Indegy
Activate All Your Senses

Indegy Device Integrity

The Most Advanced Active Detection Solution For Industrial Security Environments

This document will explain the OT challenges faced by IT security teams. It will outline why you need Indegy Device Integrity, how it works, what it delivers, why it's safe and the available options for implementation.

The Industrial Cyber Security Challenge

Today's sophisticated Operations Technology (OT) environment has a large attack surface with numerous attack vectors. Without complete coverage, the likelihood of getting attacked is not a matter of 'if'; it's a matter of 'when'.

For security and SOC teams, network monitoring is not enough. You need the ability to access the details that provide in-depth visibility into the industrial control system (ICS) environment. Without it, you can only hope your industrial control devices have not been compromised by unauthorized activities or external threats. In these environments, substantial amounts of data reside on a variety of different devices. Much of that data, does not traverse the network.

Critical asset inventory information like records of user log-ins and controller firmware versions, as well as changes to devices made via direct connections, don't typically present themselves in network traffic. If network monitoring missed an attack on a device, it can remain infected for days, weeks, or months without detection. In fact, network monitoring only provides operators with 50% visibility and coverage across the OT environment. You need to see it all and Indegy enables you to activate access to all the data you need.

Are you missing half
of what you need to see?

WHAT INDUSTRIAL CYBER SECURITY PROFESSIONALS NEED

- Timely situational awareness of your OT network
- Vital up-to-date data on all assets, vulnerabilities and security risks
- Alerts to any changes made to control devices via direct physical connections
- Details – e.g. operating systems, firmware, configurations, ladder logic and more
- More contextual meaningful alerts; fewer false positives

WHY DEVICE INTEGRITY CAPABILITIES ARE CRITICAL

- Network sniffing alone cannot collect the information essential to industrial security
- Network alerts must have additional context for more efficient incident response
- Discovery of non-communicating devices is paramount to complete security
- Any change, even if done directly onto a device, must be visible
- OT devices mandate read only communications in their native language protocols

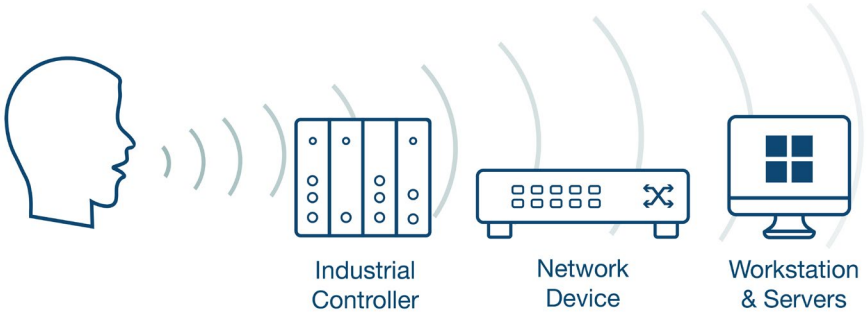
Network monitoring only provides operators with 50% visibility and coverage:

Much of the data, does not traverse the network

How Indegy Device Integrity Works

In February 2016, Indegy introduced the industry's first active detection solution for industrial security environments. Indegy Device Integrity is part of the Indegy Industrial Cyber Security Suite. While the Basic Edition of the Indegy Industrial Cyber Security Suite provides an option for passive-only detection, the Preferred and Enterprise Editions include Device Integrity. Indegy's patent-pending active detection technology provides organizations with complete security coverage by surveying the Industrial Control System (ICS) network – including all its devices. Using the devices' native communication protocols, Indegy Device Integrity discovers and classifies all ICS assets even when they are not communicating in the network. In querying all the device's meta-data and configuration, it can provide insights and alerts to changes in configurations and risk factors that can impact industrial operations. This technology has no impact on network operations and augments network sniffing by collecting information that is impossible to find in the network; yet crucial to protect the OT environment.

To ensure the integrity of your industrial network, you must identify every change made to every device in your network: from operating systems and software, through firmware and configurations, all the way down to ladder logic.



Indegy Device Integrity automatically and proactively:

- Discovers and classifies all ICS assets, including lower-level devices like PLCs, RTUs and DCS controllers – even when they're not communicating in the network by leveraging unique native broadcast packets
- Identifies changes in the device's metadata (e.g. firmware version and configuration details) as well as changes in each code and function block in the ladder logic and critical memory segments
- Amplifies detection through dedicated vendor specific, native, read-only protocols which yields a more comprehensive collection of information compared to the generic use of SNMP or Modbus

Indegy Device Integrity knows what you need to have:

- Creates a full snapshot of the controller at a specific point in time
- Compares it to previous baselined snapshots to validate the device's integrity
- Provides comprehensive detailed information about any configuration changes

Using the devices' native communication protocols;

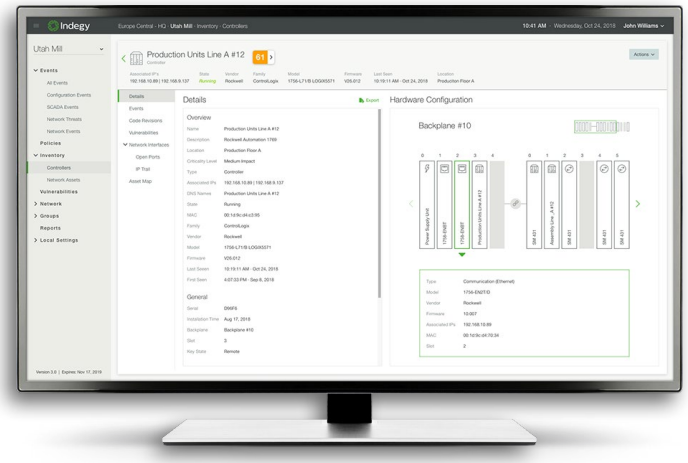
Indegy Device Integrity discovers, classifies and provides rich details for all your ICS assets

What Indegy Device Integrity Delivers

In-Depth Enterprise Visibility

Delivers the industry's most comprehensive set of critical information for industrial environments - faster.

Asset Management is key for being in control of your environment. The problem is that the most important asset data does not normally flow in network communications. Details like the logged in user or latest hotfixes installed on PCs and Servers, or the firmware version and open port list of a PLC/DCS controller, are stored within the devices themselves and typically have no reason to be transmitted. Indegy Device Integrity solves that problem by querying the devices and automatically gathers the most intimate, comprehensive and critical information about every asset in your environment, providing you with the ultimate asset management and visibility capabilities.



Enterprise-wide landscape with drill-down views of current status and alerts.

Greater Efficiency for Incident Response

Provides improved situational awareness with critical context.

Alerts can be meaningless without added contextual information such as "who is the logged in user to the engineering station at a specific time" and "what was the impact of specific activity to the PLC ladder logic". When Indegy's Industrial Cyber Security Suite detects a suspicious network event, Device Integrity kicks into action. By using native protocols, it automatically queries the relevant devices to gather further contextual details. This provides more meaningful alerts compared to a passive-only solution and results in significantly improved situational awareness and quicker forensic and mitigation activity. It also frees up time for the Incident Response (IR) team.

Insight into Vulnerability and Risk

Ensures you have up-to-date vulnerability management and risk posture.

By regularly querying the servers and controllers for details such as the OS & firmware version, open ports, latest software, hotfixes, hardware configuration, patch level and more, Indegy's Industrial Cyber security Suite ensures complete awareness of the most current vulnerabilities that may put the industrial controllers at risk. First, this provides more accurate risk scoring which is augmented based on non-networked data. Second, Indegy does not wait for device information to be passed over the network. Instead, it requests it to provide you with the most updated and accurate information on the device.

Asset details, Enhanced Alert Context, and Risk Scores:

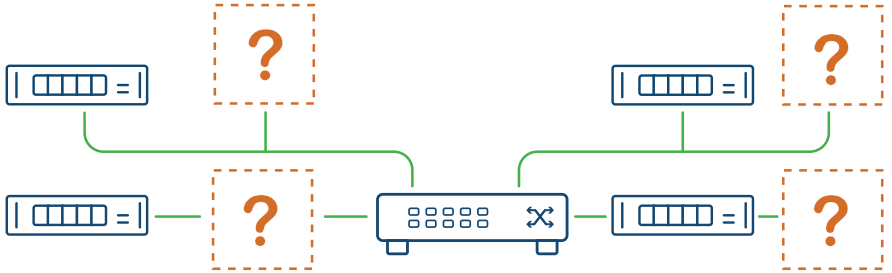
See the difference with Indegy Device Integrity

What Indegy Device Integrity Delivers

Safeguard from Malicious Insiders and Human Error

Validates controller integrity by identifying changes made via direct physical connections.

It is very common for employees, contractors and integrators to connect to control devices using a serial cable or USB. A malicious actor that has physical access to the network can also connect to controllers this way. Changes made to the controller code, firmware or configuration - whether authorized or not - cannot be detected by network monitoring. It is also plausible that an employee or contractor unknowingly exposed controllers to threats by using a compromised device, for example a laptop or USB drive infected with malware. By periodically capturing device snapshots and comparing them to previous baselines, the Indegy Industrial Cyber security Suite can identify changes and validate that the integrity of the device is not compromised.



Capture of “Blind Spots”

Discovers assets that do not communicate over the network.

Device Integrity discovers dormant industrial devices that are connected to the network but are not communicating. Most industrial control vendors support a “find me” mechanism built into their controllers that allows detecting them with a single broadcast of a unique packet. This is how engineering stations can find all controllers in the network automatically. Device Integrity uses that same built-in mechanism to make sure your asset inventory is complete and accurate.

Alerts you of any change in your industrial environment:

Including changes by insiders and third parties directly on your devices and not through the network

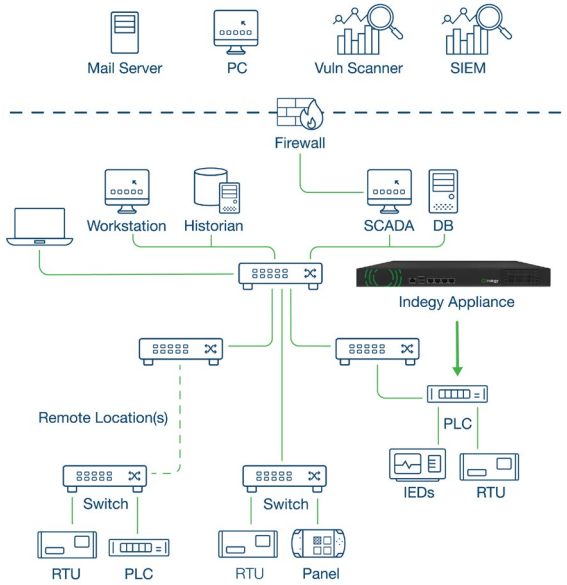
What Indegy Device Integrity Delivers

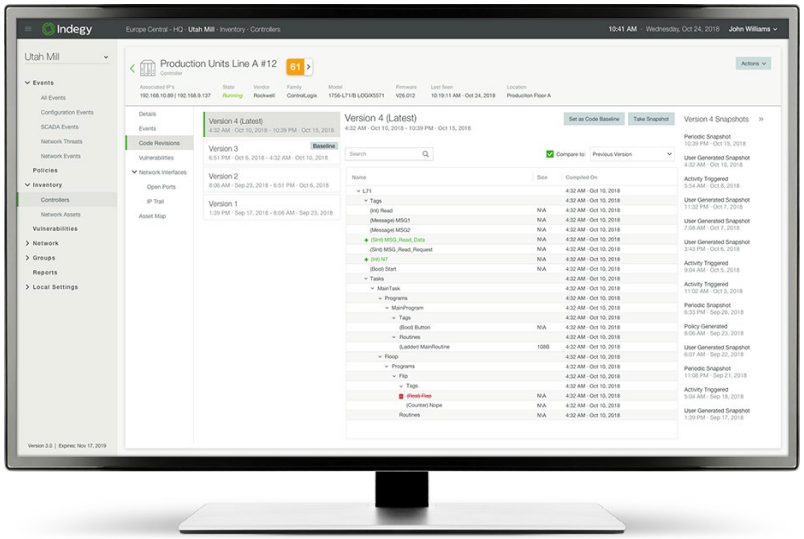
Lower Total Cost of Ownership (TCO)

Architected to provide optimal efficiency and value.

A major disadvantage of network-only technologies is the necessity to deploy them at every intersection and switch of the network you want to monitor. This can be very expensive for a large environment with multiple subnets. The typical response to save hardware and maintenance cost is to deploy fewer appliances in the network. Too often, this results in a sacrifice of control and/or visibility when using a network-only approach. Device Integrity technology, however, provides the ability to monitor all routable sections of the network with one single Indegy appliance.

Imagine knowing every detail of what's in your OT network, seeing it all in a single pane of glass – and reducing your footprint for hardware and maintenance costs significantly.





Comparing two device snapshots identifies changes to the controller logic.

Operations Network Resiliency

Preserves data to deliver holistic back-up and recovery.

Unless there is backup that traces the changes made to control devices, incident recovery can be very difficult. With Indegy Device Integrity, we enable you to simplify architecture and reduce costs at the same time. For Device Integrity, keeping track of changes also means preserving data of what was there before. By capturing a complete snapshot of the device including firmware, configuration, complete ladder logic, diagnostic buffer and tag structure, Indegy's Industrial Cybersecurity Suite keeps track of all versioning history of the controller and can help identify a previously known "good" state. Note that Indegy's Device Integrity does not actively push the snapshot or make any changes to recover the device.

Architected for Simplicity, Precision and Value:

Delivers greater deployment efficiency with ability to recover using configuration snapshots

Indegy Brings You Safe, Smart Active Detection

Indegy patent-pending technology uses read-only queries in the native device communication protocols, so there is no impact on the devices being enquired.

How does Indegy Device Integrity do that?

Devices are queried only in native language, when positively identified

Indegy Device Integrity never uses communication protocols that the device might not support or that are not native. It also never "blindly scans" the network looking for devices. Only after positively identifying a specific asset down to the vendor model and version, Device Integrity will activate and start querying that asset to gather information.

Industrial Controllers are accessed only as they are designed

Most of the industrial controllers use different electronic modules for different purposes. Consequently, ethernet based communication, with engineering station software are executed by the networking module and aren't part of the critical control loop. Additionally, mission critical I/O activity has its reserved processing resources, which prevents a network traffic overload. If the controllers aren't being exploited or maliciously scanned, an overload will not occur.

Schedules and policy settings are customizable to your business needs

Choose your query frequency: every 8 hours, only at specific times of day, for specific subnets, or only by manual activation. With Indegy, it is possible to customize policies to query only predefined set of IP ranges or asset types. It is also possible to check the network load and CPU load on the devices before surveying them.

Activity is Read-Only, Out of band

Indegy Device Integrity utilizes 100% read-only communication and by design, does not have the ability to change configurations and settings of any of the devices in the network

Approach is vendor agnostic

Indegy works closely with controller vendors and performs extensive lab tests with physical devices to ensure that queries have no impact on the controllers and do not have the potential to cause any disruptions.

ABOUT ACTIVE-BASED TECHNOLOGY

History has taught us that the only way to effectively monitor devices, whether for security or for operations is by actively communicating with them. Below are some examples.

IT SECURITY

These breakthrough security technologies began in a passive mode and today are relied on for active threat hunting.

- Intrusion Detection Systems (IDS) communicate with endpoints
- Deception technologies communicate with assets
- Anti-viruses and firewalls sharing information between devices

OPERATIONS

Here are some operations technologies that are and have always been active based.

- 100% of OT tools used to monitor the process environment are active by nature
- HMI and SCADA software query PLCs, RTUs and DCS controllers
- Active directory, DHCP & even DNS servers

Indegy is the originator of this technology with a patent pending:

Large to small organizations worldwide trust Indegy Device Integrity

Indegy Industrial Cyber Security Suite

Device Integrity is part of Indegy's holistic hybrid detection solution for the comprehensive protection of industrial environments. It is included in both the Indegy Preferred and Enterprise Editions and can also be purchased as a standalone option for customers (with Indegy Basic Edition which provides the option for passive only detection).

Customizable Packages

Indegy *Basic* Edition

Customizable Packages

- Indegy Security Platform
- Indegy Core Software
- 5 Indegy Sensors

Passive Detection Only

Indegy *Preferred* Edition

Customizable Packages

- Indegy Security Platform
- Indegy Core Software
- Indegy Device Integrity
- 20 Indegy Sensors

Hybrid Technology: Passive with Active Detection

Indegy *Enterprise* Edition

Customizable Packages

- Indegy Security Platform
- Indegy Core Software
- Indegy Device Integrity
- Unlimited Indegy Sensors
- Indegy Enterprise Mgmt
- Managed Security Service

Hybrid Technology: Passive with Active Detection

Optional: Stand alone Risk Assessment Service

Products

Appliance

- Indegy Security Platform C1000
- Indegy Security Platform V1000
- Indegy Sensor RS100- Rack Mount
- Indegy Sensor DS100- DIN Mount Rail

Software

- Indegy Core Software*
- Indegy Device Integrity Software
- Indegy Enterprise Management Software

* Included with Indegy Security Platform

For more information, contact us at: info@indegy.com
Or visit us at: