





Engagement Results

-  Receive a prioritized roadmap for configuration improvements
-  Identify and mitigate security vulnerabilities in your AD 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 Active Directory 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 Active Directory helping secure your business—or silently exposing it to risk?

The Foundation of Enterprise Identity and Access

Active Directory 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 AD 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, AD can become a significant vulnerability, making adherence to best practices essential for business resilience and security.



Why assess your Active Directory?

Your AD 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 AD infrastructure for performance, security, and scalability.

Properly configured AD reduces vulnerabilities

Best practices ensure consistent replication, minimizing outages and performance issues

Aligning AD with Microsoft and industry standards supports audit readiness

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

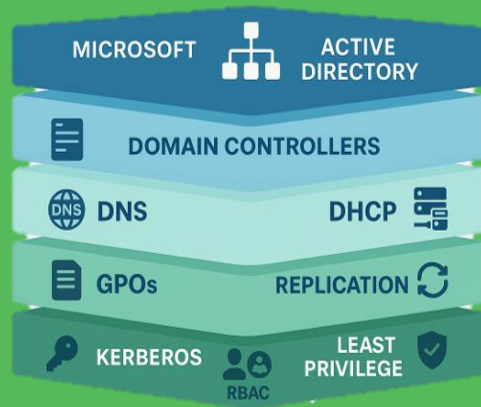
What to expect

TechNet UC's certified experts will evaluate your AD environment across key areas including domain structure, DNS integration, GPOs, replication, and security policies. You'll receive a detailed report with findings, risk ratings, and actionable recommendations.

We'll work with you to:

- Review domain and forest structure, DNS, GPOs, and replication
- Identify misconfigurations and non-compliance with Microsoft best practices
- Assess user accounts, permissions, and security policies
- Deliver a knowledge transfer session to empower your IT team

Active Directory Assessment Aligned with Microsoft Best Practices



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 have helped hundreds of customers deployment Intune in their environment. Let us help you too.



TechNet UC