Active Directory Security Review

AD is the market leading directory service solution used by 95% of organisations globally to authorise and authenticate resources (including users, devices, and applications) at the core of their environment.

AD is now 30+ years old and in many cases has been configured and customised over time to meet the specific needs of the business and its users. As technology and cyber awareness advance, threats increase, leaving both known and unknown gaps within core security infrastructure.

Cyber Security across industry is at an all-time high and breadth/depth of experience is often limited within organisations based on in house skills and experience only. Recruitment and resourcing challenges within public sector present an opportunity for cost effective short term external engagement to address critical security concerns or issues. Experience suggests market demand for a series of AD Core Services is high due to the risk related to its age as well as common misconfiguration and embedded complexities within legacy AD infrastructures.

Gain Critical AD Security Insight

An Active Directory (AD) security review is a comprehensive assessment of the security measures and practices within an organisation's Active Directory environment. Active Directory is a critical component of many Windows-based networks, and securing it is crucial to protect sensitive information and maintain the overall security of the network.

The Active Directory Security Review (ADSR) is designed to assess any Active Directory deployment and offer pragmatic mitigations to increase the security and operational strength across the many discrete infrastructures and components that comprise a typical AD deployment.

The primary objective is to highlight the most common critical issues that directly affect security and operations which, when remediated correctly, will greatly increase the security of the Active Directory itself, its host platform, and the infrastructure that it serves.

MTI - A Trusted Security Partner

Conducted over 120 meticulous AD Security audits within the NHS over the past 24 months

Successfully executed Active Directory enhancement projects for over 20 NHS organisations amidst the challenges posed by the COVID-19 pandemic

Conducted Microsoft Security integration projects, encompassing deployment of AOVPN, WDAC, MDE, and MEM, enhancing the overall security posture

Implemented Privileged Access Management solutions for a prominent central government organisation

Recognised as a founding member of CREST, while maintaining active membership in both CREST and NCSC CHECK security organisations

Holding ISO 27001 certification and CE+ accreditations

8 Reasons to Understand and Secure your AD Now

At the end of the review you will receive a full and detailed report documenting the findings and suggesting mitigation and remediation for critical and high-risk findings for both security and functional issues.

- **Identify Vulnerabilities:** Helps identify vulnerabilities and weaknesses in the Active Directory setup. This can include misconfigurations, outdated software, or insecure practices that could be exploited by attackers.
- **Enhance Security Posture:** By identifying vulnerabilities and weaknesses, organisations can take proactive steps to enhance their security posture. This may involve implementing additional security controls, patching systems, or reconfiguring AD settings.
- **Detect Unauthorised Access:** An AD security review can help detect unauthorised access or suspicious activities within the Active Directory environment. This includes identifying unauthorised users, unusual access patterns, or privilege escalation attempts.
- **Ensure Compliance:** Many organisations are subject to regulatory requirements and compliance standards that mandate specific security measures for protecting sensitive data. A security review can help ensure that the AD environment aligns with these compliance requirements.
- **Prevent Data Breaches:** AD security reviews can help prevent data breaches by identifying and mitigating security risks before they can be exploited by attackers. This can save an organisation from the financial and repetitional damage associated with data breaches.
- **Improve User Management:** Helps organisations improve user account management practices. This includes reviewing and optimising user provisioning and deprovisioning processes, ensuring that user permissions are appropriate, and reducing the risk of dormant or unused accounts.
- **Enhance Incident Response:** In the event of a security incident, having a well-documented and regularly reviewed AD security plan can facilitate a more effective incident response. It allows organisations to quickly identify and remediate security issues.
- **Streamline Access Control:** Help organisations streamline access control by ensuring that users have the appropriate level of access to resources and that permissions are based on the principle of least privilege.
- **Improve Password Policies:** Weak or insecure password policies can be a significant security risk. A security review can help organisations strengthen their password policies, enforce password complexity, and implement multi-factor authentication where necessary.

Case Study

"We needed a provider that could meet our volume of demand. We have over 300 web sites, apps and portals, in over 10 countries, each running in it's own silo, in local initiatives, collecting personal information. MTI is that provider."

Ian Livingstone
Cyber Security Manager
British Council