: Three-Phase Zero Trust Lifecycle

Zero Trust flips the traditional model by assuming: "Never trust. Always verify. Everyone and everything."

Phase 1
Verify Everyone, All the Time

Continuously authenticate identity, device health, location, and behaviour. Any change mid-session revokes access

Phase 2
Give People Only What They Need

Enforce least-privilege access so a stolen password only exposes one user's narrow scope of permissions.

Phase 3
Assume You Are Already Hacked

Segment networks into distinct zones, monitor all activity, and design systems so attackers cannot move laterally.

Our Coverage: The Six Areas to Protect

Zero Trust security requires comprehensive protection across six distinct vectors:

🔑 **Identity**
Strong passwords, MFA, and continuous verification for users, IoT, and OT assets.

💻 **Devices**
Inventory, access control, and health checks for computers, phones, and smart equipment.

🔌 **Applications**
Secure the software people use and the connections between them to prevent hijacking.

🗄️ **Data**
Classify, encrypt, monitor access, and prevent exfiltration of sensitive information.

🚧 **Infrastructure**
Monitor behaviour and apply security settings across servers, cloud, and industrial controllers.

🌐 **Networks**
Segment IT, IoT, and OT environments to contain a single compromised device.

The Organizational Impact

For IT Leaders
Gain better visibility, replace manual access approvals with automated policy enforcement, and reduce breach response times to hours.

For Managers
Benefit from faster onboarding, immediate offboarding, and enhanced control over team data access.

For Business Users
Get seamless, frictionless access to the tools you need every day, without security friction slowing you down.

Real-World Use Cases

The Zero Trust framework is applicable across a wide range of enterprise security scenarios:

Use Case	Description
Hybrid & Remote Workforce Security	Enforce continuous verification for distributed teams accessing SaaS and cloud apps from any device or location.
AI & Copilot Governance	Apply Zero Trust controls to AI agents and copilots to meet EU AI Act and NIST accountability requirements.
Insider Threat & Credential Theft Mitigation	Limit blast radius when credentials are compromised through least-privilege access and continuous monitoring.
Cloud & SaaS Application Security	Secure access and connections across dozens of SaaS applications beyond the traditional network perimeter.
IoT/OT Network Segmentation	Isolate industrial controllers, sensors, and smart equipment from critical operations to contain compromised devices.
Regulatory Compliance & Audit Readiness	Reduce manual compliance overhead with automated policy enforcement and full audit trails.

Why This Matters Now

Zero Trust is not simply a tooling upgrade — it is a foundational shift in how the enterprise defends itself. As AI agents, copilots, and distributed workforces expand the attack surface, a verify-everything security posture is becoming the baseline expectation, not a differentiator.

- Contain breaches faster with least-privilege access and continuous verification
- Meet emerging AI governance requirements under the EU AI Act and NIST
- Replace manual compliance overhead with automated policy enforcement
- Build stakeholder and customer trust in your security posture

Protect every identity, device, and AI interaction — with Zero Trust, powered by Evoke Technologies.

Ready to Strengthen Your **Security Posture?**

Connect with Evoke's experts today to schedule a Zero Trust security assessment or personalized demo.

www.evoketechnologies.com | mktg@evoketechnologies.com