SILVERFORT

Breaking Through MFA Barriers in Oil & Gas Air-Gapped Networks

Silverfort helps oil and gas organizations protect their identity attack surface by mitigating ransomware risk and extending MFA protection to all resources in their IT and OT environments.

Today's interconnected world has made the cybersecurity landscape increasingly complex, particularly for industries such as oil and gas. Ransomware attacks have increased in frequency in this sector, causing serious concerns about the security of their operational technology (OT) networks.

Traditionally considered safe because of their air-gapped nature, OT networks are no longer as isolated as they once were. Due to the ever-growing convergence between OT and IT, even air-gapped OT networks are at risk of malicious intrusion. The gradual transition from local logins to Active Directory Single Sign On (SSO) has increased adversaries' ability to follow up on such initial access with lateral movement.

What Makes Oil & Gas Companies a Key Target for Identity Threats

IT/OT Convergence and Third-Party Access	Air-Gapped Networks Exposed to Ransomware	Shifting to Active Directory Single Sign-On
Since the convergence of IT and OT environments, OT networks need to be accessed regularly by third-party contractors and service providers for maintenance and support, creating a link between air-gapped networks and external systems. File transfers between OT and IT networks further erode the isolation between the two networks.	Since air-gapped networks are becoming more interconnected, attackers can exploit these gaps to infiltrate the OT network and plant ransomware payloads on critical assets like engineering workstations, HMIs, and databases. This ransomware propagation can lead to operational downtime, data loss, and significant financial losses.	As OT networks have transitioned from local authentication to Active Directory Single Sign-On (SSO), user access has become more seamless. A significant security flaw has also been exposed as a result of this. Once an attacker gains access to the network, centralized credentials facilitate lateral movement, increasing the risk of a breach causing significant damage.

How Silverfort Solves Oil & Gas Identity Security Challenges

Secure Third-Party Access	FIDO2 Token Support Helps Prevent Lateral Movement Attacks	Seamless AD Integration and SSO Capabilities
Silverfort does not require agents on the protected devices, meaning MFA can be enforced on all access attempts to any resource, including ones made by external vendors. This ensures that only authorized personnel can access the network and significantly reduces the attack surface.	By supporting FIDO2 tokens, Silverfort adds an extra layer of protection to the OT network against lateral movement. By requiring strong authentication for every access attempt, even if an attacker gains initial access, their ability to move laterally and spread ransomware is severely limited.	Silverfort's direct integration with Active Directory enables users to leverage the benefits of SSO access while maintaining full protection against identity threats. This approach simplifies the authentication process and enhances the overall security posture.

Learn more about how Silverfort helps Oil & Gas companies solve their key identity security challenges.

Download our Full eBook