



Solution Brief

OT Asset Management

According to a Ponemon Institute study¹, only 29% of organizations said that asset discovery and management is being used to protect their industrial control system environments. **Asset management is one of the most undervalued activities in the operational technology space**, despite its critical importance to a strong cybersecurity program and regulatory compliance efforts. We're here to change that.

¹ 2021 State of Industrial Cybersecurity, The Risks Created by the Cultural Divide Between the IT & OT Teams Survey, The Ponemon Institute



What Is OT Asset Management (OTAM)?

“The ability for organizations to properly and consistently identify and consistently manage data, personnel, devices, systems, and facilities based on their relative importance to provide the foundational capability to support an organizational cybersecurity program.”²

Why Is OT Asset Management Important?

To ensure the safety of their employees and the public, create an effective cybersecurity program, and prepare for future regulatory requirements, critical infrastructure organizations must build a future-proof foundation by identifying, monitoring and managing changes for every OT asset in their infrastructure.

Why You Need OTAM



Safety

In OT environments, digital assets impact the physical world. OT asset management helps ensure safety if an unintended or unauthorized change occurs in a device or system.



Security

Accurate asset data and security baselines are the foundation of a strong cybersecurity program. Historizing asset changes also provides a template for backup and recovery if an incident does occur.



Compliance

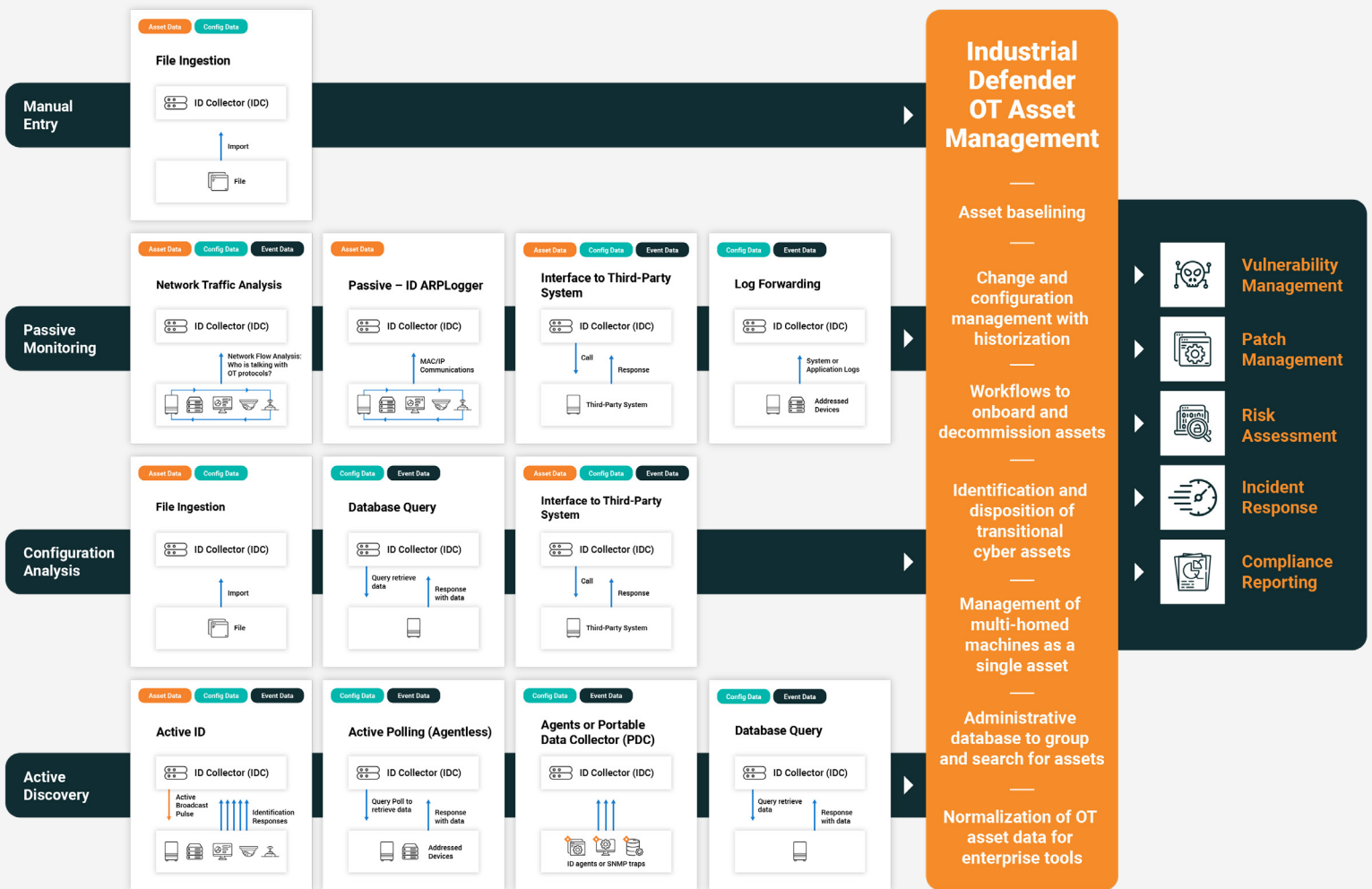
Having an OT asset management foundation in place helps you prepare for future compliance regulations that could affect your industry.

² NIST 800-82 Special Publication, Revision 3, Guide to Operational Technology Security , Initial Public Draft” NIST, April 2022

Industrial Defender's OTAM Solution

Security teams need an automated approach to identify, monitor and manage every asset and document appropriate changes. Having a single source of truth for your asset base that includes configuration and change management enables a centralized cybersecurity program that can include vulnerability and patch management, version control, security baselines, risk assessments, incident response and compliance reporting.

To do this effectively, teams need access to four sources of data: physical inspection information, passive monitoring methods, configuration analysis and active discovery techniques. Industrial Defender leverages all four data collection methods needed for true OTAM in one UI.



Types of OT Asset Data Managed by Industrial Defender

Device Configuration Data

- ◆ Firmware and software, including versions and vulnerabilities
- ◆ OS, including version and patches installed
- ◆ Open ports and services
- ◆ Removable media installed
- ◆ Malicious code detected/AV
- ◆ Failure of event logging
- ◆ Serial number
- ◆ Policies modified

Firewall Information & Events

- ◆ Firewall rules, including change detection
- ◆ Blocked execution (packet)
- ◆ Blocked unauthorized file
- ◆ Policies modified

System Access & Authentication

- ◆ Successful and failed login attempts
- ◆ Generic and shared user accounts
- ◆ Local and A/D accounts
- ◆ Password parameters and age
- ◆ User account locked
- ◆ Policies modified
- ◆ Privilege raised
- ◆ Failure of event logging

Asset Resource Utilization & Status

- ◆ CPU & RAM usage over time
- ◆ Disk space
- ◆ Swap space
- ◆ Connectivity lost
- ◆ Shutdown
- ◆ Rebooted and boot checksum
- ◆ Backup failure

*This list is not all encompassing. The data collected varies for each device, dependent upon the manufacturer, model, and version.

Benefits of Industrial Defender's OTAM

- ✓ Create an efficient configuration and change management process
- ✓ Support more comprehensive risk assessments and mitigations
- ✓ Reduce MTTR
- ✓ Build a single source of truth for maintenance efficiency
- ✓ Enable ongoing vulnerability and patch management
- ✓ Establish a backup and recovery foundation

Industrial Defender's OTAM Features

-  100% asset coverage via active, agentless, and passive data collection methods for connected assets, plus manual import capabilities for disconnected assets.
-  Creation of asset baseline configurations that our change detection engine compares with actual configuration data. All asset changes are historized over time.
-  Built-in workflows for onboarding and decommissioning of assets.
-  The ability to merge multi-homed machines into a single asset.
-  Identification and disposition of transitional cyber assets.
-  An extensive, customizable administrative database to group and search for assets.
-  Integrations to share OT asset data with third party software via REST API.

The Industrial Defender Difference

Industrial Defender protects the world's critical infrastructure from cyberattacks. As the leader in OT cybersecurity innovation, the company's scalable platform is used by the largest organizations in the world to empower security stakeholders with actionable data about their OT and IIoT infrastructure, enabling them to make informed risk management decisions. Learn more at [IndustrialDefender.com](https://www.IndustrialDefender.com).

[Schedule a demo](#)

For more information

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 0203