Silverfort

# Solving key identity security challenges in mining with Silverfort

The mining industry is undergoing rapid digital transformation, bringing IT and OT environments closer together that ever before. As these systems converge and become more accessible, particularly by third-party vendors, new cybersecurity risks emerge – especially identity-based threats.

Traditionally, isolated networks are now increasingly connected to support operational efficiency, remote maintenance, and real-time data insights. However, this shift introduces critical security risks. Air-gapped OT networks are now exposed to ransomware due to IT/OT integration, and attackers can leverage compromised credentials to move laterally once inside the network. At the same time, many mining organizations are migrating from standalone access methods to Active Directory (AD) and Single-Sign-On (SSO), expanding the blast radius of credential-based attacks.

To stay resilient, mining organizations must strengthen identity security across all systems and user types, ensuring every access attempt is continuously verified, monitored, and secured.

## What makes mining sector a key target for identity threats?

### IT/OT convergence and third-party access

With IT and OT networks becoming more integrated, mining operations increasingly rely on third-party vendors for remote maintenance and monitoring. This creates new access points to internal systems, and regular data exchanges between IT and OT environments make it harder to maintain proper network isolation.

### Air-Gapped networks exposed to ransomware

As air-gapped networks has gained more connectivity, attackers are finding new access paths to deploy ransomware into OT environments. Critical assets, including HMIs and engineering workstations, become prime targets for attackers, leading to downtime, data loss, and financial damage.

### Shifting to Active Directory Single Sign-On

Migrating from standalone authentication to AD-based SSO has improved OT access but also introduced risk. A single compromised account can grant attackers lateral movement across both IT and OT systems, amplifying the potential impact of a breach.

## How Silverfort solves identity security challenges in the mining sector

### Secure Third-Party Access

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.

### FIDO2 token support prevents lateral movement attacks

By supporting FIDO2 tokens, Silverfort strengthens OT network defenses against lateral movement. Requiring strong authentication for each access attempt limits an attacker's ability to spread ransomware

### Seamless AD Integration and SSO Capabilities

Silverfort's integration with Active Directory allows users to benefit from SSO while staying protected against identity threats and streamlining authentication and strengthening security.

**Learn more about how Silverfort helps mining sector solve their key identity security challenges.**