Mitigating identity risk: How a UK-based financial services organisation secured service accounts and strengthened access controls for external advisers

BASED
UK

INDUSTRY
Finance

PROTECTED ACCOUNTS
750 employees
6,000 external advisers

PROTECTED ENVIRONMENT
Two-forest Active Directory (one parent domain, two child domains)
Windows servers, Entra ID, Microsoft 365
Legacy applications using NTLM and LDAP

THE CHALLENGE:

The organisation needed to strengthen its identity security posture across its legacy infrastructure and hybrid Active Directory environment. This initiative aimed to reduce risk exposure from unmanaged service accounts and enforce MFA for high-risk user access. It also sought to ensure consistent protection for a constantly changing network of internal staff and thousands of external advisers operating across unmanaged endpoints.

CUSTOMER OVERVIEW

About

This UK-based financial services organisation provides wealth, mortgage, investment, and protection advice through a nationwide network of independent advisers. With a centralised operations team and unified technology infrastructure, the organisation supports thousands of distributed users across a complex identity environment while ensuring secure access to critical business services.

Environment

The organisation operates a hybrid environment built on legacy on-prem infrastructure and multi-domain Active Directory (AD). It manages two forests, including one parent and two child domains, alongside a separate testing forest that does not have a trusted relationship with the production environment. The ecosystem includes Microsoft Entra ID, Windows servers, and Microsoft 365, with many business-critical applications relying on New Technology LAN Manager (NTLM) and Lightweight Directory Access Protocol (LDAP) authentication. Thousands of users, both internal staff and external advisers, access resources across managed and unmanaged devices.

Why now:
Responding to growing identity risk and legacy system exposure

With increasing reliance on legacy on-premises infrastructure and externally accessible systems, the organisation faced mounting pressure to modernise its identity security controls. The team had limited visibility into how Active Directory service accounts were being used, including what resources they were accessing, how frequently, and from which systems. They also needed to enforce access policies across older applications and non-managed adviser devices. As identity-based threats continued to expand and operational complexity increased, the organisation sought a solution that could deliver modern protection capabilities without disrupting business operations or rewriting applications.

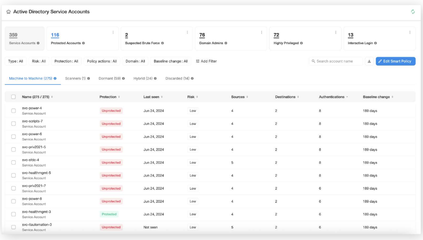
Challenge 1: Visibility and control of unmanaged service accounts

Identity risk from unmanaged service accounts

The organisation had limited visibility into their service accounts which were scattered across multiple forests and domains within a complex AD environment. Many of these accounts lacked clear ownership, had not undergone password rotation in years, or were deeply embedded in legacy processes. Without visibility into how they were used or where they were configured, the organisation could not accurately assess risks associated with each account, safely remove dormant accounts, or apply any access controls. These unmanaged identities posed a growing risk of lateral movement and credential misuse.

Gaining end-to-end visibility and control of service accounts

As a long-standing managed security service provider to the organisation, ITC Secure (ITC) guided the IT team to identify blind spots, including the adoption of Silverfort's Identity Security Platform. This collaboration helped to accelerate deployment and ensure the solution aligned with both technical and operational goals. With Silverfort, the organisation gained end-to-end visibility into more than 550 on-premises service accounts, including many dormant and previously undocumented identities. The security team classified accounts based on usage patterns, removed those no longer in use, and applied virtual fencing policies to limit active service accounts to specific, approved access paths. This approach significantly reduced the identity attack surface while maintaining operational continuity, without requiring any infrastructure changes or rewriting legacy application code.



The company's active directory service accounts dashboard in Silverfort displays all detected service accounts, including name, source, destination, number of authentications, risk score, baseline change and other account info.

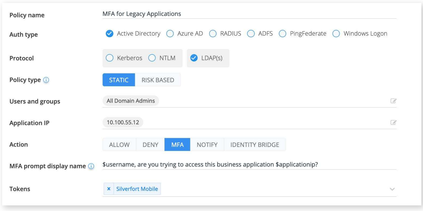
Challenge 2: Enforcing identity security controls across a distributed AD with legacy protocols and external users

Access control gaps across internal and external users

The organisation needed to enforce consistent access policies for both internal employees and a large network of external users, many of whom accessed legacy systems from unmanaged or personal devices. Critical applications still relied on outdated authentication protocols, such as NTLM and LDAP, which made it difficult to enforce modern security controls like MFA. With thousands of users operating across a complex environment, the lack of protocol-level enforcement created significant risk exposure – especially for systems accessible over the internet.

Enforcing MFA protection across legacy applications

With Silverfort, the organisation enforced MFA protection for high-risk authentication activity across NTLM and LDAP-based applications without modifying user workflows. This enabled the IT team to implement modern identity security controls even on legacy systems that did not support native MFA integration. By gradually applying access-based policies and monitoring access behaviour through Silverfort's Access Intelligence, the team could phase rollout across user groups, reducing disruption while strengthening security posture across the hybrid environment.



The company's active directory service accounts dashboard in Silverfort displays all detected service accounts, including name, source, destination, number of authentications, risk score, baseline change and other account info.

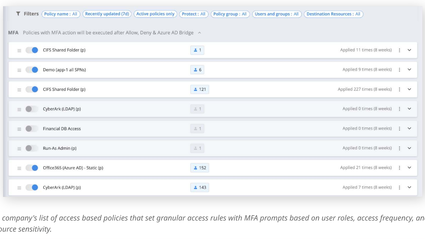
Challenge 3: Deploying identity security controls without operational disruption

Balancing protection with day-to-day operations

With thousands of users, including external advisers operating across varied device types, the organisation needed to strengthen identity security without introducing friction that could interrupt day-to-day business operations. Deploying access controls at scale carried the risk of authentication failures, increased helpdesk tickets, or unintended downtime. The internal team also had to maintain service continuity across legacy systems and ensure new policies would not interfere with business-critical workflows.

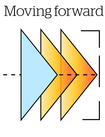
Fast, frictionless deployment with immediate results

Silverfort's unique architecture enabled the organisation to deploy identity security controls rapidly without modifying legacy applications. The IT team gained visibility into authentication activity and started to roll out access-based policies in a phased approach, enabling them to enforce MFA protection and service accounts virtual fencing with minimal disruption. This approach helped maintain user productivity while significantly improving organisation's identity security posture. Throughout the rollout, ITC provided technical and best practice guidance, helping the internal team to configure access policies and reduce operational friction.



The company's list of access based policies that set granular access rules with MFA prompts based on user roles, access frequency, and resource sensitivity.

Moving forward



What began as a service account discovery and MFA enforcement initiative evolved into a broader identity security transformation. With complete visibility, granular access-based policy control, and adaptive access enforcement in place, the organisation significantly reduced its exposure to identity-based threats—without requiring changes to legacy applications or disrupting users.

Looking ahead, and with ITC's continued support, the organisation plans to expand coverage by integrating Microsoft Teams to support step-up MFA for privileged users during PowerShell and remote desktop protocol (RDP) access. They also intend to onboard cloud-based non-human identities into Silverfort's protection model to ensure consistent policy enforcement across on-premises and cloud environments.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more

About ITC

ITC Secure (ITC) is an advisory-led cyber security services provider and a Microsoft Solutions Partner with designations in Security, Modern Work, and Infrastructure. The company has a 25+ year track record of delivering business-critical services to over 300 global blue-chip organisations, bringing together the best minds in security, a relentless focus on customer service, and advanced technological expertise to help businesses succeed. With its integrated delivery model, 24×7 fully managed state-of-the-art Security Operations Centre, and customer-first mindset, ITC works as an extension of its customers' teams to accelerate their cyber maturity – safeguarding their digital ecosystem, securing their business, and their reputation. ITC serves global organisations from its locations in the UK and US with a world-class team of cyber consultants, technical designers, and cyber experts. The company is an active member of the Microsoft Intelligent Security Association (MISA). ITC is also the winner of the 'Cyber Security Company of the Year 2022' award, 'Customers at the Heart of Everything 2022' award, Best WorkplacesTM 2022, Best WorkplacesTM in Tech 2022 and Best WorkplacesTM for Wellbeing 2023.

Learn more