











Zero Trust  
Discovery



# Independently audited and certified expertise



## Azure Expert MSP

 <b>Microsoft</b> Modernisation of Web Applications Advanced Specialisation	 <b>Microsoft</b> Windows SQL Server Advanced Specialisation	 <b>Microsoft</b> Azure Virtual Desktop Advanced Specialisation	 <b>Microsoft</b> Teams Calling Advanced Specialisation
 <b>Microsoft</b> Adoption and Change Management Advanced Specialisation	 <b>Microsoft</b> Identity and Access Management Advanced Specialisation	 <b>Microsoft</b> Information Protection and Governance Advanced Specialisation	 <b>Microsoft</b> Threat Protection Advanced Specialisation



# Assess

How

Zero Trust Discovery

What

- Solution assessment to review security vulnerabilities
- Requirement gathering workshops
- Analysis and interpretation of assessment data
- Stakeholder walk through

Value

- Interpret assessment data
- Visualise the future state
- Understand the blockers to secure scalable growth
- Get early stakeholder buy-in

Assess



Plan



Implement



Operate

# Zero Trust Discovery

## Positioning

### Understand your security maturity level

Fully understand your current deployed security systems and how to align them within the best practice guidance to Microsoft's Zero Trust architecture.

Identifying stakeholder, functional and organisational requirements.

## Benefits

### Adoption plan

This service will provide you with an adoption business case to build confidence in the proposed plans.

## Deliverables

Target State solution design that is aligned to your organisation requirements and the Microsoft Zero Trust architecture.

Walk through with key business stakeholders.

## Summary of works

### Microsoft Assessment

This service is best wrapped around a Microsoft delivered solution assessment. Our team can recommend the most suitable assessment and nominate you for it to be fully funded by Microsoft.

### Deep analysis of in-scope workloads and databases

Assessment data will be given a high-level analysis to contextualise it with the requirements uncovered from the workshops.

This analysis will see our architects utilise both Cloud Direct and Microsoft design patterns, best practice, and experience to identify the target state solution.

### Requirement gathering deep-dive workshops

Organisational – what are the drivers and expected value of Zero Trust

Service – what commitments are in place for securing the environment

Operational – how is security currently deployed and supported within the environment and business

### Stakeholder walkthrough

A walk through of the analysis, requirements and solution design with stakeholders.

Helping all parties understand the findings and recommendations to help inform a business decision on next steps.

Assess



Plan



Implement



Operate

