Silverfort

Solving key identity security challenges in manufacturing with Silverfort

The manufacturing sector is facing a significant surge in cyberattacks, with ransomware remaining one of the most prevalent threats. In 2024 alone, ransomware attacks on manufacturers increased by over 40%, with attackers targeting production lines, operational technology (OT), and supply chains to maximize disruption and extort higher ransoms.

This evolving threat landscape is compounded by the growing connectivity of manufacturing environments, which are rapidly shifting from isolated access to centralized Single Sign-On (SSO) via Active Directory (AD). While this transition boosts productivity and streamlines user management, it also broadens the attack surface, enabling identity-based threats to exploit the same AD infrastructure for unauthorized access.

The tried and tested solution against identity threats is comprehensive MFA protection across all users, systems, and environments. However, manufacturing environments introduce unique MFA deployment challenges, often leaving critical resources unprotected and vulnerable to attack.

What makes manufacturing institutions a key target for identity threats?

Legacy On-Prem Applications

Legacy applications were developed long before MFA technology was widely available and don't natively support its incorporation in their default authentication process.

Third-Party Access

Manufacturers rely on third-party software providers who regularly access their environment. Security teams often lack control over these users' devices and have limited visibility into their actions and external risks.

Hybrid IAM Infrastructure

Modern manufacturing environments span on-prem systems, multi-cloud workloads.This fragmentation limits security teams' visibility into user behavior, making it harder to detect malicious logins and trigger MFA step-ups.

How Silverfort solves identity security challenges in the manufacturing sector

Secure authentication to legacy apps

All user access requests are forwarded to Silverfort via its native integration with Active Directory. This includes authentications made via NTLM and Kerberos, so legacy servers can be protected with MFA.

Third-party access protection

Silverfort requires no agents on protected devices, enabling MFA on all access attempts including those by external vendors. This ensures only authorized users gain access and significantly reduces the attack surface.

Visibility into Hybrid Environments

Silverfort's integration with all IdPs, on-prem and in the cloud, enables it to monitor and analyze every user's full authentication trail context and extend MFA to the entire on-prem environment, including resources that couldn't be protected before.

Learn more about how Silverfort helps manufacturers solve their key identity security challenges.

Download the full eBook