OT ASSET INVENTORY MADE EASY

How to get a comprehensive OT asset inventory without hardware sensors or manual discovery

CONTENTS

Control engineers and OT security experts agree that a comprehensive and accurate OT asset inventory is necessary. Why? A system of record is needed for various use cases, such as OT vulnerability management, obsolescence management, and configuration management. At the same time, it is obvious that most asset owners struggle to produce such an inventory.

This guide is about making OT asset inventory easy and how applying the right approach can save countless hours of valuable engineering time.

“The OT Asset Inventory in an accurate and comprehensive form is the start of every OT security journey. It's the first step. And if you get that step wrong, everything that follows will go in the wrong direction." — **Ralph Langner,** OTbase CEO

Microsoft Excel Inappropriate for OT Asset Inventories

Microsoft Excel is by far the most used application for OT asset inventories. While it is great for many things, an OT asset inventory is not one of them.

If your organization uses the application, the result is undoubtedly a list of IP addresses and entries for OT asset make and model. Additional information might also include OS or firmware version. This is not nearly enough information, nor contextualized in any meaningful way. There are quite a few shortcomings to using Excel for creating an OT asset inventory:

1. **Excel is a manual application.** You must assign someone, likely an entire team, to visually inspect and enter all the information. The information gathered barely scratches the surface of what you have installed. For example, you send a team to gather serial numbers and firmware versions for all I/O modules in all PLC racks. Not only is it time-consuming, but the information you get is superficial and will, more likely than not, become outdated in short order.
2. **The Excel file is generally stored on someone's local machine and is not accessible by anyone else or updated regularly.** There is no access control. Often, a "version conflict" can be created. Consider for a moment: someone requests the Excel inventory file you've created. You send them a copy. They open and start changing the information contained within. Then, that file gets shared with others who make additional changes. Suddenly, you have no "single source of truth" regarding your inventory. That's in addition to the high likelihood that the information, as noted before, is not accurate or recent.
3. **There is no device identity.** OT asset inventories kept in Excel are usually specific to a general location and don't contain global OT asset inventory information. Also, outside of the basic information, you are missing critical details that simply aren't generally recorded, such as what the asset is and where it is in the world.

OT Threat Detection Products

Outside of Excel, a lot of organizations employ some type of OT threat detection product. OT threat detection is primarily focused on identifying cyber threats. These vendors like to claim they can provide a useful OT asset inventory, but they can't. Here's why:

1. **The information is basic and ambiguous.** This is thanks to OT threat detection's ability to "passively sniff" OT assets, which provides little information of consequence. For example, it's akin to someone manually entering information into Excel. Sure, you have some basic information, but no real meaning is associated with it.
2. **There's no device identity.** Passive scanning doesn't provide true device identity. That's because it "sniffs" assets' IP addresses, which is useless in OT because there can be and often are many duplicates.
3. **Devices cannot be added manually or via import.**
4. **Fieldbus devices are not covered.** Examples include ControlNet, DeviceNet, SERCOS, Profibus, and DH+.
5. **There is no network data.** OT threat detection products don't inventory networks, port lists, or generate topology maps.
6. **There is no meta data enrichment.**

WATCH: HAS OT THREAT DETECTION FAILED?

Automatic Active Asset Discovery

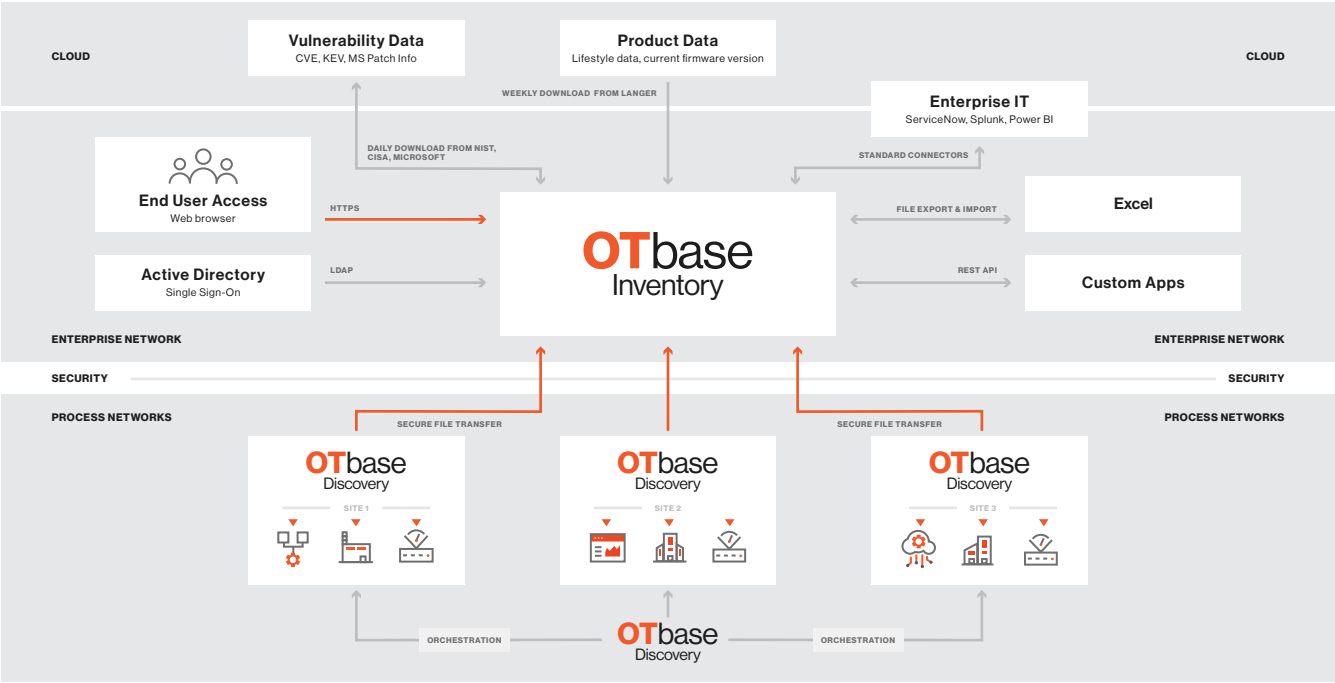
Recall the concept of passive scanning mentioned previously. It provides you with bare-bones information about your OT assets. While it is used frequently with the attempt to create an OT asset inventory, passive scanning just doesn't deliver because the data is not precise enough.

For any detailed discovery, the only way to go is active. Before you run away screaming, this is not the active scanning that you heard crashes control systems just like that. Active discovery as implemented in the OTbase probes OT devices, including network switches and routers, Windows PCs, sensors and actuators, barcode readers, and so on, **using legitimate protocols and access credentials.** It's as dangerous as having your RSLinx executing an RSWho search. It leverages the fact that virtually every relevant protocol in the OT space can query meta data from product identity over firmware versions to layer 2 network connectivity.

You may still have reservations because you don't want a central server to discover all the devices in all your process networks, and you would be right. That would be a security nightmare. In a centralized architecture, a central server scans subnets that it can route into. Since the server also stores access credentials for your network endpoints, you introduce a security risk.

For this reason, OTbase features a decentralized discovery approach. It uses a distinct two-tier architecture with one central server that usually sits in the enterprise network. This server, however, does not do any discovery on its own. That happens in the OTbase Discovery software, a standalone software that is deployed in a decentralized manner in your process networks. It's a Windows service (or Linux daemon) that you install on an appropriate system in your OT environment from where it can execute active probing with legitimate industrial protocols such as Modbus or Ethernet/IP.

WATCH: OT ASSET INVENTORY BASICS – PASSIVE, ACTIVE, AND HOST-BASED OT ASSET DISCOVERY



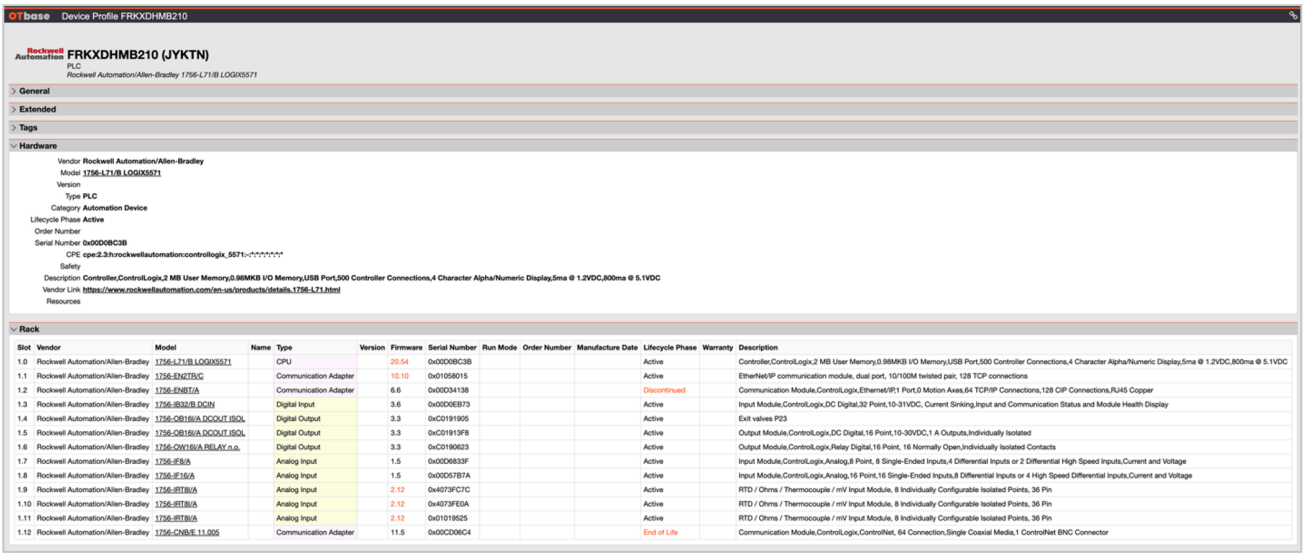
Why is this important in an OT asset inventory? A decentralized architecture carries little risk when it comes to OT asset discovery. Unlike centralized discovery, it doesn't house access credentials and exists behind a security wall.

What Details Do You Get with Automated Active Discovery?

With OTbase Discovery, and within a few hours, you will discover the technical properties of the bulk of OT assets in your installed base. Those technical properties include:

- Hardware make and model
- Device type (PLC, operator station, VFD, …)
- Network address(es)
- MAC address(es)
- Serial number for control system racks: Hardware configuration details, exposing all installed I/O modules (make, model, hardware version, firmware version)
- Installed firmware or OS version
- Installed application software and patches (in the case of computers).

For most OT devices, these properties can be discovered automatically via the network, using the same approach that engineering software uses. Industrial protocols such as Modbus, Ethernet/IP, Profinet, and Windows Remote Management (WinRM) include commands for obtaining information about device identity and configuration. These commands can be leveraged by an OT asset inventory solution. Using this methodology is referred to as “active probing”, or simply “active discovery”.



A Comprehensive OT Asset Inventory Makes OT Vulnerability Management Easier

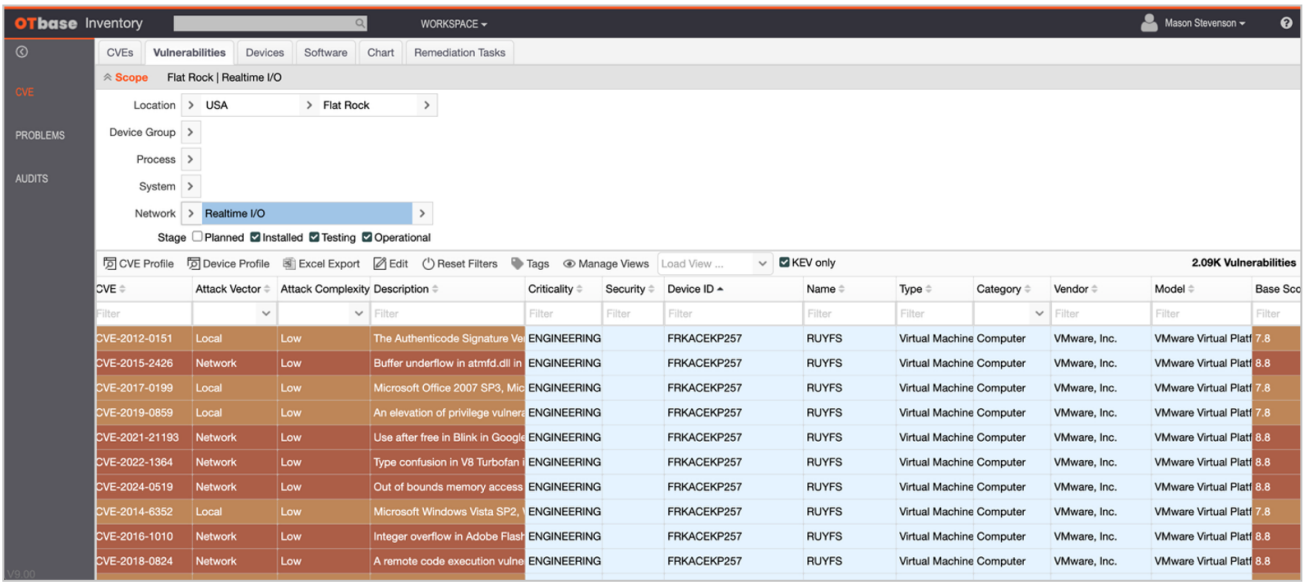
One of the major use cases of an OT asset inventory is effective OT vulnerability management.

How can you know about all the vulnerabilities that affect your installed base? The good news is once you have a comprehensive and accurate OT asset inventory in place, identifying known vulnerabilities automatically becomes quite easy. That's right, no more browsing through Cybersecurity Infrastructure Security Agency (CISA) or National Institute of Standards and Technology (NIST) websites. Automation is possible.

The reason is that **every single known vulnerability, or CVE, is tied to a specific product version.** Therefore, once the versions of your OT products are known, your OT asset inventory can inform you about known cyber vulnerabilities that affect you.

WATCH: OT VULNERABILITY MANAGEMENT MADE EASY

The National Vulnerability Database (NVD), operated by NIST (under the United States Department of Commerce), is integrated into OTbase. In OTbase, there is no need to run a vulnerability scan, as it's an automatic process that is evergreen in its effectiveness.

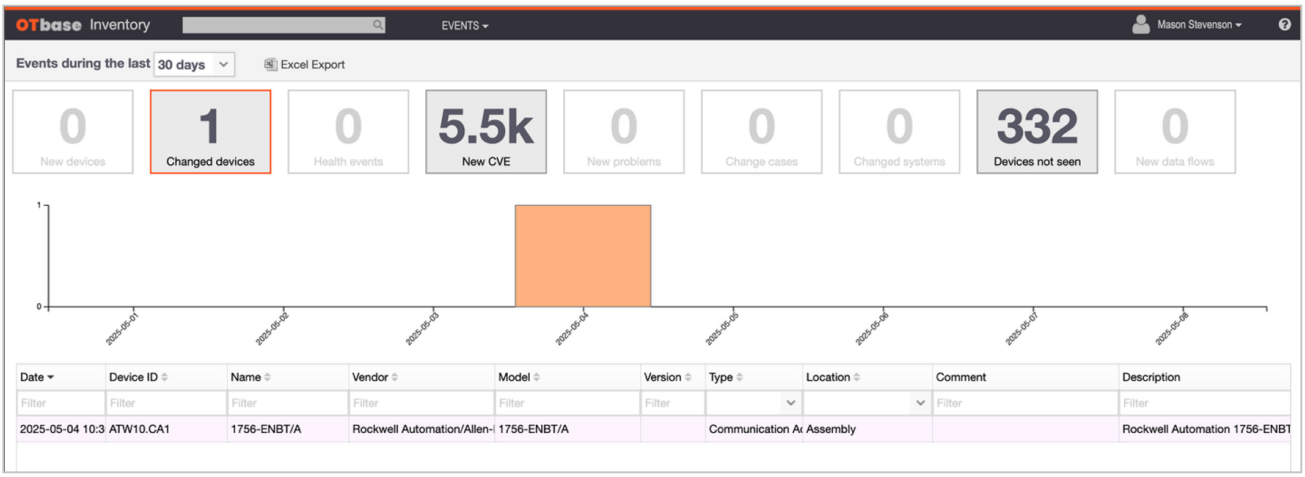


Keeping the OT Asset Inventory Evergreen

The concept of a comprehensive and accurate OT asset inventory being needed cannot be stressed enough.

The same can be said about the idea that it is not a "one and done" type of project. This type of OT asset inventory must be consistently updated and maintained for accuracy. Thankfully, OTbase does that automatically for you.

OTbase Discovery executes an active probing process automatically every 24 hours. Utilizing this approach, OTbase catches new devices on networks and configuration changes, which are automatically logged in the respective device's configuration timeline within OTbase Inventory. Once logged, those changes are immediately seen on the events page of OTbase Inventory. You can also receive email updates about changes.



A Clear-Cut ROI Case for a Comprehensive OT Asset Inventory

If your engineers are still building OT asset inventories with spreadsheets or OT threat detection tools, you're not just wasting time, you're setting yourself up for failure. Manual data collection is a tedious and error-prone process that drains engineering resources and delivers outdated, incomplete results. The same goes for OT threat detection tools masquerading as OT asset inventory solutions. They offer superficial insights at best.

A comprehensive and accurate OT asset inventory solution like OTbase automates the discovery of detailed asset data using active probing with legitimate protocols. It doesn't just capture MAC addresses and serial numbers—it delivers full hardware configurations, installed firmware, OS versions, and more. And it keeps that data current, automatically.

The result? Engineers no longer need to waste weeks hunting down I/O module versions or tracing asset identities across fragmented spreadsheets. They can focus on tasks that align with the business. That's your ROI: thousands of hours reclaimed from repetitive busywork and redirected toward real engineering value.

ABOUT OTBASE

OTbase is a productivity and collaboration tool for your journey towards secure and resilient OT networks. OTbase inventories your OT systems automatically and acts as a platform to streamline, plan, and document your digital transformation journey. It turns complex tasks such as vulnerability management, auditing, and obsolescence management into structured workflows with measurable results.

We have been among the first to develop the field of OT security, way back in the Nineties. We have cracked the Stuxnet malware. We have helped asset owners in critical infrastructure and manufacturing to protect against nation-state level cyber attacks.

Our game-changing OTbase OT asset management software helps companies to build secure and resilient OT networks in times of shrinking head counts.

Learn more at www.langner.com

OTbase