

Zero Trust Workshop

Leverage your Microsoft investment to create a strong Zero Trust security environment.



The premise of Zero Trust is “don’t trust, verify.” This approach applies to users, devices, and connectivity sessions.

Organizations should move toward a Zero Trust architecture to better secure their assets and data.



CHALLENGES

As more employees work remotely and cyber attacks continue to increase and become more damaging, organizations must provide an environment that enables employee productivity while keeping identities and assets secure.

IDEAL SOLUTION

Leverage an identity-focused Zero Trust security model to prevent breaches and protect the entire IT ecosystem. Through tailored interviews and discussions, OCG will identify your concerns and objects, review the threat landscape, and identify opportunities for improvement. Our results will be presented in a detailed report and briefing session.

DESIRED OUTCOMES

OCG's Zero Trust workshop will help your organization learn about, explore, and prioritize the identity and security capabilities provided by Microsoft Entra, Microsoft 365, and Windows. With our recommendations, you'll be able to increase security, improve productivity, and reduce risk.



Zero Trust Workshop

What should your organization be doing to ensure data and digital assets stay secure? How can you leverage your Microsoft 365, Microsoft Entra, and Windows investments to get started adopting a Zero Trust framework?

OCG's Zero Trust workshop will help your organization learn about, explore, and prioritize Microsoft Entra's identity and security capabilities so you can increase security, improve productivity, and reduce risk.

The workshop starts at 3 days long but is customized to include your desired scope.

Day 1 Interviews and Discussions

- Identify specific concerns, objectives, and projects already underway
- Review the threat landscape, understand how it applies to your business
- Identify gaps and opportunities for improvement

Day 2 Report Creating

- Current security status
- Key risks and gap analysis
- Identify cost savings potential
- Recommendations for improvements in Identity protection, Threat management, Access management, Device management, and Data loss prevention

Day 3 Briefing Session & Deliverables

- Detailed report and executive briefing
- Discuss implementation roadmap and next steps

Zero Trust Guiding Principles

Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, risk, and anomalies.

Use Least Privileged Access

Minimize user access with Just-In-Time, privilege escalation, risk-based adaptive policies, and data protection (Microsoft refers to this as Just-Enough-Access).

Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.



Zero Trust Workshop

Call for more information: +1 877-862-1617

Ask a question via email: info@oxfordcomputergroup.com

 **Microsoft**
Solutions Partner
Security

Specialist
Identity and Access
Management