Silverfort | BlueFort Security

CASE STUDY

NHS trust strengthens identity security posture and compliance by protecting patient services

BASED
London, UK

INDUSTRY
Healthcare (NHS)

PROTECTED ACCOUNTS
4,000+ users
100+ service accounts

ENVIRONMENT
Domain controllers: 6
Core on-prem apps: 12+
Privileged admin tools:
PowerShell, CLI, RDP, VPN

THE CHALLENGE:

The NHS trust needed to modernise its identity security stack to protect patient services. This effort aimed to meet evolving CAF and DSPT compliance standards and reduce risk exposure from unprotected service accounts and privileged users.

CUSTOMER OVERVIEW

About

The London-based NHS trust is one of the largest healthcare providers in the UK, serving over one million residents across multiple boroughs. As a world-class teaching hospital and specialist care provider, the trust plays a critical role in delivering life-saving services to its community.

Environment

The Trust operates a hybrid environment with legacy on-prem infrastructure, Active Directory (AD), and multiple core clinical and administrative applications. Their ecosystem includes 6 domain controllers, 100+ service accounts and thousands of end users and clinical staff accessing resources through VPN, RDP, PowerShell, and CLI tools.

Why now: Responding to compliance pressure and evolving threats

In the wake of the high-profile Synnovis ransomware attack in 2024 and the introduction of stricter NHS cyber regulations, the NHS trust was under mounting pressure to strengthen identity hygiene and implement modern access controls. Constrained by limited internal resources, the IT team looked for a scalable solution that would ensure compliance with the Cyber Assessment Framework (CAF) and the Data Security and Protection Toolkit (DSPT)—all while minimising disruption to clinical operations.

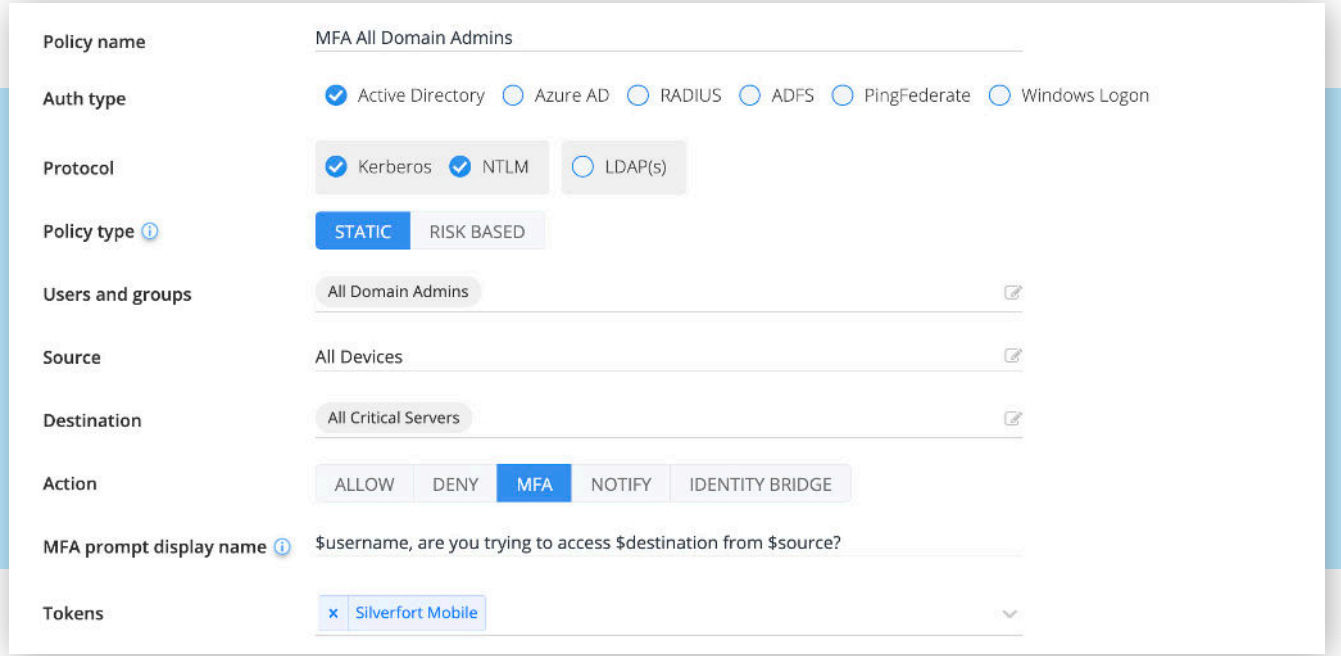
Challenge 1: Meeting CAF and DSPT identity security requirements

Compliance pressure and identity risk

The NHS CAF and DSPT compliance regulations introduced stricter identity security requirements, including multi-factor authentication (MFA) for privileged users, risk-based access controls, and visibility into authentication activity. In response, the NHS trust needed to modernise its access controls across their users and environments to comply with these new regulations. Identity security had become a critical concern, particularly for privileged users and non-human identities (NHIs), yet legacy systems lacked the capabilities to enforce robust access policies with MFA. The challenge was further complicated by limited visibility into authentication activity, making it difficult to demonstrate compliance readiness or protect against lateral movement.

Meeting CAF and DSPT requirements

As a long-standing cybersecurity partner of the Trust, BlueFort Security guided the IT team in adopting Silverfort's Identity Security Platform. This enabled the NHS trust to enforce MFA for over 4,000 users across all critical access points, including on-prem applications, VPN, PowerShell, and CLI, without adding operational overhead. Silverfort also provided full visibility into authentication activity and automatically discovered privileged users and non-human identities (NHIs), allowing the IT team to enforce granular access controls for privilege users and service accounts. With these capabilities in place, the Trust strengthened its compliance posture under CAF and DSPT and significantly improved identity protection, all without critical day-today hospital operations.



The company's MFA policy requires all access requests by domain admin accounts to be verified with MFA. During Kerberos or NTLM authentications, they see which critical server the admin is trying to access and the ID address of users

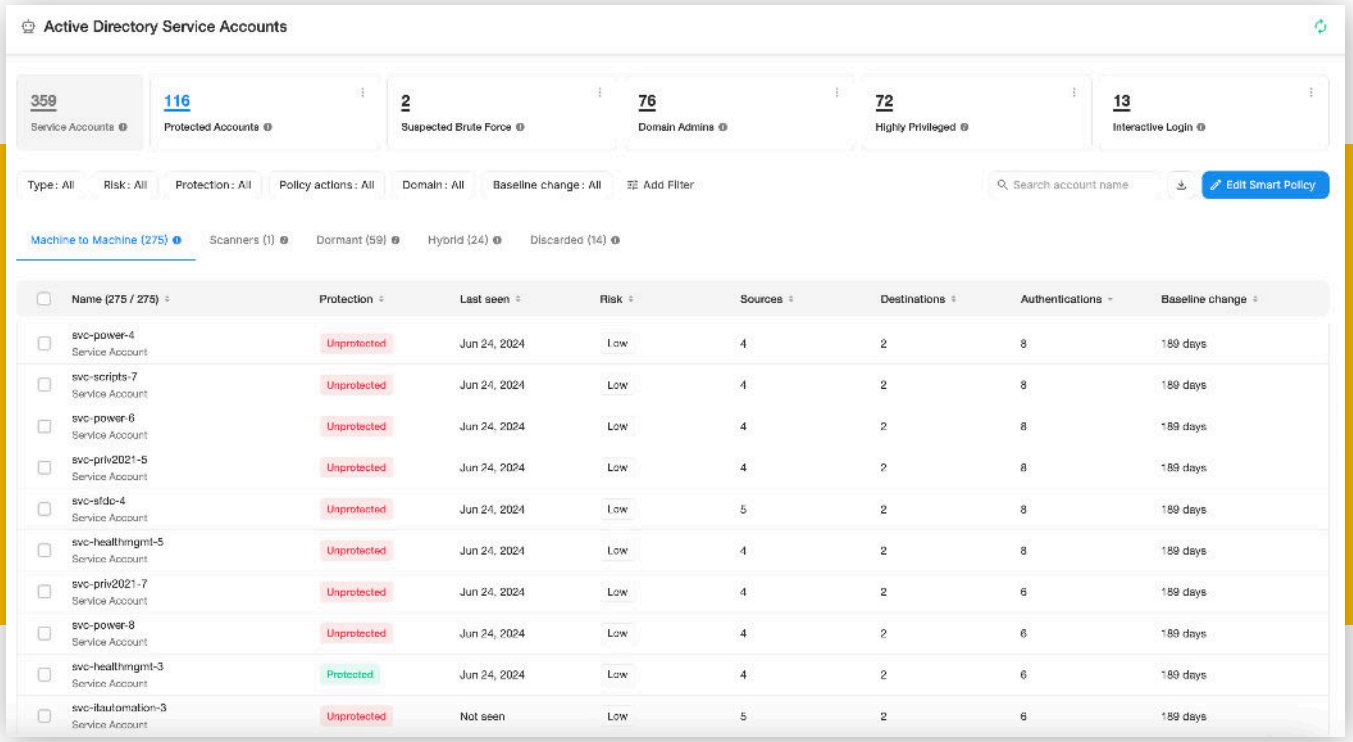
Challenge 2: Visibility into service accounts

Limited visibility into authentications of service accounts

The Trust had limited visibility into the ability to monitoring authentication flows, tracking service account activity, and detecting of stale users or identities with excessive privileges. In particular, unmanaged or legacy service accounts posed a serious risk of lateral movement, especially in clinical systems where automation scripts or third-party integrations were common. Without a way to see or manage these accounts, the team couldn't effectively secure their environment.

Gaining end-to-end visibility into service accounts with Silverfort

With Silverfort, the NHS trust gained full visibility into every authentication request across users, systems and NHIs. Silverfort automatically discovered 100+ service accounts and provided insights on where and how they were being used, including last activity, source and destination, and associated risk levels. This visibility enabled the IT team to clean up overprivileged accounts, detect suspicious behaviour, and significantly reduce identity risk.



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.

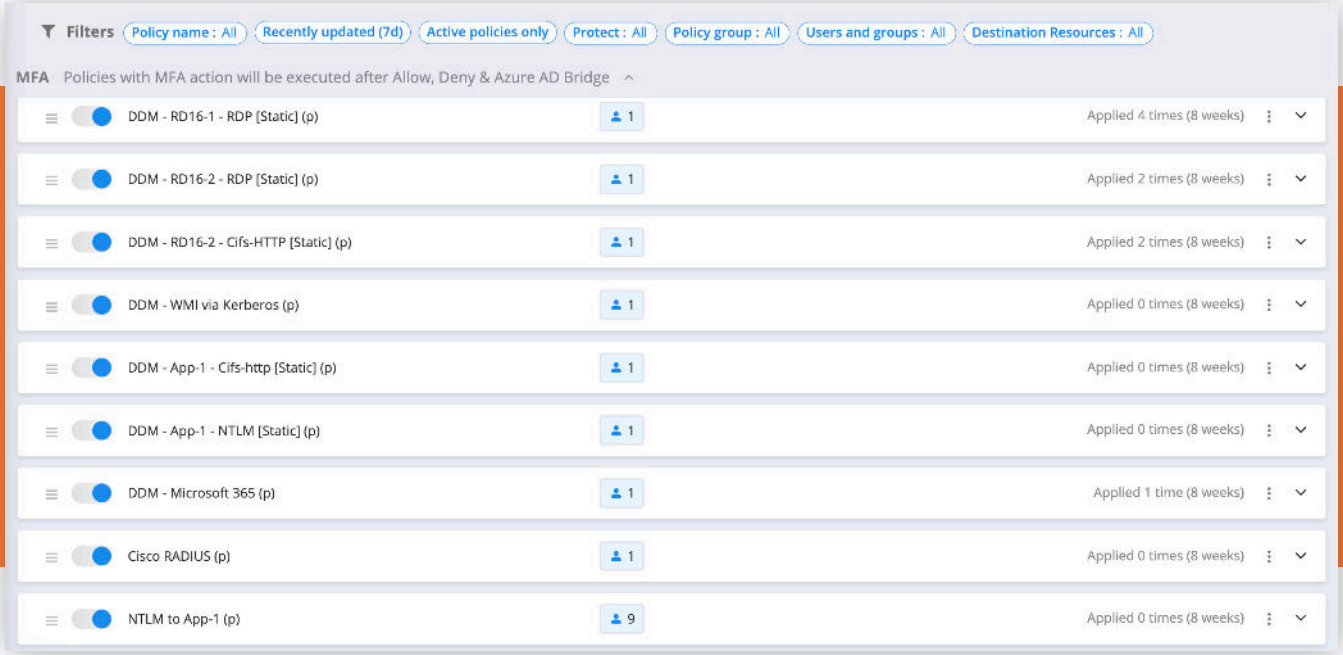
Challenge 3: Deploying identity security controls without disrupting patient services

Strengthening identity security controls without care delivery disruption

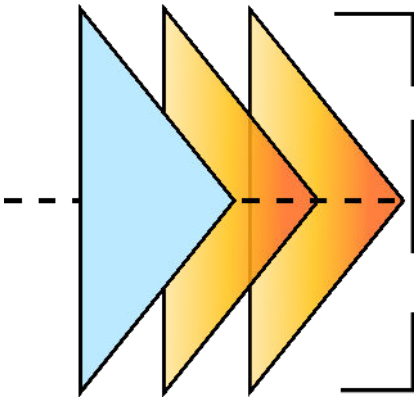
One of the most pressing concerns for the NHS trust's IT team was how to strengthen identity security posture without disrupting day-to-day critical hospital operations. With a lean security team and thousands of clinical users, any major deployment carried the risk of user friction, helpdesk tickets, or downtime that could affect patient care directly. The IT team needed a solution that could be deployed rapidly and provide immediate value without requiring endpoint agents or changes to user workflows.

Fast and seamless deployment with Silverfort and BlueFort Security's Evolve Program

Silverfort's unique architecture enabled the NHS trust to quickly replace its legacy MFA solution with minimal disruption to hospital operations. By working together as part of BlueFort's Evolve services program, the team deployed Silverfort's Identity Security Platform in just three weeks during the winter holiday period and successfully migrated 88% of users before staff returned. This fast, low-friction rollout was made possible by Silverfort's seamless user experience and flexible policy engine, which allowed the IT team to strengthen identity security controls without straining internal resources. BlueFort Evolve services ensure the Trust is supported throughout the entire tool lifecycle. After deployment, BlueFort continues to manage, optimise, and provide ongoing support to maximise performance and value.



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 targeted MFA tool deployment quickly evolved into a broader identity security transformation. With Silverfort, the NHS trust was able to meet with CAF and DSPT requirements, significantly reduced identity security risk, and gained end-to-end visibility into authentications activity across all users and resources, including on-prem service accounts.

The deployment was completed without disrupting hospital operations, and the IT team is now equipped with granular policy-based controls, real-time monitoring of all the authentications, and complete coverage of privileged access. With Silverfort in place, the NHS trust has laid the foundation for a proactive identity security strategy that protects critical and sensitive patient services and strengthens resilience against identity-based threats.

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver an end-to-end identity security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surfaces, and enforce security controls inline to stop lateral movement, ransomware, and other identity threats.

About BlueFort Security

BlueFort is the UK's leading Security Solutions Provider (SSP), trusted since 2007 to help organisations operate securely in an increasingly complex digital world. BlueFort protects hundreds of organisations and millions of users through solutions aligned with globally recognised security and compliance frameworks — from NIST, ISO 27001, and Cyber Essentials Plus to CIS Controls, NIS2, SOC 2, DORA and the UK's NCSC guidelines. Their expertise begins with robust identity & access management and advanced cloud security, then extends across the full landscape of cybersecurity, including operational technology (OT) security, data protection, threat detection and response, compliance, and the safe adoption of AI tools. BlueFort Security is a trusted cybersecurity partner and a Crown Commercial Services and G-Cloud 14 supplier.