CLAROTY

TOP RISKS THAT IT REMOTE ACCESS TOOLS POSE TO OT

Integrating IT remote access tools in OT (Operational Technology) environments introduces critical risks that must be carefully managed. These tools, including VPNs and jump boxes, were not originally designed with the unique requirements of OT systems in mind. Understanding and mitigating these risks is crucial for critical infrastructure safety, security, and operational efficiency.

Legacy System Exposure

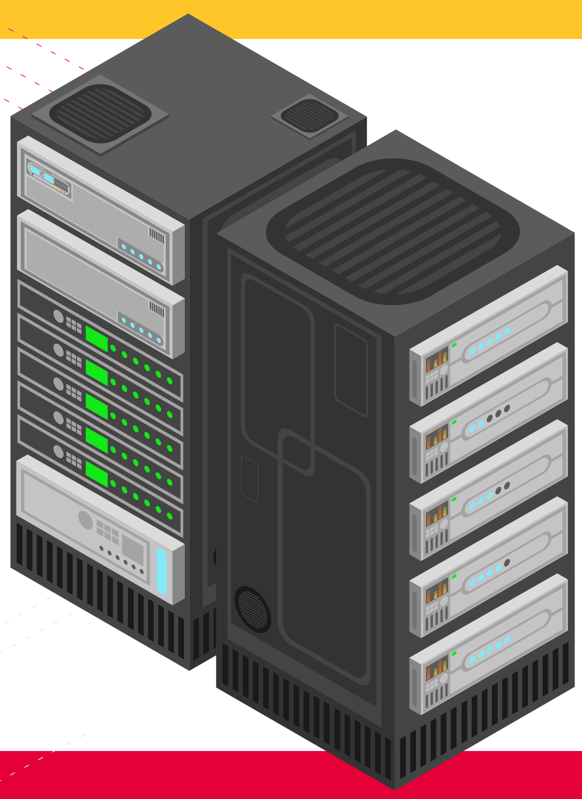
Legacy systems are common in OT environments due to their low tolerance for operational downtime. This condition, combined with the additional connectivity introduced by IT remote access tools, amplifies OT's exposure to cyber risks.

Network Segmentation Violations

Without a clear understanding of OT's unique segmentation needs, IT tools inadvertently create a bridge between IT and OT environments. This violates the OT segmentation principle of the Purdue Model, potentially exposing the critical physical processes in OT to cyber threats from IT.

Privilege Escalation & Insider Threats

Limitations in the permissions and access controls offered by conventional IT remote access solutions increase the likelihood that internal and external users will gain and intentionally or unknowingly leverage privileges that exceed what is required for their role in the OT environment. These conditions amplify the risk of unauthorized changes and other malicious or unintentional acts occurring in the environment.



Poor Password Hygiene

Many IT remote access solutions lack stringent, OT-required authentication protocols. Weak or reused passwords, especially without multi-factor authentication, elevate the risk of unauthorized access, making OT systems more vulnerable to cyber threats.

Unmonitored Activities & Undetected Threats

Traditional IT remote access tools typically do not offer real-time monitoring capabilities for OT remote sessions. This gap increases the likelihood that malicious activities, unintentional errors, or operational anomalies will go unnoticed, thereby extending response times and ultimately potentially jeopardizing both operational infrastructure and data.

Claroty Secure Remote Access (SRA): Your Solution to OT Risks

To counter these risks and improve the protection and resilience of your OT environment, consider Claroty Secure Remote Access (SRA). Explore its features and see how it's tailored to mitigate the unique risks IT tools pose to OT. Contact us or visit the Claroty SRA webpage to learn more.

#OTSecurityRisks #CyberSecurityAwareness #OTRemoteAccess

CLAROTY