Many operational technology (OT) systems lack basic security controls that can leave you vulnerable to cyberattacks.

**Top Threats to your critical SCADA infrastructure**

Legacy devices and software

- Lack of user and system authentication
- Weak data confidentiality
- Insufficient data integrity checking
- Inability to encrypt communications
- Supervisory control and data acquisition (SCADA) systems connected to unaudited dial-up lines or remote access servers
- OT systems connected to the network and accessible via web interfaces
- Out-of-the-box systems with default configurations and passwords may be unprotected:
  - Misconfigured firewalls can fail to detect or block malicious activity
  - Lack of segmentation between IT and OT networks
  - No microsegmentation within OT networks
  - Unauthorized access
  - Distributed Denial of Service (DDoS) attacks
  - Supply chain attacks
  - IoT device hijacking
  - Production delays
  - Physical damage to production facilities

Defend your OT / Industrial IoT / SCADA infrastructure with AT&T next-generation firewalls powered by Check Point Software Technologies

**Operational Benefits:***
- Gain deep visibility into OT assets and networks
- Help prevent OT threats with virtual patching, OT threat intelligence, and auto-isolation of infected assets
- Dynamically apply a rich IoT access policy specific to your environment and assets

**Security Benefits:***
- Secure industrial oil and gas asset infrastructure
- Help prevent OT threats with virtual patching, OT threat intelligence, and auto-isolation of infected assets
- Dynamically apply a rich IoT access policy specific to your environment and assets

Contact your AT&T representative to learn more about how AT&T can help protect your manufacturing environment.