







## Engagement Results

-  Receive a prioritized roadmap for configuration improvements
-  Identify and mitigate security vulnerabilities in your Entra ID environment
-  Improve performance and reliability by aligning with Microsoft best practices
-  Determine the best way to give your users access to the apps they need on the devices of their choosing

“Defining the structure of the Entra ID and ensuring that everything operates as it should can be a difficult and time-consuming process but a crucial investment in your company's security.” \*

Is your Entra ID helping secure your business—or silently exposing it to risk?

## The Foundation of Enterprise Identity and Access

Entra ID is the backbone of identity and access management for most organizations, playing a critical role in securing user authentication, managing permissions, and enabling seamless access to resources. A well-maintained Entra infrastructure ensures operational continuity, supports compliance with regulatory standards, and forms the foundation for modern security models like Zero Trust. Without proper configuration and oversight, Entra can become a significant vulnerability, making adherence to best practices essential for business resilience and security.



## Why assess your Entra ID?

Your Entra ID environment is critical to identity, access, and security across your organization. Over time, misconfigurations, legacy policies, and lack of visibility can introduce risk. This assessment helps you uncover those risks and optimize your Entra infrastructure for performance, security, and scalability.

Properly configured Entra ID reduces vulnerabilities

Best practices ensure consistent replication, minimizing outages and performance issues

Aligning Entra with Microsoft and industry standards supports audit readiness

A well-structured Entra environment is easier to manage, scale, and integrate with modern cloud services

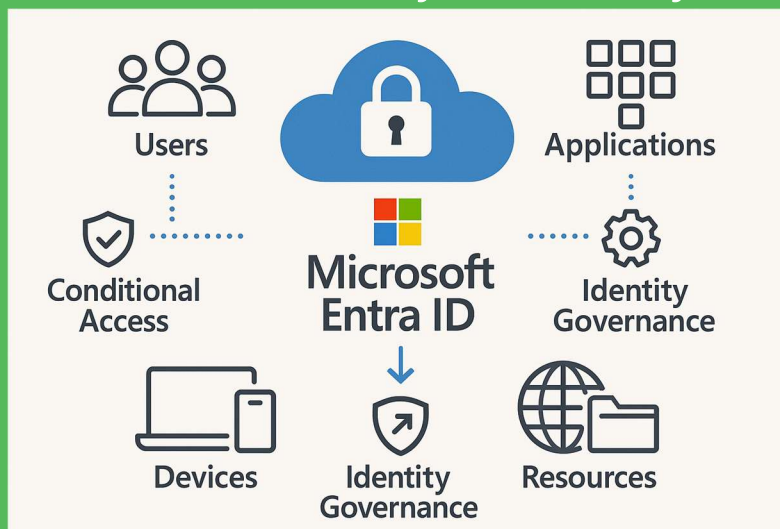
## What to expect

TechNet UC's certified experts will evaluate your Entra ID environment across key areas tenant configuration, domain federation, Conditional Access, synchronization, and identity governance policies. You'll receive a detailed report with findings, risk ratings, and actionable recommendations.

We'll work with you to:

- Review tenant configuration and domain federation setup
- Identify misconfigurations and non-compliance with Microsoft best practices
- Assess user identities, roles, and governance policies
- Deliver a knowledge transfer session to empower your IT team

## Entra ID Assessment – The Key to A Healthy Environment



### Who should be interested

The engagement is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Endpoint & Device Management owners/ decision makers
- Application business owners
- IT Security
- IT Operations
- Security Architect
- Security Engineers

### Why TechNet UC?

When it comes to unified endpoint management you need an experienced partner.

We've helped hundreds of customers. Let us help you too.



TechNet UC