SILVERFORT

Securing Manufacturing Environments with MFA

Silverfort enables manufacturers to overcome common identity protection challenges by enforcing adaptive access policies and advanced MFA protection across all manufacturing resources – including those that couldn't be protected before.

Manufacturers are more connected than ever, with a rapidly increasing number of manufacturing environments shifting from local user access to HMI, engineering workstations, and production apps to centralized SSO via Active Directory (AD). While the productivity advantages of this transition are clear, it also exposes their environments to a wide range of identity threats that leverage the same AD infrastructure for malicious resource access.

The tried and tested security solution against identity threats is to use comprehensive MFA protection across all users, systems, and environments. However, the nature of manufacturing production environments introduces unique challenges for MFA deployment, often leaving critical resources deprived of protection and exposed to attack.

Key Manufacturing Protection Challenges

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. To integrate MFA into a legacy application, organizations would need to make changes to the application's code, which could cause friction to their operational continuity and hence is generally avoided.

Third-Party Access

Manufacturers make extensive use of software that's supported and maintained by third-party providers who routinely access their environment. Typically, security teams have limited to no control over the security state of third-party users' devices and very limited visibility into their actions and the risks they are subject to beyond the manufacturer's environment.

Hybrid IAM Infrastructure

Manufacturing environments today comprise on-prem workstations and servers (for both the shop floor and the IT network), multi-cloud workloads, and SaaS applications. Fragmenting the different types of environments creates a disadvantage for security teams in having visibility into the full context of each user account's behavior, significantly reducing their ability to detect an attempted authentication as malicious and trigger an MFA step-up.

How Silverfort Solves Manufacturing Identity Protection Challenges

Legacy Applications

All IdPs including Active Directory forward every access request to Silverfort, including those made by legacy applications, enabling Silverfort to cover them with MFA protection regardless of whether the application supports MFA.

Third-Party Access

Silverfort does not require agents on the protected devices, enabling it to easily enforce MFA on access attempts to any resource, including ones made by external vendors.

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.

Want to learn more about how Silverfort solves key identity protection challenges for manufacturing organizations? Read our full eBook.