



Solution Brief

Configuration and Change Management for Operational Environments

Manage Changes to Your OT Assets and Maintain
Secure & Compliant Configurations

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

Introduction

Deep Configuration Visibility is Vital to OT Security

The foundation to any effective OT cybersecurity program starts with an understanding of an organization's systems, assets, data, and risks. This is a requirement in all major cybersecurity frameworks and regulations (NIST, CIS Controls, NERC-CIP, IEC/ISA 62443) and it serves as the basis on which other components or aspects of security are built or depend upon.

What does an “understanding” of the OT environment entail? It begins with conducting an asset inventory to identify all the OT assets and systems present in your environment. However, simply knowing what systems are present is not enough to fully understand and address security risks. Many asset inventory or “visibility” solutions in the OT space stop at identifying only what OT devices present on the network. They may provide device type, make and model, but fail to provide key configuration details such as software versions, vulnerabilities, patches, firewall rules, and PLC key switch positions. These configuration details are vital to accurately assess the cyber risk associated with each asset and implementing appropriate security controls.

Detecting Changes That Weaken Security Posture

Understanding current configuration settings helps you identify potential entry points for attackers and assess whether you meet certain security standards, such as hardening best practices or regulatory frameworks. Even more important for maintaining security and compliance on an on-going basis, configuration data enables you to manage change. Changes to system configurations can significantly impact your security posture. System changes, if not managed properly, can introduce misconfigurations and vulnerabilities that expose your environment to attacks. Unauthorized changes can also introduce operational issues and system instability. Keeping track of configuration changes allows you to quickly identify and respond to any unexpected or unauthorized changes, reducing the risk of a security breach or compliance violation.

Configuration & Change Management

Effective management of configurations and changes requires a reliable Configuration and Change Management (CCM) program. CCM is not simply an exercise focused on taking snapshots of current configuration states, but rather a sustainable program for consistently and accurately gathering, analyzing, and comparing configuration data on an on-going basis. The goal of CCM is to maintain system integrity, security, and compliance over time.

A solid CCM program will also enable your team with context — helping you understand whether a change is “good” or “bad” and how it has affected your security posture. By providing details of who changed what, when, and where each change was made, CCM guides preventative measures against system outages or data breaches.

CCM also enables you to measure the extent of configuration drift across your environment. By establishing a baseline for what a secure and stable system should look like, CCM allows you to quickly identify any deviations from the established “good” configuration and take action to mitigate any potential risks to the system’s security and reliability.

With CCM, you can proactively monitor system changes and assess their impact on the established baseline, ensuring that the system remains secure and compliant with established standards and requirements. Ultimately, CCM plays a critical role in ensuring system integrity and mitigating the risks associated with configuration changes over time.

Implementing this in an OT Environment

In IT environments, Configuration and Change Management is considered a fundamental requirement and it is well adopted, championed, and enforced across all leading IT security frameworks. However, the benefits of CCM have not been as easily realized or leveraged in OT environments. Due to the complexity and operational requirements of OT devices, it takes a unique approach to effectively gather endpoint configuration data in a way that is operationally safe. Implementing CCM using IT-specific tools has been shown to disrupt OT assets that drive critical processes, leading to potential plant downtime. Therefore, the adoption of CCM in OT requires a tailored approach to ensure its effectiveness without disrupting critical operations. In lieu of a solution specifically designed for this, industrial organizations have run into challenges trying to accomplish this manually or with disparate tools.

The Problem with Manually Tracking

Some organizations conduct CCM manually. They may do this to fulfill a compliance requirement (such as NERC-CIP which has requirements for regular inventory updates and documentation of changes). However, manual CCM can be a time-consuming and expensive process, particularly for large-scale systems with multiple sites. This typically involves manual inspections and travel to various locations to gather data from machines on a routine basis. The collected data is then recorded manually and managed using spreadsheets, which can be error-prone and cumbersome to manage. This approach also makes it difficult to compare historical data and track system changes, making it challenging to

maintain continuous security posture or on-going compliance with established standards and baselines. Automated CCM solutions, on the other hand, can provide real-time data, automate inventory updates, streamline change management, and reduce costs and errors, providing more effective support for continuous maintenance of system security posture and on-going compliance.

Separate Solutions for Asset Inventory and CCM

Again, while many asset inventory or “visibility” solutions in the OT space excel at identifying OT devices, they often lack in-depth endpoint configuration details. These “passive” discovery tools are designed to collect information at the network-level and are great for monitoring network-level behaviors and threat indicators. However, the OT asset details that can be obtained from the network are limited and do not provide the necessary configuration details required to track system changes. This can result in incomplete asset inventories, lacking the deeper configuration details that provide the basis for CCM.

Automating OT Configuration and Change Management with Industrial Defender

Industrial Defender is the pioneer and leader of OT Configuration and Change Management. Purpose-built for OT environments, the Industrial Defender Platform enables organizations to safely and effectively automate CCM to maintain OT asset integrity, security and compliance.

Since 2006, Industrial Defender has solely focused on OT environments. With core capabilities in providing in-depth asset data and essential endpoint information, along with historical context and change detection, Industrial Defender’s platform enables organizations to stay on top of cyber risks across their OT environment. Our extensive experience and expertise drive the Industrial Defender Platform, which provides the most comprehensive centralized hub of rich OT asset data using a best-in-class approach to data collection.

Understand OT Asset Configurations with Industrial Defender

- OS details
- Software installed
- Patches
- Ports and services
- Firewall rules
- User accounts
- NICs and more

Integrated Data Collection Approach – Effective & Operationally Safe

Get the most comprehensive OT asset data with our integrated data collection approach. Our best-in-class data collection is proven to be operationally safe and effective for managing even your hard-to-reach and/or offline assets by combining the following methods:

- Manual Ingestion
- Passive Monitoring
- Native Polling
- Agentless
- Agent
- Direct Database

Proper Historical Context for Maintaining System Integrity

Unlike other solutions that provide basic configuration snapshots, the Industrial Defender Platform was specifically designed to store historical configuration data, enabling you to compare configuration states over time. As an automated solution, Industrial Defender automatically detects system changes and provides additional insights on their impact on your operations, security and/or compliance. By continuously monitoring against configuration baselines, you will always be aware of any configuration drift.

Ready to learn more about how Industrial Defender can help with your specific needs?

Visit our [website](#) or connect with your representative to discover how we can safeguard your operations and help you achieve your goals.

The Industrial Defender Difference

Industrial Defender is the single best source of OT asset data needed to protect industrial operations. 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. Organizations leverage Industrial Defender's platform as a single source of truth for all operational asset information, enabling them to achieve key goals in OT asset management, change and configuration management, vulnerability management, and policy compliance. Serving customers globally across all OT-intensive sectors, Industrial Defender supports the safety, availability, and security of critical infrastructure and industrial operations. Learn more at IndustrialDefender.com.

[Schedule a demo](#)

For more information

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