softcat

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified
Managed XDR Solution

Microsoft Zero Trust Workshop

Build a clear, actionable path to a stronger security posture

---

What is Zero Trust?

The Zero Trust framework is a modern security strategy that operates on 3 core principle of;

- ***Verify Explicitly*** – Always authenticate and authorise based on all available data points
- ***Use Least Privilege Access*** – Limit user access with solutions such as Just-In-Time and Just-Enough-Access (JIT/JEA). Deploy risk-based, adaptive policies
- ***Assume Compromise*** – Building business processes and systems if a breach has already happened or soon will.

It assumes that threats can come from both inside and outside the network, and therefore, every access request must be authenticated, authorised, and encrypted.

Commented [AC1]: Should we change this to Assume Compromise, as mentioned in the Microsoft Documentation? Happy either way, just a thought

---

Overview of the Workshop

The Microsoft Zero Trust Workshop helps organisations evaluate their current security posture and define a practical roadmap for adopting Zero Trust principles. Guided by Microsoft security experts, participants will explore their existing environment, identify gaps, and prioritise improvements. The workshop also demonstrates how Microsoft Security solutions can support and strengthen an organisation's overall cybersecurity strategy, leaving attendees with a tailored, actionable plan for advancing their Zero Trust journey.

Why it matters

Without a structured framework, it's challenging to assess your progress toward Zero Trust or determine which security gaps to prioritise.

This workshop:

- Pinpoints your current Zero Trust maturity level
- Highlights your most pressing security risks
- Maximises the value of your existing Microsoft security investments

- Delivers clear, actionable next steps to strengthen your security posture

---

Our approach

We structure the workshop around the six core pillars of Microsoft's Zero Trust model:

1. **Identities** – Verify every identity explicitly
2. **Devices** – Ensure all endpoints are secure and compliant
3. **Data** – Classify, protect, and monitor sensitive information
4. **Networks** – Limit access and segment traffic to reduce risk
5. **Infrastructure** – Secure workloads across on-premises and cloud environments
6. **Security Operations** – Detect threats, respond effectively, and recover quickly

We recommend selecting the **Identity** and **Security Operations** pillars as we see the highest value from these workshops.

What you get

- **Free delivery of 2 modules** from the 6-pillar framework
- Conducted online via Microsoft Teams in a conversational, interactive format
- Tailored guidance based on your needs and current maturity
- A comprehensive written report with your starting position and recommended next steps
- Optional follow-up sessions for guidance on implementation support

Commented [AC2]: Next

Workshop format

- **Duration:** 2 days of customer time + report delivery
- **Delivery:** Online via Microsoft Teams
- **Style:** Collaborative discussions with Microsoft Security experts

---

Call to Action

If your organisation is ready to take the first steps towards a robust Zero Trust posture, contact your aligned Softcat Account Manager who can contact our internal **Microsoft Commercial Team** for next steps.