



Protect AD, legacy, and OT systems with Silverfort

Modern Identity Security for systems that can't be modified or replaced

Most enterprises run legacy and OT systems that can't be modernized and can't support modern Identity Security. They're a top target for attackers and a common source of compliance gaps. Silverfort protects them by enforcing MFA and access-based controls at runtime, with no changes and no downtime. Close the security and compliance gaps they leave behind. No rip-and-replace.

The hardest systems to change are the easiest to attack

Legacy and homegrown apps, OT and air-gapped systems run critical operations, but they were never built to support modern Identity Security controls. Many still authenticate to Active Directory (AD) over legacy protocols, including NTLM and LDAP. They can't be refactored, retired, or simply taken offline to fix that, so they stay exactly as they are. That's why 82% of organizations report still running significant legacy infrastructure that creates additional security risk.

The result:

- **Blind spots in MFA coverage:** the systems MFA never reached
- **Service accounts no one owns:** critical, highly vulnerable non-human identities (NHIs) running on legacy systems, unmanaged and unprotected
- **Environments outside identity controls:** OT and air-gapped networks with no internet connectivity, beyond the reach of cloud-dependent tools

And the stakes are rising. Legacy systems, especially AD, are the biggest cybersecurity risk in most organizations. Taking over AD gives attackers the broadest access across the business. Organizations used to hope attackers wouldn't find these blind spots, but AI-powered attacks find them easily. Compliance pressure is growing too. Auditors and insurers no longer accept exceptions, and a single unprotected system can fail a compliance audit or break a cyber insurance attestation. The systems most often left out are the ones that matter most: the manufacturing line, the core banking platform, the clinical systems that can't afford downtime.

How Silverfort closes the gap

Silverfort's patented Runtime Access Protection™ (RAP) technology integrates natively with AD and enforces Identity Security controls inline, at runtime. Legacy systems keep using their existing authentication protocols, unaware that Silverfort adds controls on top. Nothing needs to change, and protection extends even to OT and air-gapped networks.

- **Extend MFA protection to every resource and access path**
Enforce it on legacy and homegrown apps, command-line tools, OT systems, and Windows local accounts
- **Protect the service accounts these systems run on**
Gain full visibility into all AD service accounts with automated discovery, monitoring, and risk insights, and enforce virtual fencing to restrict how each one can be used, without password rotation.
- **Control what legacy systems can access**
Apply Zero Trust access policies and identity segmentation at the authentication layer, blocking credential misuse and stopping lateral movement at runtime.

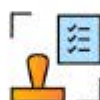


Key benefits



Reduce the risk of AD compromise

Protect the systems and service accounts most exposed to attack, so a single foothold can't turn into an AD takeover.



Pass audits and hold attestations

Prove that Identity Security controls are enforced across all systems auditors and insurers ask about, including the legacy and OT systems that used to be the exception.



Save time and cost on technical debt

Extend modern Identity Security to legacy systems without replacing applications, rewriting code, or interrupting the business.



Consolidate identity security from AD to AI

Start with legacy systems and expand to every identity, including humans, non-human identities, and AI agents, on-prem and in the cloud, from a single platform.

"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, IAM Engineer, NHS Blood and Transplant

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across cloud and on-prem environments. We are the first to deliver an end-to-end identity security platform that is easy to deploy and doesn't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls at runtime to stop lateral movement, ransomware, and other identity threats.