NHS England: Multi-factor authentication (MFA) policy compliance with Silverfort

NHS organisations and contractors are being encouraged to implement multi-factor authentication (MFA) controls for all privileged users and services accessing critical systems and data. In order to reduce the number of exposed attack surfaces, especially identity-based attacks that utilise compromised credentials, this framework has been developed. According to this new policy, which was published at the beginning of 2023, UK NHS organisations are required to make every reasonable effort to comply as soon as possible.

Who does the MFA policy apply to

- NHS trusts and foundation trusts
- Integrated care boards
- Arm's length bodies of the Department of Health and Social Care
- Commissioning support units in NHS England
- Operators of essential services for the health sector in England as designated under the NIS Regulations
- genomics organisations as nominated by the Department of Health and Social Care

MFA challenges for NHS organisations

There is a lack of visibility within most NHS organisations regarding how privileged users are accessing critical assets, and which users and resources require MFA. Many critical NHS resources are legacy applications deployed into on-prem environments and are usually accessed remotely. Many legacy Electronic Patient Records (EPR) and on-prem health information technology systems were not designed to implement modern security controls such as MFA.
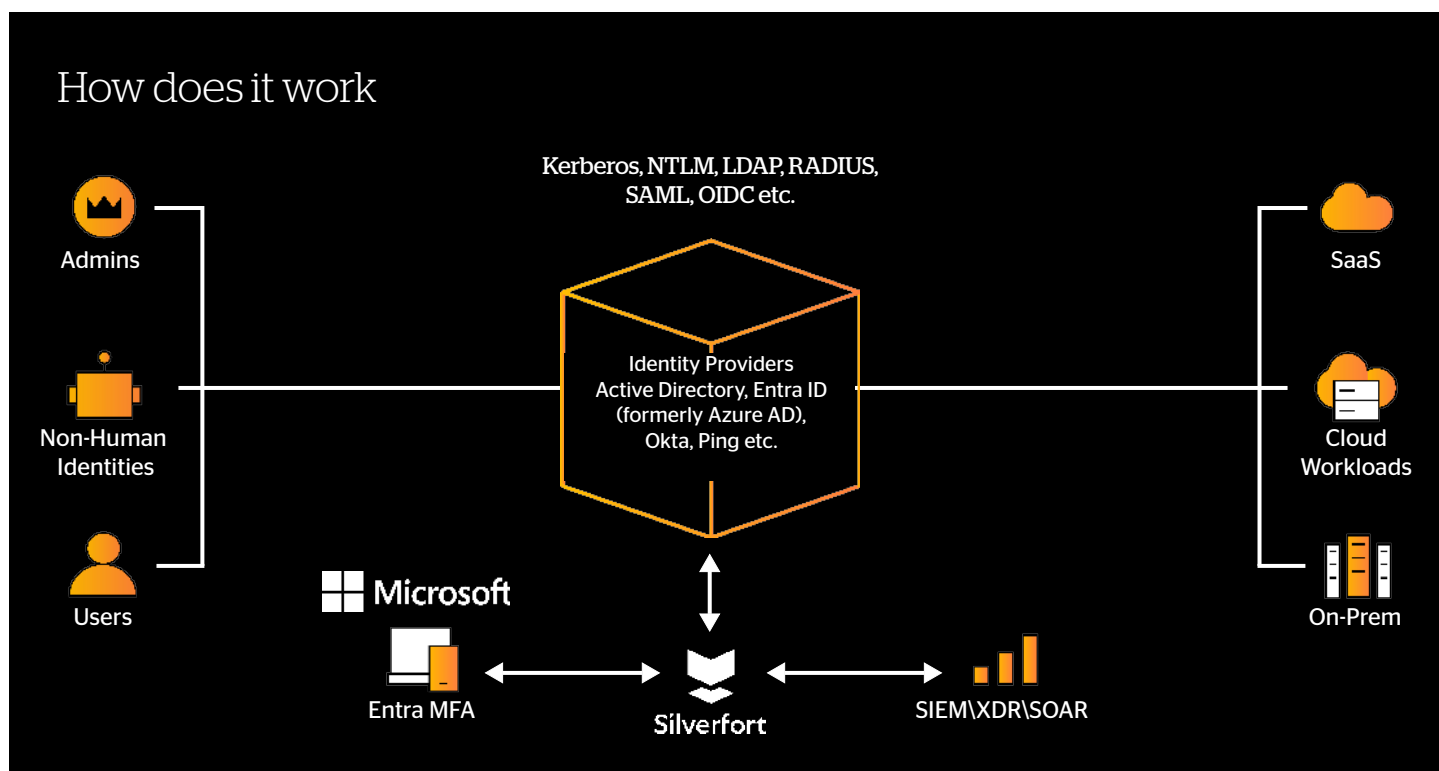
According to Microsoft, multi-factor authentication (MFA) can prevent more than 99.9% of account compromise attempts. Despite the fact that MFA is the ideal solution to prevent identity-based attacks in theory, its usability and flexibility challenges create friction during the adoption process by medical professionals. In healthcare environments, this can result in potential system failures.

The solution: Silverfort's Identity Security Platform

Silverfort enables NHS organisations to extend MFA protection to all environments and resources, whether cloud-based or on-prem, without making changes to applications or infrastructure. Silverfort integrates with existing IAM & MFA solutions, allowing NHS trusts to extends controls, such as Entra MFA across their hybrid environment. This enables modern MFA protection for any AD-authenticated resource, including legacy medical devices, clinical applications, file shares, and other systems that could not previously support MFA.

Silverfort evaluates every authentication request using identity, behavioural, and contextual signals through its risk engine, enforcing the appropriate access-based policy in real time. This prevents attackers from using compromised credentials to move laterally, escalate privileges, or spread ransomware. By enforcing MFA at the identity and authentication protocol layer, Silverfort provides NHS organisations with a unified security layer against identity-based threats across their hybrid environments.

How does it work

Kerberos, NTLM, LDAP, RADIUS, SAML, OIDC etc.

Admins

Non-Human Identities

Users

Identity Providers
Active Directory, Entra ID
(formerly Azure AD),
Okta, Ping etc.

SaaS

Cloud Workloads

On-Prem

Microsoft

Entra MFA

Silverfort

SIEM\XDR\SOAR

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.

Silverfort

silverfort.com