Client Success Story – Financial Industry

Securing a Multi-Forest Active Directory Environment for a Leading Financial Technology Provider

---

Client Profile

A prominent financial technology and data services provider based in the northeastern United States; this enterprise supports over 20,000 users across eight nationally distributed sites. The organization maintains a highly customized, multi-forest Active Directory environment, originally architected in 2001 and expanded over time to support complex identity and access needs. With five AD forests and numerous cross-forest trusts, the environment had become increasingly intricate, prompting the Information Security and IT teams to pursue a focused assessment of their Active Directory platform. The objective was to identify legacy exposures and strengthen the identity infrastructure's security posture.

The Challenge

The organization relied on a deeply layered Active Directory environment to manage global authentication and access. While the environment had evolved to support complex operations, years of legacy configurations introduced unaddressed technical debt. The client needed a thorough evaluation to identify configuration weaknesses, privilege mismanagement, and areas of risk impacting the integrity of their identity platform.

Top 3 Highest-Risk Discoveries

- **Administrator Accounts with Unconstrained Kerberos Delegation**
  Enabled potential Golden Ticket–style attacks with unrestricted credential exposure.
- **Service Accounts with Domain Admin Privileges**
  Allowed persistent administrative access with minimal oversight or lifecycle controls.

- **KRBTGT Account Password Never Rotated**
  Exposed the forest to long-term ticket forgery risk, undermining the Kerberos trust model.

Security Risks Identified

The assessment revealed several critical security issues, including:

- **LM Authentication Enabled**: Legacy, insecure protocols still permitted via Group Policy, weakening authentication integrity.
- **Unsecured User Rights on Domain Controllers**: Non-administrative accounts granted excessive local rights.
- **Service Accounts with Domain Admin Privileges**: Non-human accounts had unrestricted access, increasing lateral movement risk.
- **Unconstrained Kerberos Delegation**: Administrator accounts exposed to ticket-forging attacks due to legacy delegation settings.
- **KRBTGT Account Password Never Rotated**: Created a potential for persistent Golden Ticket attacks.

The Approach & Solution

Working closely with internal Information Security and IT teams, a methodical, risk-based strategy was executed to strengthen the platform:

- **Authentication Policies Hardened**: Disabled LM Authentication and enforced NTLMv2/Kerberos across forests.
- **Domain Controller Protections Implemented**: User rights assignments reviewed and restricted to prevent privilege escalation.
- **Privileged Access Reassessment**: Excessive permissions removed from service accounts, and managed service accounts introduced where applicable.
- **KRBTGT Password Rotated in Stages**: Mitigated long-term ticket forgery risks using a safe, staged reset process.
- **Kerberos Delegation Restrictions Applied**: Unconstrained delegation replaced with secure alternatives.

The Impact

The organization achieved measurable improvements in security posture, including:

- **Eliminated over a dozen high-risk misconfigurations** across the identity platform.

- **Reduced Active Directory attack surface by an estimated 60%** through privilege boundary enforcement and delegation reconfiguration.
- **Improved audit readiness** by aligning configurations with current best practices and internal security standards.
- **Established a defensible identity foundation** for future platform integrations and compliance initiatives.

These outcomes were directly integrated into the enterprise's broader governance framework, reinforcing centralized identity oversight and long-term risk mitigation.

Strategic Takeaway

Even mature organizations can carry substantial legacy risk in their identity infrastructure. This engagement highlights the importance of periodic, platform-specific security posture assessments to uncover hidden exposures and align operational realities with modern security expectations.