

Best In Class Integrated Approach to Data Collection for OT Security & Compliance

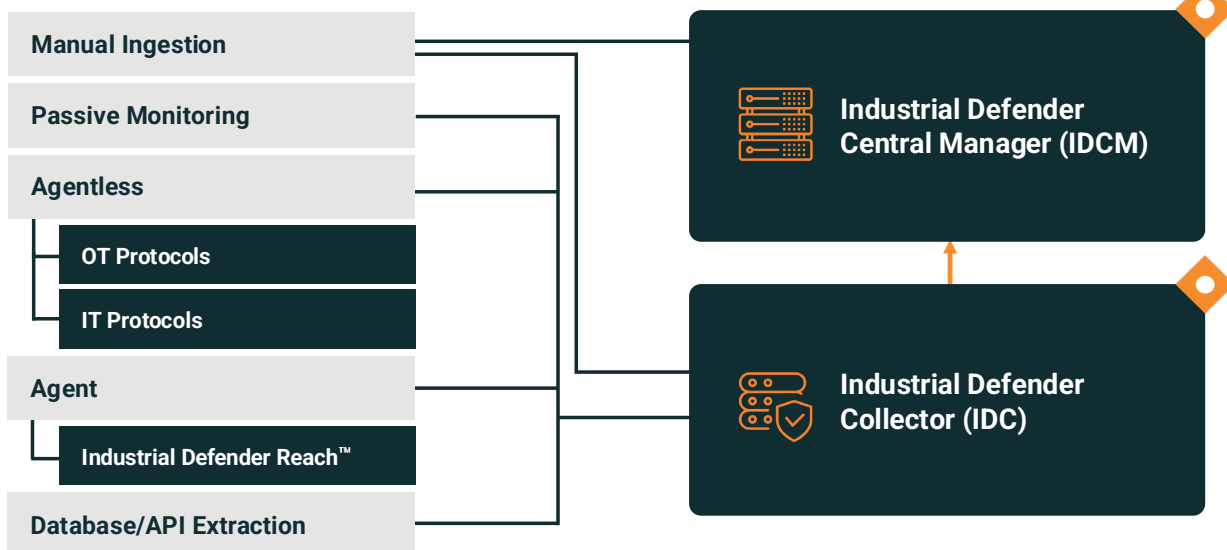
The most comprehensive and operationally safe approach to understanding your OT environment

The cornerstone of security and compliance in operational environments is reliable OT asset data. Understanding of your OT environment begins with an asset inventory. If that's limited to simply knowing what devices are present on your network, you need to go deeper.

To manage your OT assets and cyber risks, you need detailed information about each endpoint, such as software versions, configurations, vulnerabilities, patches, firewall rules, and PLC key switch positions. This requires an integrated approach to data collection, combining passive and active methods, and offering both agent-based and agentless options.

Industrial Defender takes an integrated data collection approach, tailored to your specific environment, providing the most effective and operationally safe way to gain deep insights into your OT environment.

Best-in-Class Data Collection Methods



Manual Data Ingestion

Any existing data that you've collected or will continue to need to collect manually can be ingested into the Industrial Defender platform. This can include spreadsheets in various formats like CSV, JSON etc., which can then be pulled directly into the platform and integrated centrally with the rest of your OT data.

Passive Monitoring

Industrial Defender utilizes both passive and active data collection, depending on the environment. Where passive monitoring is ideal, Industrial Defender monitors OT network traffic to identify device information by interpreting industrial protocols and parsing out the configuration state data. The system also captures messages that indicate abnormal events. Example protocols include DNS, ENIP/CIP, HTTPS, ICMP, IEC-104, MMS, Modbus, OPC UA, S7, Profinet DCP, and others.

Active Capabilities

For the richest asset information, Industrial Defender leverages active approaches that are deployed in a specific manner that is operationally safe for your industrial environment. This allows for the deepest, richest data collection, including software versions, configurations, vulnerabilities, patches, firewall rules, and PLC key switch positions.

Agentless

Understanding that agents may not always be appropriate for critical or sensitive OT systems, Industrial Defender also deploys agentless approaches to gather asset data, via both OT protocols and IT protocols.

OT Protocols

Interacts with OT devices using their native protocols such as Modbus, DNP3, S7, etc. These are the same protocols and mechanisms that the devices themselves use to communicate with each other and with the applications used to configure and manage them. We utilize a flexible framework that allows us to easily add support for new OT protocols and query mechanisms as needed.

IT Protocols

Interacts with devices using their management interfaces such as SSH or HTTPS. IT protocols are utilized in various ways, from querying Windows with PowerShell commands to using SSH connection or HTML screen scraping of web interfaces. Our comprehensive and flexible framework allows us to utilize telnet, SSH, SNMP, HTTP, HTTPS, and other mechanisms, supporting all typical authentication mechanisms.

Agent-Based

The Industrial Defender Agent boosts efficiency by operating continuously, making data available in real-time, and follows a consistent process each time, ensuring data uniformity. The agent also has built-in throttling capabilities, ensuring it never uses more than 1% of the CPU, and allowing for network bandwidth throttling.

Not Quite an Agent – But Just as Effective: A UNIQUE “PORTABLE” APPROACH WITH INDUSTRIAL DEFENDER REACH™

In cases where a networked environment is not possible or connection to the Industrial Defender Collector (IDC) or Central Manager (IDCM) is not feasible, we offer a unique solution - “Industrial Defender Reach.” This approach caters to challenging circumstances like highly distributed environments, non-networked assets, or cases where the installation of agents is not desirable. It operates through a lightweight Windows executable program, providing the same precision and depth in asset data as an installed agent, but without any continuously running services on sensitive or critical assets.

Database/API Extraction

Data can be obtained from external sources such as databases or asset management applications, rather than directly from the device. This approach is used when OT devices lack mechanisms for querying configuration or when direct interaction is undesirable. Many systems store relevant data which can be accessed via a REST API. Our experts tackle these unique situations, ensuring our capabilities extend to collecting asset data through these methods as well.

No Stone Left Unturned

Using an integrated approach, Industrial Defender ensures the most complete data collection from your OT environment. By employing a mix of manual data ingestion, passive and active data collection, and both agent-based and agentless methods, we provide a comprehensive, operationally safe, and efficient way to understand and manage your OT environment.

[Schedule a demo](#)

THE INDUSTRIAL DEFENDER DIFFERENCE

Industrial Defender is the single best source of OT asset data needed to protect industrial operations and meet compliance. Established in 2006 and headquartered in the United States, Industrial Defender is the leader in providing deeper-level asset data and vital endpoint information, along with historical context and change monitoring capabilities, for addressing cyber risks across the OT environment.

1 (877) 943-3363
(617) 675-4206
info@industrialdefender.com
225 Foxborough Blvd
Foxborough, MA 02035

[industrialdefender.com](https://www.industrialdefender.com)

© 2024 iDefender, LLC