Protect critical industrial control ecosystems

The safety and integrity of operational technology environments are essential to productivity

Potential benefits

Provide for the safety of industrial assets and personnel

Help keep critical industrial processes running with a choice of passive or active enforcement, e.g., alerting or blocking

Gain deep visibility into OT assets and networks, facilitating asset inventory and anomaly detection

Support compliance with OT cybersecurity regulations (e.g., NERC CIP, NIST 800-82 and ISA/IEC 62443)

Prevent OT-targeted threats with virtual patching of vulnerable assets, OT-specific threat intelligence and auto-isolation of infected assets

Operational technology assets are attractive targets

Industrial control systems (ICS) are becoming more interconnected. Operational technology (OT) and information technology (IT) networks are converging. As a result, the opportunities to attack industrial manufacturing and critical infrastructure facilities continue to expand.

While interconnected ICS systems enhance productivity and yield, they can also open the door to opportunities for threat actors to cause harm to manufacturing operations and processes. For example, attackers can alter commands sent to controllers, changing their logical sequence or sensor readings, thereby disrupting industrial processes. These disturbances may be so subtle that they're difficult to detect at the onset. As a result, they will cause compounded damage over time.

Easy to hack, hard to patch

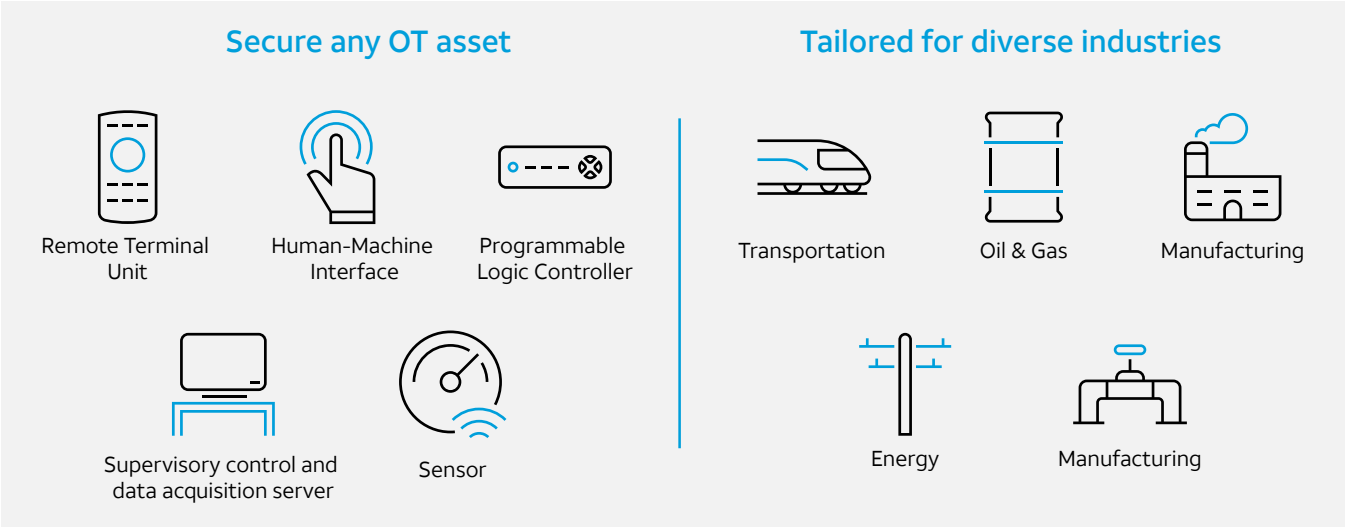
ICS assets and networks can be vulnerable to attack due to:

- Weak or hardcoded passwords
- Flat network design
- Assets run legacy or proprietary software that lacks security support
- Software that cannot be updated or patched frequently due to access limitations, concerns over downtime, or the need to recertify systems

Organizations can only protect what can be seen. Dedicated OT security solutions offer visibility and security to the abundance of assets connected to industrial and operational networks.

Industrial IoT security solutions from AT&T, powered by Check Point Software Technologies

AT&T Cybersecurity, in collaboration with Check Point, offers a comprehensive cybersecurity solution for ICS that keeps connected assets on the OT network protected. This includes programmable logic controllers (PLCs), human machine interfaces (HMIs) and supervisory control and data acquisition (SCADA) servers. With industrial domain expertise, the solution prevents OT-related attacks and continually minimizes the OT attack surface—all in a way that is easily scalable and non-disruptive to critical industrial processes.



Core capabilities

Securing connected devices across ICS networks, AT&T Business industrial IoT security solutions, powered by Check Point offer:

Deep ICS asset visibility and risk analysis

- Identify, classify, and analyze every OT device inside the network with advanced discovery engines tailored per industry
- Get granular fingerprints on each device, including communication protocol used, brand, model, type, IP, MAC address, firmware version, and more
- Obtain a behavioral baseline of normal activity across ICS asset communications to easily detect anomalies
- Expose risk indicators such as weak passwords, outdated firmware, and known vulnerabilities (CVEs)

Intuitive Zero Trust segmentation

- Segment the IT network from the OT network to prevent lateral movement and lateral infection
- Add micro-segmentation to prevent unauthorized east-west communication between ICS assets
- Apply granular security rules based on device attributes, risks, and OT protocols
- Easily create security rules based on dynamic grouping of devices
- Gain single-pane policy management for IT and IoT/OT, with a distinct OT policy layer
- Manage remote access to ICS assets

Mitigate known vulnerabilities, prevent threats and zero-day malware

- Virtually patch OT devices running unpatched firmware and legacy operating systems
- Identify and block, or alert of unauthorized access to and from OT devices and servers
- Prevent the newest OT-targeted malware attacks with real-time threat intelligence from ThreatCloud

Why AT&T and Check Point?

Encompassing network and device-level ICS protection, industrial IoT security solutions from AT&T Business, powered by Check Point, help prevent IoT cyberattacks. Our solutions adapt defenses to IoT or OT devices across smart-office, smart-building, medical and industrial environments, offering:

- Broad range of cybersecurity solutions to protect IoT devices
- Comprehensive threat prevention against the latest and most evasive IoT cyber attacks
- IT and IoT consolidated into unified cyber security architecture
- Choice of SMB/branch and enterprise-scale security gateways

The provider you need

AT&T Cybersecurity offers a variety of solutions to fit the unique needs of your business. Our knowledgeable, certified consultants are here to help, taking the time to understand your environment, helping you assess your IoT and manufacturing security status and goals to design policies and solutions that align with your business needs. The AT&T Security Operations Center (SOC) supports your security solution 24x7 with monitoring, help desk support, and implementation of approved security patches and updates.

With our industry-leading operations technology security solutions, AT&T Cybersecurity can help you safeguard your assets, act with confidence against threats, and drive efficiency into your security operations.

To learn more about Industrial IoT security solutions from AT&T Business, powered by Check Point Software Technologies, contact us or reach out to your AT&T account manager.

AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.