Silverfort | CSTEM

ENHANCING SECURITY AT TRINITY COLLEGE CAMBRIDGE:

Strengthening MFA and service account protection with Silverfort

BASED	INDUSTRY	USERS	ENVIRONMENT
Cambridge, UK	Higher Education	1,000+	On-prem Active Directory, Azure Entra ID, privileged admin accounts and legacy applications

Founded by Henry VIII in 1546, Trinity College is one of 31 constituent colleges of the University of Cambridge and counts 34 Nobel Laureates amongst its members. Today Trinity is a thriving international community of 750 undergraduates and 357 postgraduates, 190 fellows and 350 staff, renowned for its excellent teaching and research.

TRINITY COLLEGE CAMBRIDGE

THE CHALLENGE:

Comprehensive identity security for all Active Directory users

- Enforce MFA on privileged accounts in on-prem infrastructure
- Gain visibility and control over service account behaviours
- Implement security measures without disrupting existing IT operations

THE RESULTS:

Enhanced protection for privileged and service accounts

- MFA enforcement extended to on-prem privileged accounts
- Improved visibility into service account activities and risks
- Seamless integration with existing Microsoft environment

The challenge: Strengthening on-prem infrastructure and service account management

Trinity College's IT and security team recognised several security challenges in their identity security strategy. While cloud-based applications were well-protected, their on-prem infrastructure lacked **MFA enforcement**, leaving privileged accounts vulnerable. **Service accounts, a critical part of their IT operations, also had limited oversight**, increasing the risk of misuse or compromise.

The IT and security team sought a **solution that would enforce MFA on all privileged users, provide visibility into service accounts, and integrate smoothly with their existing Microsoft environment without causing disruptions.**

> "Our privileged accounts and service accounts were a primary area of concern. We lacked visibility into service account behaviours, and our on-prem applications had no MFA support, leaving potential security gaps,"
>
> – Duncan Malthouse-Hobbs, Head of IT at Trinity College.

Finding the right identity security partner

C-STEM, a long-standing supplier to the Oxford and Cambridge University Colleges, conducted a thorough review of **Identity & Access Management (IAM) solutions** to address their specific challenges. As part of this due diligence, C-STEM gathered valuable feedback from a Cambridge College, confirming **Silverfort** was the right solution to provide **on-prem multi-factor authentication (MFA) and service account discovery.**

The opportunity to work with **Trinity College**—an early adopter of Silverfort—marked C-STEM's first collaboration with their IT and security team. This engagement allowed C-STEM to demonstrate its value as a partner, build confidence in the team's ability to successfully deliver security projects, and lay the foundation for a long-term, **trusted partnership**.

Trinity College selected **Silverfort** as its **identity security vendor**, drawn to its proven success in **seamless MFA enforcement, real-time authentication insights, and integration with Active Directory**. The **IT and security teams** began deployment with a **proof-of-concept (POC)** on a **single domain controller**, ensuring a smooth transition before expanding Silverfort campus-wide. Its ability to **analyse authentication requests in real time and enforce security policies** made the implementation **efficient and non-disruptive**.

The solution: Implementing MFA and service account protection with Silverfort

MFA protection and adaptive identity protection policies

As Head of IT Duncan Malthouse-Hobbs noted: "Silverfort has provided us with a strong solution that was easy to deploy and delivered immediate identity security benefits. Its ability to protect legacy applications with MFA has made it an invaluable tool in our cybersecurity strategy."

The implementation delivered key security capabilities:

Advanced risk-based authentication:

- MFA enforcement for access to sensitive resources from unfamiliar locations
- Detection and securing legacy authentication protocols to prevent unauthorised access

Command-line and RDP security enhancement:

- MFA verification for PsExec executions across network segments
- Enhanced authentication for PowerShell remote sessions, script execution and RDP connections
- Granular control over WMI command usage for system administration

IT Infrastructure Engineer Bryan Carpenter also validated the seamless deployment: "Rolling out Silverfort was incredibly straightforward. We quickly saw value in its ability to enforce MFA on legacy systems without requiring additional software."

Service account protection and lateral movement prevention

The implementation transformed Trinity College's service account management through:

Advanced risk-based authentication:

- Intelligent mapping of service account usage across multiple domains
- Continuous real-time monitoring of service account behaviour patterns
- Identification and remediation of dormant admin accounts
- Real-time detection and prevention of suspicious lateral movement attempts

The impact surpassed expectations, as Carpenter shared: "One of our team members was initially sceptical about Silverfort, but after seeing its impact, he became a strong advocate. It has not only helped secure our accounts but also revealed security gaps we didn't even know existed".

Through this implementation, Trinity College established effective identity security that balances protection with operational efficiency. Their partnership with C-STEM and Silverfort has been instrumental in achieving these outcomes.