SILVERFORT

Identity Protection in Healthcare: Challenges and Solutions

Silverfort protects healthcare organizations by giving them full visibility into service accounts, extending MFA to all resources, including medical devices running legacy OSs, and blocking access through customized policies.

The healthcare industry carries the highest average cost of a data breach at nearly $11 million as of mid-2023, far exceeding the global average of $4.45 million. Over the past few years, more than 700 cases of large-scale data breaches (involving the loss of 500 or more health records) have been reported each year in the US alone.

Healthcare organizations are particularly vulnerable to identity threats, as losing access to patient information could be detrimental to patient treatment. In 2021, around 30% of cyberattacks in the healthcare industry caused emergency service disruptions, while a further 17% resulted in serious injury or harm (source: Statista).

What Makes Healthcare a Key Target for Identity Threats

Lack of Visibility of Service Accounts	Authentication in Legacy Systems Doesn't Support MFA	Highly Complex Identity Infrastructure
Only 10% of healthcare organizations have full visibility into their service accounts (source: Silverfort & Osterman Research), exposing them to security risks like lateral movement and ransomware.	Healthcare organizations rely heavily on Active Directory, with many still using Windows Server 2008 and Windows XP. Many overlook the unique security requirements of legacy systems, putting them at risk of breaches (source: HIMSS, HHS)	Healthcare identity infrastructure is large, fragmented and involves multiple security practices. For example, enforcing strict security measures on MPI or EMS users but not HR, or not updating legacy systems to avoid disruptions.

The Silverfort Way: Unified Identity Protection

Service Account Protection	MFA Everywhere	ITDR
Silverfort automatically identifies accounts with predictable and repetitive behavior as service accounts and generates policies accordingly. Each access attempt is compared with the policy and any deviations are blocked.	By integrating with Active Directory, all access requests are forwarded to Silverfort. This allows Silverfort to enforce MFA verification on all healthcare systems, including legacy systems, health information systems, HR, and command-line interfaces.	Silverfort provides real-time Identity Threat Detection and Response (ITDR) for every authentication and access attempt across all user, admin and service accounts, and for any resource, system, and authentication protocol.

Learn more about how Silverfort helps healthcare organizations solve their identity protection challenges.

Download our Full eBook