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.

Client Success Story – Healthcare Industry

Discovering Cross-Platform Vulnerabilities in a Healthcare Technology Provider's Identity and Virtualization Stack

---

Client Profile

A nationally recognized healthcare technology provider specializing in electronic medical records (EMR), this organization operates a sophisticated internal IT infrastructure supporting over 13,000 users. Headquartered in the Midwest, the company plays a pivotal role in powering digital healthcare platforms across the U.S. The internal IT and Information Security teams, including cybersecurity leadership and virtualization SMEs, initiated a security assessment of their Active Directory that was later expanded to include the VMware vSphere environment after indicators of compromise suggested cross-platform vulnerabilities. While the organization maintained a generally mature security posture, the assessment revealed key blind spots, particularly in legacy authentication settings and virtualization layer protections, prompting corrective action in alignment with HIPAA compliance objectives.

The Challenge

The engagement began as a focused identity security posture review but quickly evolved when signs of deeper architectural risk surfaced. A potential attack path extending from Active Directory into the virtualization layer raised concern about cross-platform exposure. The organization needed visibility into both layers and a path to close the security gaps threatening the integrity of its electronic medical records infrastructure.

Top 3 Highest-Risk Discoveries

- **VMware Tools Vulnerability on Virtualized Domain Controllers**
  Allowed non-privileged AD users to exploit a known weakness and gain elevated access.
- **Lack of Network Segmentation Between AD and vSphere Components**
  Created an opportunity for lateral movement across trust boundaries.

- **Insecure Configuration of Virtualized Domain Controllers**
  Enabled potential guest-to-host privilege escalation from within critical systems.

Security Risks Identified

Initial findings in the identity platform revealed a potential lateral attack vector into the virtualization environment. Key risks included:

- **Outdated VMware Tools Installed on Domain Controllers**: Allowed exploitation of known privilege escalation vulnerabilities.
- **No Segmentation Between vSphere and AD Management Traffic**: Permitted unrestricted bidirectional access.
- **Lack of Hardening on Virtualized Domain Controllers**: Included insecure VM configuration parameters and excessive guest privileges.
- **Overlapping Administrative Access Rights**: Exposed both platforms to compromise from a single point of failure.

The Approach & Solution

The assessment scope was expanded in coordination with IT and InfoSec leadership to fully evaluate both AD and vSphere platforms. The following steps were taken:

- **Vulnerability Remediation**: Patched VMware Tools on all virtualized systems to close known exploit paths.
- **Network Segmentation Enforcement**: Introduced strict controls separating Active Directory components from vSphere management interfaces.
- **VM Hardening Standards Applied**: Hardened Domain Controllers by disabling unnecessary virtual features and restricting privileges.
- **Privileged Access Review Conducted**: Aligned roles and rights across platforms to reduce cross-platform administrative exposure.

The Impact

The organization successfully closed critical gaps that could have enabled lateral movement from Active Directory into the virtualization layer. Tangible outcomes included:

- Closed a high-risk privilege escalation vector affecting virtualized Domain Controllers
- Reduced likelihood of lateral compromise between identity and infrastructure layers
- Established enforceable segmentation policies separating identity and virtualization planes

- Improved HIPAA audit alignment by ensuring safeguards around systems housing electronic medical records

This cross-platform security posture improvement reinforced the organization's commitment to safeguarding healthcare infrastructure while supporting ongoing compliance initiatives.

Strategic Takeaway

Platform-specific assessments are not always sufficient when risks extend beyond their boundaries. This engagement demonstrated the importance of interconnected reviews that uncover how weaknesses in one layer (identity) can cascade into another (virtualization). Securing modern enterprise environments requires a holistic view of privilege, configuration, and exposure across all critical systems.

Client Success Story – Telecommunications Industry

Hardening a Nationwide VMware vSphere Environment Supporting Critical Telecommunications Services

---

Client Profile

One of the largest wireless telecommunications providers in the United States, this enterprise operates a vast national infrastructure that supports mobile communications, customer services, and backend operations. The organization conducted a security assessment on its VMware vSphere platform, spanning more than 10 distinct production enclaves, over 60 vCenter Servers, and more than 10,000 ESXi hosts. While infrastructure maturity and operational excellence in virtualization management were evident, the assessment uncovered systemic gaps in security posture across the platform. Working alongside Information Security and IT infrastructure teams, prioritized recommendations were implemented to strengthen privilege boundaries and secure hypervisor configurations. Baseline enforcement controls were applied at scale, reducing the platform-level attack surface and enhancing resiliency for critical IT services.

The Challenge

This vSphere environment served as the foundational infrastructure for the organization's nationwide operations. Despite high levels of virtualization maturity and platform standardization, inconsistent security enforcement and inherited configuration drift introduced significant exposure. The client needed a large-scale, production-grade assessment to uncover hidden risks, eliminate known exploit paths, and establish sustainable governance across its virtualization layer.

Top 3 Highest-Risk Discoveries

- **Exploitable VMware Tools Versions on Production VMs**
  Enabled guest-to-host privilege escalation, particularly dangerous on critical infrastructure workloads.

- **Unsigned vSphere Installation Bundles (VIBs) on ESXi Hosts**
  Allowed potential introduction of unauthorized or malicious software at the hypervisor level.
- **Highly Privileged Active Directory Accounts with vSphere Admin Rights**
  Created a single point of compromise bridging identity and infrastructure platforms.

Security Risks Identified

The assessment uncovered multiple systemic and high-impact vulnerabilities, including:

- **VMware Tools Versions with Known Exploits**: Widespread across production workloads, increasing risk of local escalation.
- **ESXi Hosts Without Secure Boot**: Allowed unsigned code execution during boot, undermining hypervisor integrity.
- **Unsigned VIBs Installed**: Introduced unmanaged software elements across the host layer.
- **Flat Management Network Architecture**: Lacked traffic separation between vCenter, ESXi hosts, and workloads.
- **Over-Privileged AD Accounts in vSphere**: Identity-based admin rights created excessive blast radius potential.

The Approach & Solution

The organization worked across multiple infrastructure and security teams to execute a phased remediation effort. Key actions included:

- **VMware Tools Patch Enforcement**: Ensured all workloads ran versions hardened against known vulnerabilities.
- **Secure Boot Implementation on ESXi Hosts**: Verified trusted boot configurations to block unauthorized code.
- **Signed VIB Enforcement Policy**: Established installation standards to permit only verified software.
- **Management Traffic Isolation**: Introduced dedicated VLANs and subnet segregation between management and production layers.
- **RBAC Implementation in vSphere**: Replaced broad AD administrative rights with fine-grained access controls.

The Impact

The security overhaul hardened one of the most expansive vSphere deployments in the telecommunications sector. Tangible results included:

- **Eliminated major guest-to-host escalation vectors** through patching and VM configuration updates
- **Established chain-of-trust enforcement across the ESXi host layer**
- **Reduced administrative risk surface by decoupling privileged identity accounts from infrastructure control**
- **Improved configuration consistency across 10,000+ hosts** with scalable policy enforcement
- **Laid the foundation for continuous compliance and security governance at scale**

These outcomes helped the organization operationalize a secure baseline, while empowering infrastructure teams to maintain agility and uptime without compromising integrity.

Strategic Takeaway

Scale does not equate to security. Even well-managed infrastructure can harbor platform-wide vulnerabilities if baseline enforcement is inconsistent. This engagement highlights the importance of deep configuration posture assessments in environments where virtualization is not just a component, but the foundation, of business operations.