WHITE PAPER

Mitigating Security Threats in the Age of the Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT)—which connects the physical operations and production capabilities of industrial enterprises with smart, digital technologies and machine learning—has been reshaping entire sectors of industry as enterprises experience major shifts in how they operate and innovate.

Through applications like smart manufacturing or connected field service, IIoT solutions connect devices, systems, and processes to monitor, analyze, and share data that provides visibility into machine performance and factory operations. An effective IIoT strategy empowers enterprises to transform operations by integrating real-time IIoT data and insights throughout the business to enhance decision-making, improve operational efficiencies, predict outcomes, and reduce costs.

But along with the many innovations made possible by IIoT technology comes inherent risk. Connected devices open up new vulnerabilities to threats, introducing unique security challenges not easily addressed with traditional approaches.

According to Frost & Sullivan, the number of deployed IIoT devices is expected to reach 45.4 billion by 2023.[1] Such risks can only continue to grow as more devices are connected. Industrial enterprises must adopt adequate practices for risk control and security to meet the unique challenges posed by IIoT solutions throughout their lifecycle and the current security threat landscape.

[1] *Securing the Connected Ecosystem—Leading Security Solutions and Approaches for IoT, Frost & Sullivan, Jan. 12, 2018*

New Vulnerabilities for Industrial Enterprise

Despite impressive advances in IIoT and supporting technologies in recent years, manufacturing and industrial operations still remain "islands of vulnerability." As legacy industrial control systems, which were never built with cybersecurity in mind, are retrofitted for IIoT and integrated with enterprise systems, new security vulnerabilities emerge.

Security at the device, network, and system levels is paramount to the safe, reliable operation of connected devices and systems. Each newly connected device adds another entry point into a network, where they ultimately connect to higher-value assets, such as data stores or financial systems. This makes IIoT devices attractive targets for bad actors seeking access to other enterprise systems.

There is no single answer to this problem; no new, definitive security solution designed specifically to mitigate threats to IIoT applications. Businesses need to implement a multi-layered approach to security, adapting or reengineering established security practices and controls to meet the unique constraints of connected devices, in their many variations.

The Security Threat Landscape

The security threat landscape for today's smart factories and machines is continuously expanding and evolving. As industrial enterprises become more and more connected, security issues are no longer purely an Information Technology (IT) problem; they can directly impact machines and physical business operations.

The increased saturation of connected assets, remotely-deployed equipment, and mobile devices represents a vast virtual expansion of the enterprise network perimeter, exposing organizations to a broader attack surface. As they integrate IIoT applications into day-to-day operations, businesses may add new capabilities and infrastructure or experience an uptick in the use of existing systems—like running regular analytics or storing data in the cloud—which may reshape an organization's security considerations.

This seemingly endless variety of connected devices and system configurations translates to a similarly wide variety of challenges to security that must be addressed. While IIoT devices and systems come in many shapes and sizes, security threats tend to fall into a few distinct categories.

Cyber Threat Actors

Growing levels of remote connectivity are significantly changing security threat models. Systems which had enjoyed relative isolation from threats are now being deliberately connected to monitor performance and collect data, exposing them to myriad potential adversaries.

Creating new points of entry to networks, industrial IoT environments present an attractive opportunity for threat actors with malicious intent. Cyber threat actors use a range of tactics, techniques, and procedures (TTPs), and will typically fall into one of these four primary categories:

Organized Crime Networks

Cyber criminals have persisted as a long-standing, common global threat, and are primarily driven by profit. Both individually and in groups, they steal data with the intent to sell, hold for ransom, or otherwise exploit for monetary gain.

- Common TTPs: Phishing, social engineering, business email compromise (BEC) scams, botnets, ransomware

Nation-State Actors

Nation-State actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. They either belong to, are directly affiliated with, or receive direction, funding, and/or technical assistance from a nation-state.

- Common TTPs: Spear phishing, social engineering, data exfiltration, remote access trojans, and destructive malware

Hacktivists

Hacktivists are politically, socially, or ideologically motivated. They identify targets for the purpose of gaining publicity or to effect change, and their actions often garner high-profile publicity.

- Common TTPs: DDoS attacks, doxxing, website defacements

Malicious Insiders

Current or former employees, contractors, or other partners who have access to an organization's networks, systems, or data can become inside threats. Malicious insiders intentionally misuse and exploit their privileges to compromise an organization's information systems or to access sensitive data.

- Common TTPs: Industrial espionage or sabotage

The People Problem

In many industry sectors—manufacturing in particular—factory operations have remained largely unconnected, giving way to the persistence of cultures that may not prioritize IT security, or know how. Employees running day-to-day operations on the plant floor may not understand the importance of security measures, or are indifferent or resistant to change.

Common manifestations of this include:

Lack of Awareness: "I didn't know those outages were caused by a vulnerability."

Assumptions: "All of our devices sit behind a firewall, so they must be secure."

Common Misperceptions: "An air-gap will protect against all cyber threat actors."

Myths and Dogma: "The FDA won't let me patch."

Inertia: "This is how we've always done it."

Insufficient Sharing: "I didn't know about the threats other systems were encountering."

Complexity: "We've got a lot of moving parts, and each one has its own security."

As new IIoT systems and solutions are implemented, businesses must dedicate resources to the education and training of employees as well as keeping the workforce updated on issues, threats, procedures. Properly trained and informed employees help to mitigate the risks to IIoT systems caused by human error.

The Pace of Connectivity

Throughout the world, businesses and individuals are connecting devices at an unprecedented rate, creating what may be the greatest challenge in the implementation of effective IIoT security. But as connectivity accelerates, so does complexity. Every new connected device is a new security consideration.

Industrial enterprises undergoing massive digital transformation may struggle to maintain security amidst rapid growth, emerging technologies, and evolving requirements. In the meantime, predators are continually honing their abilities and becoming more sophisticated in their tactics.

In large-scale IIoT environments, complexity in terms of the volume and variety of connected devices and systems make it more difficult to detect vulnerabilities and breaches and complicate the implementation of security controls.

Today's businesses want to be more proactive when it comes to security—to not only detect and mitigate threats as they occur but to anticipate future issues. With better insights, they can proactively adjust security measures today to more effectively counter tomorrow's threats.

Security is a Shared Responsibility

IIoT presents a set of unique challenges that requires solutions and controls. To design, implement, and execute on an effective IIoT security strategy, industrial enterprises should consider a mixture of tools, technologies, and partnerships.

In the age of digital transformation and innovation, this new landscape requires a fusion of once-disparate disciplines. As with safety and security in the physical world, everyone must do their part.

For example:

- IIoT developers must use best efforts to build and maintain secure, agile, and defensible products and platforms
- Partners and system integrators must use best efforts to securely extend, deploy, and maintain solutions in a dynamic threat landscape
- Users must operate solutions safely and securely, and remain vigilant to respond with speed and agility to emerging threats
- Governments and regulators should work with private sector to incentivize and assist IIoT efforts while monitoring national security threats
- Philanthropic sources and civil society are always welcome to provide contributions that help catalyze necessary adaptations

Commitment to a Secure Future

As a leading provider of IIoT technology solutions, PTC is committed to fulfill the responsibility inherent to such a foundational role. PTC invites partners and customers to join together in developing a collaborative approach and establishing best practices that will optimize security for IIoT. PTC strives to enhance third-party collaboration through the launch of its coordinated vulnerability disclosure program, as well as promotion of greater engagement amongst IIoT and security solution providers.

ThingWorx IIoT Solutions Platform

PTC's ThingWorx is a technology platform that facilitates the connectivity of devices—or, "things"—and the development of IoT solutions in an industrial environment. In order to meet the needs of diverse industrial enterprises, PTC has equipped ThingWorx with a broad set of flexible capabilities.

The ThingWorx platform consists of a series of preconfigured blocks or modules with a governing software that, based on customer requirements, will define the solution the customer needs.

New, preconfigured blocks can be added in a smart way to obtain the new results. Many different communication paths can be configured related to entities such as machines, devices, workers, facilities, or entire systems, in various orders and directions depending on the desired target solution.

The first steps in designing a smart solution are focused on business value to the customer. ThingWorx users should take great care when considering their deployment configurations, methods for extending the functionality of the platform, and access control strategies, among other things. Additionally, it is critical that the organization creates an end-to-end security strategy to protect devices, applications, architecture, and infrastructure.

The ThingWorx Shared Responsibility Model

Due to the open and extensible nature of the platform, ThingWorx relies on a shared responsibility model for security. ThingWorx enables users to create applications that are flexible—including the security features—and provides a range of extensions from partners to configure additional security measures as they see fit.

ThingWorx helps customers to build secure IIoT solutions by supporting:

- Extremely flexible permissions and visibility capabilities including Access Control Lists
- Design and runtime permissions down to the property level
- Robust user and group management
- Ability to remotely update edge devices for security
- Integration with Active Directory and Single Sign-on (via Ping Federate)
- Transport Layer Security (TLS) encryption
- Audit trail of all actions in the development environment

The ThingWorx Approach to Security

To ensure the security features of ThingWorx solutions continue to meet or exceed industry standards and best practices for IIoT, PTC takes security into account throughout the software development lifecycle, from the beginning.

Threat Modeling

Threat modeling is the process of identifying, understanding, and communicating security threats and suggested mitigations. PTC has implemented several processes for ensuring security in the development of ThingWorx, including mandating regular security training for all research and development personnel. PTC also has a full-time security architect who trains product engineers and developers on threat modeling and identifies and reviews potentially high-risk features.

From design–time forward, ThingWorx products are developed using the threat modeling process in conjunction with industry best practices for secure coding. PTC uses a modern, agile, building-block approach to threat modeling that streamlines the process.

Identifying Vulnerabilities

During development of ThingWorx products and features, PTC uses standard tools to analyze and test APIs and to identify and remediate vulnerabilities prior to release. ThingWorx also uses industry-standard analysis tools to scan ThingWorx code and automated applications that evaluate relevant third-party libraries.

Quality Assurance

PTC's ThingWorx quality assurance (QA) organization performs planning, testing, reporting, analysis, tracking, and final approval for product releases. The team is comprised of experienced quality and test engineers around the globe who use cutting-edge tools to test issues with product performance or processes and work closely with software engineers during the development process.

Security Updates

PTC provides maintenance releases with functional and security improvements for all versions of ThingWorx in Standard Support approximately every 6-8 weeks, and strongly advises customers to always upgrade to the latest version. For critical security issues, PTC may make changes that impact backwards compatibility.

Learn More

Determining the right approach to security is a critical step in digital transformation for industrial enterprises. A multi-layered, shared responsibility approach - centered around an IIoT platform with built-in security is a good first step.

Contact us to learn more about PTC's approach to security for IIoT.