Silverfort | CSTEM

CASE STUDY

How NHS Blood and Transplant secured privileged access to protect patient-critical services

BASED
Bristol, UK

INDUSTRY
Healthcare (NHS)

USERS
7,000+ users
Hundreds of service accounts

ENVIRONMENT
Active Directory
Entra ID with MFA and conditional access
Corporate SIEM

NHS Blood and Transplant

NHS Blood and Transplant (NHSBT) is a critical part of the UK's National Health Service, responsible for supplying blood to hospitals in England and managing organ donation across the entire UK. Its work underpins patient care nationwide, ensuring that vital treatments and transplants are delivered safely and on time.

THE CHALLENGE:

Protect privileged access and legacy infrastructure without disrupting critical patient services

- Inability to enforce MFA protection on domain admins authentications in Active Directory (AD)
- Lack of visibility into service accounts, including shadow accounts
- Dependence on legacy-heavy, risk-averse environment with limited ability to apply modern security controls

THE SOLUTION:

Achieved compliance readiness, secured privileged access for domain admins and gained visibility into service accounts

- Enforced MFA protection across all privileged access for domain admins within AD
- Gained visibility into hundreds service accounts and safely removed dormant accounts
- Strengthened compliance with NHS Data Security Protection Toolkit (DSPT) and Cyber Assessment Framework (CAF) frameworks

The challenge: Lack of MFA protection and visibility left weak security controls

As a national healthcare organisation, NHSBT is responsible for maintaining the continuity of life-critical services across the UK. Its legacy and complex AD environment limited its ability to secure privileged and service accounts, creating a risk that disruptions of the critical patient services could have direct consequences on patient safety.

"The biggest security gap for us was that we were unable to provide multi-factor authentication for our domain administrators using what we already had in place. There's a push within the NHS to secure critical infrastructure and privileged identities with MFA, and that was a gap we simply couldn't close."

— Jakub Witkowski,
Technology Services Engineer – IAM

Limited visibility into service accounts created an additional security gap. Strict regulatory processes in place, made it difficult to disabling dormant accounts or identifying the owners of inherited accounts from the old projects, making it hard to apply any modern controls.

"We have some computers and servers in place which go back almost 20 years. Many of the service accounts are still tied to those systems, and trying to disable them or apply modern controls is difficult when ownership isn't clear. If you try and find out who owns a service account from 20 years ago, it's almost impossible, and when you try to disable it, people push back saying it might break something," – said Daniel Bhatoa, Technology Services Engineer – Networks, Security & IAM

Finding the right identity security platform

NHSBT's IT team recognised the urgent need for a solution that could enforce MFA on privileged accounts in AD and bring visibility into service accounts across its legacy on-prem environment. Alternatives on the market were often heavy, complex, or required agents' deployment on every endpoint – an approach that would have been unmanageable across thousands of resources.

NHS Blood and Transplant first connected with Silverfort through C-STEM, a Managed Service Provider and trusted partner of other NHS trusts. Around that time, the organisation faced mandatory MFA enforcement requirements as part of the transition from the NHS Data Security Protection Toolkit (DSPT) to the Cyber Assessment Framework (CAF). C-STEM recommended Silverfort, part of their CloudSMART Solutions for Healthcare, as a best-of-breed solution that aligns closely with the security needs and priorities of NHS organisations. Acting on this recommendation, the NHSBT team met with Silverfort during the Gartner Conference. Following a successful discussion at the event, the organisation re-engaged with C-STEM to arrange a Proof of Concept (POC).

C-STEM coordinated a successful workshop and POC, demonstrating how Silverfort could close critical compliance gaps without the overhead of traditional tools. **As the first NHS trust to test Silverfort Identity Security Platform, NHSBT run a pilot, positioning the project as a strategic benchmark for the wider NHS community.**

"We wanted a solution focused on Active Directory and privileged accounts, not a big Swiss Army knife that tried to do everything but didn't specialise in anything. Silverfort stood out because it delivered exactly what we needed – MFA for domain administrators and the ability to secure service accounts – without unnecessary complexity."

— Jakub Witkowski,
Technology Services Engineer – IAM

The solution: MFA enforcement for domain admins with full service accounts visibility

After the POC, NHSBT rolled out Silverfort across its hybrid environment with the support of C-STEM. Its IT team quickly was able to enforce MFA protection to all domain admins to secure RDP access and other key legacy protocols with minimal disruption, closing a long-standing compliance gap.

"From a deployment perspective, the deployment was very easy and straightforward. We had guidance every step of the way, and even when configuration questions came up, the support team jumped on calls with us straight away. The focus for us was enforcing MFA for domain administrators – something we simply couldn't do before. Silverfort gave us that control with minimal disruption, and compared to other vendors we've worked with, the rollout was exceptional."

— Jakub Witkowski,
Technology Services Engineer – IAM

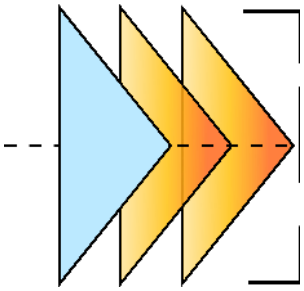
"With 7,000 servers and desktops, the overhead of installing agents would be huge. At that scale you're talking about patching, maintaining, and updating thousands of machines just to keep MFA running – and if even one device wasn't covered, it would leave a back door open. With Silverfort, we just needed to install on domain controllers. It's far more efficient and a smarter way of doing it," — said Daniel.

Another focus point for NHSBT was addressing the risks posed by service accounts. With hundreds of service accounts in use, Silverfort provided end-to-end visibility into authentication activity, highlighting heavily used accounts and identifying dormant ones that could safely be removed. The clean-up process is ongoing and directly tied to meeting CAF compliance requirements.

"Silverfort showed us which service accounts were authenticating, and which weren't. We analysed them and removed the ones that were dormant, which gave us confidence we weren't breaking anything. Normally we'd have to dig through PowerShell scripts, event logs, and SIEM dashboards to piece this together, but Silverfort brought it all into a single pane of glass. On top of that, it flagged shadow admins and unusual authentication patterns that we wouldn't have spotted otherwise. For the first time, we could start managing service accounts properly instead of just leaving them to accumulate"

— Daniel Bhatoa,
Technology Services Engineer – Networks, Security & IAM

Looking ahead: Expanding into PAS and advanced identity controls



NHSBT is now focusing on the next stage of its identity security strategy, with the immediate priority on completing the clean-up and securing of highly privileged service accounts, ensuring they can be managed without disrupting critical patient services.

As a next phase, NHSBT is interested in implementing Silverfort PAS solution to manage contractor access to medical devices, extending the controls already in place for privileged accounts. The IT team also plans to explore risk-based access policies to provide more dynamic protection, alongside longer-term initiatives such as reducing excessive admin rights and introducing biometric authentication like Windows Hello to strengthen identity security across the workforce.

"Once we've secured the service accounts and domain administrators, we'll have delivered on the two crucial needs this project was deployed for. From there, we want to look at risk-based policies once the product is fully deployed and tested, and then potentially explore privileged access controls to scope admin rights down to what's really needed. Longer term, we're also looking at biometric authentication, which would be another important step in maturing our identity security."

— Jakub Witkowski,
Technology Services Engineer – IAM

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, analyse exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

About C-Stem

C-STEM is a Zero Trust Architecture Managed Service Provider (MSP) dedicated to enabling secure, resilient, and patient-centric digital transformation in healthcare. Through our CloudSMART Solutions for Healthcare, we help organisations evolve from a fragmented digital infrastructure into a unified digital ecosystem. This approach harmonises existing investments rather than replacing them, accelerating time-to-value while improving detection, compliance and response. It also delivers cost savings and enhances overall workforce productivity.