AT&T Business | Check Point SOFTWARE TECHNOLOGIES LTD

Top **THREATS** to your critical **SCADA infrastructure**

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

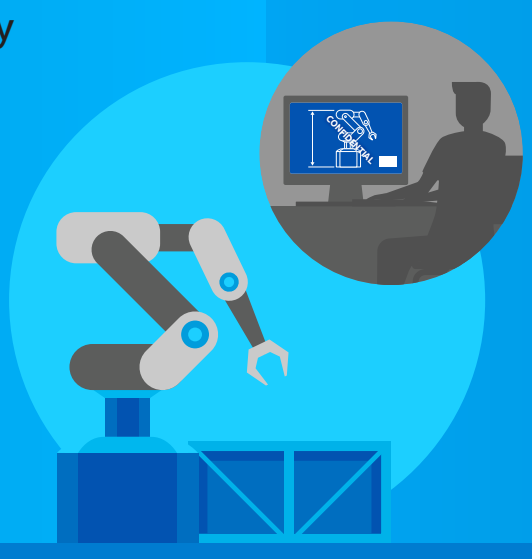
Top vulnerabilities

Top threats

Legacy devices and software

often lack critical security capabilities including:

- Lack of user and system authentication
- Without data authenticity verification
- Insufficient data integrity checking
- Inability to encrypt communications



leave your OT environment vulnerable to:

- Privilege escalation
- Identity theft
- Intellectual property theft
- Interception of login credentials

IT and OT Policies and procedures

often conflict:

- IT often prioritizes risk management, privacy, and compliance
- OT focuses on safety and resiliency of operations
- Security admins may not have oversight into OT environment, leaving gaps
- Rogue devices may exist on the network

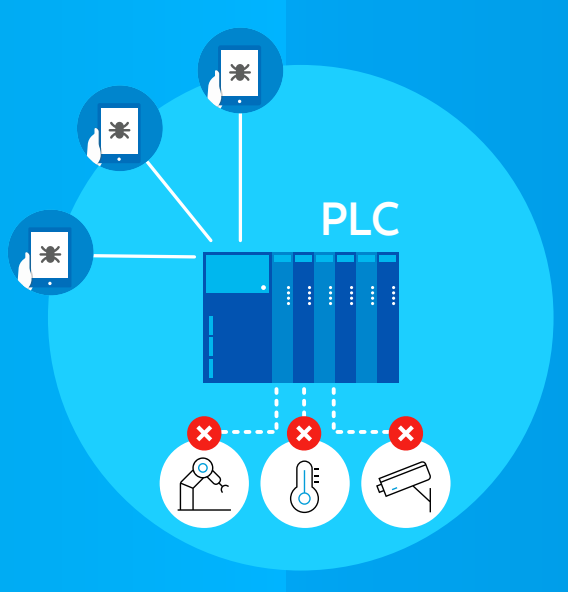
expose you to:

- A wide range of attacks and malware
- Productivity slowdowns
- Compliance violations

Connected systems

may be unprotected:

- 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



allow for malicious attacks including:

- Unauthorized access
- Distributed Denial of Service (DDoS) attacks
- Supply chain attacks
- IoT device hijacking
- Production delays
- Physical damage to production facilities

Existing security controls

may be inadequate:

- Misconfigured firewalls can fail to detect or block malicious activity
- Lack of segmentation between IT and OT networks
- No microsegmentation within OT networks

leave you unprotected from:

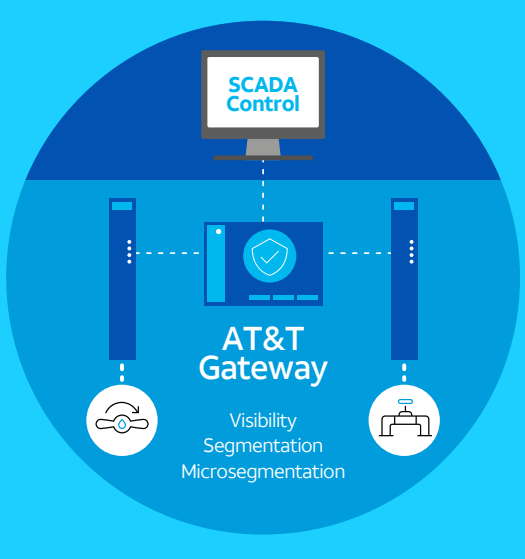
- Unauthorized access
- Ransomware
- Compromised websites
- Lateral spread within and across IT and OT networks

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

Network and device-level industrial control system (ICS) solutions

Operational benefits:

- Provide for the safety of industrial assets and personnel
- Help keep critical industrial processes running with a choice of active or passive enforcement
- Support compliance with OT cybersecurity regulations
- Help prevent product waste



Security 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

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