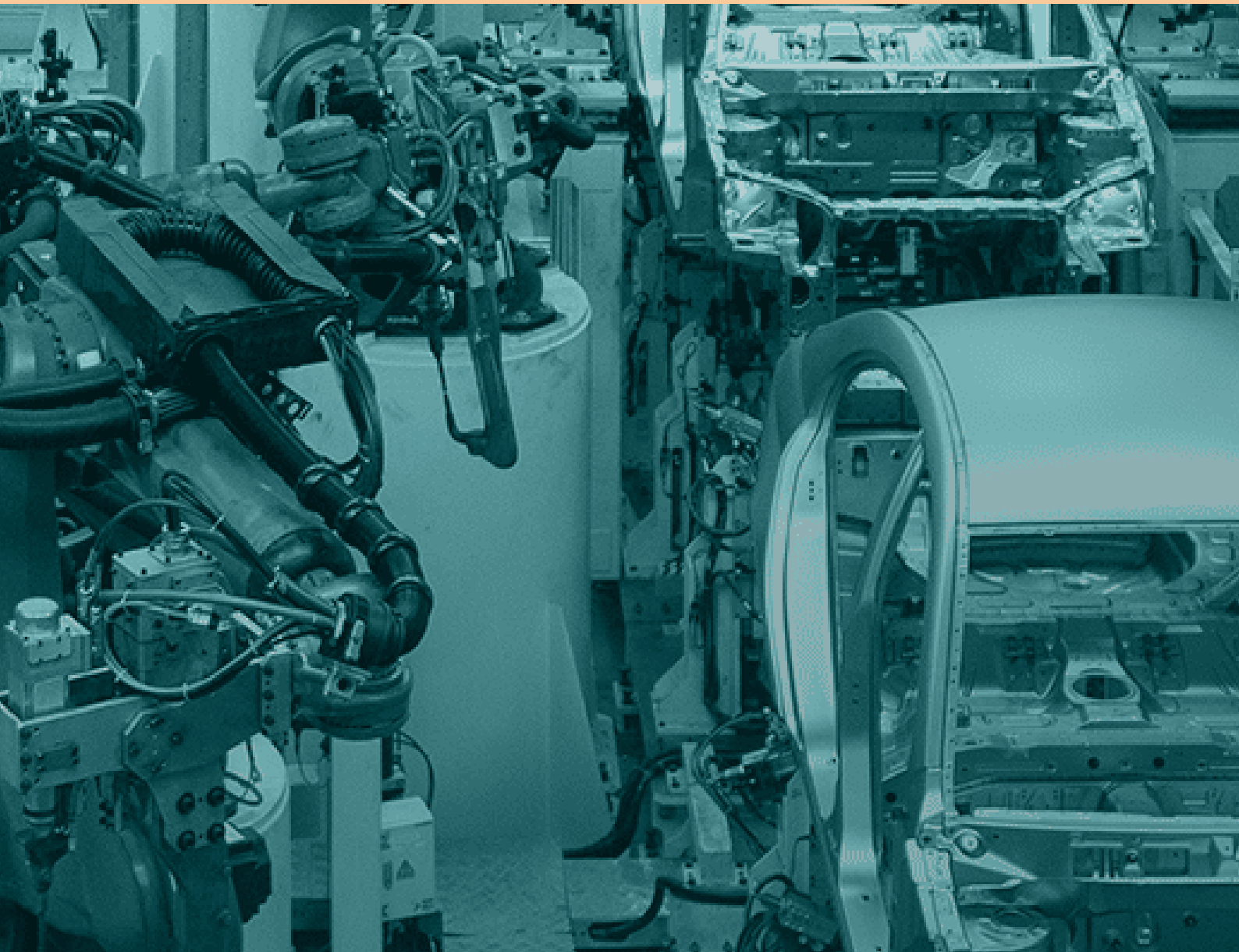
SILVERFORT

Top 5 Identity Protection Challenges for Manufacturing Companies

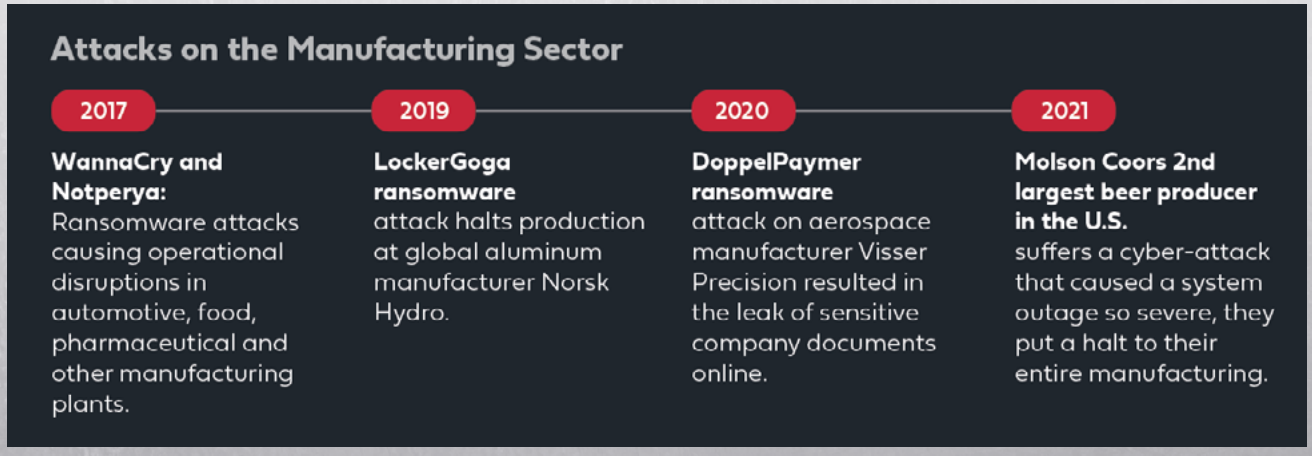


It is common knowledge that manufacturing is one of the most targeted verticals and that threat actors launch data theft and ransomware operations on manufacturing companies daily. What is less commonly known is that the rise of identity threats' part within the overall threat landscape collides with security weaknesses that are unique to this vertical, increasing manufacturers' risk exposure and the potential damage these attacks can cause.

In this collateral, you'll become familiar with the identity threats that manufacturing environments face, get to know the top five challenges they face when attempting to protect against them, and learn how Silverfort's Unified Identity Protection platform can assist identity and security teams to fully address these challenges and maintain their environments secure.

Manufacturing Threat Landscape

No sector is safe from the threat of incoming cyberattacks. This is especially true with manufacturing organizations for which the potential outcomes of a successful ransomware attack or data theft are severe due to a low tolerance for downtime and impact on production processes. IBM's X-Force 2022 Threat Intelligence Index showed that manufacturers were the most targeted industry due to a low tolerance for downtime and outdated security controls. Additionally, a Deloitte study highlighted that over 40% of manufacturing firms experienced a cyber-attack in the past year.



Manufacturers' physical operations and valuable data have attracted the attention of threat actors due to manufacturers' unwillingness to deploy modern technology across their environments which results in demanding ransomware often successful. This new approach has made it difficult for organizations to detect, prevent and respond to attacks across their hybrid environments.

Furthermore, adversaries are increasingly targeting manufacturers' employees to gain access to their critical credentials, data, and systems access. In manufacturing, employees' threat awareness is generally considered a weak link or the low-hanging fruit for adversaries to target and open the door to move laterally across a manufacturer's environment.

Manufacturing has an Identity Protection Challenge

Manufacturers are increasingly adding more entry points into their environments as well as adding partners with unprotected third-party devices. This leads manufacturing environments to be more exposed to incoming identity-based attacks which are utilizing compromised credentials to gain access to manufacturing enterprise resources.

Once a threat actor has gained access by utilizing compromised credentials, they'll gain complete access to different resources such as legacy applications and systems. This malicious access would be followed by either exfiltration of sensitive IP or extortion under threat of shutting down operations.

The typical manufacturer is not equipped with the proper identity protection controls to detect and prevent such attacks like in the scenario above where malicious actors authenticate with valid but compromised credentials. This is especially true when it comes to protecting legacy applications.

The Security Challenges that Manufacturers are Facing

The different identity protection challenges that manufacturers are facing should be a top priority for all manufacturing organizations. Here are the five most concerning identity protection challenges that manufacturers are facing.

Legacy Applications Can't be Protected with MFA

Legacy applications were developed long before MFA technology was widely available, so they 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 might cause friction to their operational continuity and hence is generally avoided. Furthermore, manufacturing applications are typically on-prem and authenticate to Active Directory over NTLM and Kerberos protocols, which also do not support MFA. Without MFA protection, legacy applications' infrastructure and sensitive data are exposed to any adversary that has successfully gained initial access to the environment and obtained compromised credentials.

Restricting Third-Party Access

Manufacturers make extensive use of software that's supported and maintained by third-party providers that routinely access their environment to perform various maintenance,

administration, and management purposes of industrial processes. However, the manufacturer's security team has 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 their direct connection to its environment. As a result, threat actors often target the supply chain rather than the direct objective, as they rightfully assume it would be easier to accomplish. Compromising the third-party vendor's user credentials allows attackers to gain access to the manufacturing environments, especially when least-privileged access is not enforced.

Hybrid Environments

A typical manufacturing environment today comprises on-prem workstations and servers (for both the shop floor and the IT network) and 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. Moreover, the core part of this environment, such as the on-prem Active Directory one, doesn't support MFA protection at all. Malicious actors exploit this weakness of the siloed visibility of each environment, to perform hybrid lateral movement attacks to move between the on-prem and the cloud uninterruptedly.

Shared Accounts

The common practice of different employees using the same credentials to access an application or machine is often implemented across manufacturing organizations. For example, ten production employees use the same user credentials to access a machine or a production application. While having one main account for several employees might be more comfortable, it creates major visibility and security risks. A malicious actor only needs to trick one of the employees to gain access to this account and move laterally across the manufacturer environment.

IT/OT convergence

Information technology (IT) and operational technology (OT) have always worked independently in manufacturing. From the various physical environments and applications, IT and OT systems were not designed to communicate with each other. As this gap continues to narrow and these networks become more connected, the attack surface for cyber threats is expanding significantly. IT/OT convergence allows OT devices to be accessible from the IT network by lateral movement. This triggers malicious actors to target manufacturers as the simple use of compromised credentials from the IT team can allow them to move laterally across the OT environments.

The Solution: Silverfort's Unified Identity Protection MFA

Silverfort has pioneered the world's first Unified Identity Protection platform that **extends MFA and modern identity security to any user and resource, including the legacy applications** that couldn't be protected before.

The Silverfort Unified Identity Protection Platform integrates with all Identity Providers (IDP) in manufacturers' hybrid environments to perform continuous monitoring, risk analysis, and adaptive access policies on all access attempts, made by all users, to all manufacturing resources.

With Silverfort, access to resources is never granted based on credentials alone. Rather, Silverfort's risk analysis determines whether or not to allow access, augment the authentication with MFA verification, or block the access attempt altogether.

Apart from the operational simplicity entailed in managing only one solution, Silverfort's architecture enables manufacturers to have full MFA coverage across all on-prem and cloud resources in their hybrid environment. In this way, Silverfort overcomes all the challenges we've described in the previous sections:

- **Legacy applications** – the IdP forwards Silverfort all access requests, including those made by legacy applications, enabling Silverfort to protect them with MFA, regardless of whether the application supports MFA.
- **Third-party access** – Silverfort doesn't require the installation of 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 the full authentication trail context of every user and extend MFA to the entire on-prem environment, including resources that couldn't be protected before.
- **Shared accounts** - Silverfort's integration with different MFA tokens allows admins to enroll different tokens for one account to multiple users. Silverfort provides FIDO2 key tokens to solve this issue.
- **IT-OT Convergence** - Silverfort enforces secure authentication and access policies across corporate networks, industrial networks, and cloud environments, including sensitive IT and OT systems that were considered 'unprotectable' until today.

To learn more about how Silverfort can help your manufacturing environments, request a demo here.