AT&T Business

Industrial IoT Security from AT&T

Powered by Bayshore IT/OT Gateway™

Unlocking the promise of the Industrial Internet of Things

The benefits of adopting IoT are tremendous as it helps reduce costs to the business, while improving efficiency and productivity. There is no surprise that analysts predict there will be 50B connected devices by 2020. The use of IoT in industrial settings (i.e. manufacturing, energy, utility, oil & gas, transportation) is called the Industrial IoT (IIoT).

Market Challenge: Security risks with Connecting OT assets to the Internet

Critical infrastructure is increasingly becoming a target…

- Manufacturing & Energy are the most targeted verticals for cyber breaches[1]
- 20% Increase in industrial control standards (ICS) Cybersecurity breaches in 2015[1]
- Our experts have seen a 458% increase in the number of times attackers scanned IoT devices for vulnerabilities over the past 2 years[2]

Market Needs: Visibility and Control into OT environments

Industrial customers need a security solution that…

- Provides security for OT systems and connected IIoT endpoints
- Supports SCADA and Industrial OT protocols
- Caters to more use cases than just firewall-based security policy management
- Supports SCADA and Industrial OT protocols

Secure Solution: AT&T Managed IT/OT Gateway

Defense in-depth approach for Industrial IoT to help secure both OT and IT…

- Visibility & control of OT environments and IIoT endpoints
- Cybersecurity protection from cyber-threats and unauthorized commands
- Safe operations & efficient use of Industrial Control Systems and endpoints
- Interoperability - Translates OT data into IT formats

As IoT gains momentum, securing the IoT ecosystem is imperative to the success of IoT. As businesses rely on machines and industrial systems for business-impacting decisions, the security, safety and operational efficiency of these endpoints is extremely important. If not properly managed, OT-related cyber incidents could lead to extended and costly production downtime, health and safety issues, and loss of sensitive information.

To help maximize and protect IIoT investments, organizations must prioritize the integration of an advanced cybersecurity solution into their environments.

Our Managed Industrial IoT Security Solution

AT&T's managed gateway specializes in the ability to help identify and stop attacks on IoT machines, applications, and industrial controls. The IT/OT Gateway enables Information Technology (IT) and Operational Technology (OT) organizations to work in concert to unlock the value of Industrial Internet applications. The IT/OT Gateway enables the Industrial Internet by allowing you to share industrial and machine data and applications with your customers, service providers and third party business entities. By using rapidly created, easily modified and globally deployed policy, the gateway helps provide for the integrity and optimization of your Industrial assets. Additionally, it's extremely granular inspection and filtration of industrial application content safe and highly secure protection for your M2M transactions, applications and workers.

Industrial-Strength Cybersecurity

When it comes to OT security and safety, AT&T's managed IT/OT Gateway provides measurable advantages over legacy enterprise and industrial network-based security solutions:

- The gateway is policy-based rather than signature based. The intuitive, predicate-based policy language is based on XML, so it can quickly adapt to proprietary data protocols and new protocols.
- It enforces policy based on content-awareness rather than metadata. It provides filtration and blocking of industrial content down to machine transaction and data value levels, much deeper than industrial firewalls.
- Years of domain intelligence on the leading industrial protocols and applications such as Modbus/TCP, DNP3, and EtherNet/IP, as well as IT protocols such as TCP/IP, HTTPs, NFS, etc..

[1]ICS-CERT 2015 and [2]AT&T Network Operations Network.

AT&T Business

AT&T Managed IT/OT Gateway

Key Differentiator: Policy Based Management Solution

- **Security Policy** - Defines how physical assets and business processes (i.e. industrial machines) are protected from compromise by rogue insiders, unauthorized users, hackers, and other adversaries
- **Safety Policy** - Defines how safety is enabled for workers, assets, customers, the public, and the environment
- **Operational Policy** - Helps enable operations and processes (i.e. robot commands) to be reliable, cost-effective and energy-efficient. Helps work towards compliance with laws, regulations and standards

Customer Benefits:

Improved security of Industrial environments

- Helps provide protection from known & emerging threats and process control commands
- Granular content & context-based DPI (Deep Packet Inspection)

Highly secure remote access

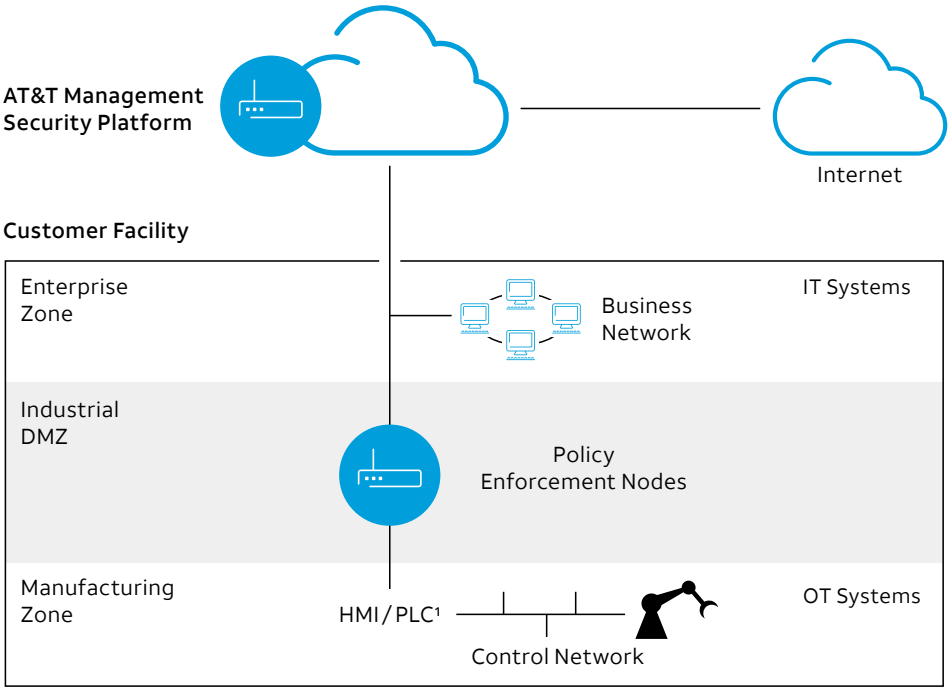
- Highly secure remote user access with identity-based policy enforcement

Plant safety

- Operations policy & assistance towards regulatory compliance
- Worker safety & reliability

Compliance

- Policy-based attributes of IoT endpoints for maintenance
- Highly secure vendor access for remote analysis & updates



IT/OT Application Policy Enforcement

Based on a policy creation and enforcement engine, the AT&T Managed IT/OT Gateway brings IT and OT together. Its ability to granularly inspect and filter application-layer data enables it to help detect, segment, block and isolate industrial protocols and applications. The IT/OT Gateway is also distinguished by its ability to automatically transform OT data and telemetry into formats that are consumable by advanced IT analytics applications.

These capabilities combine to provide IT with unprecedented visibility into OT applications and operations, and to provide OT with access to IT applications such as advanced analytics.

For more information contact one of our representatives.