Indegy
Industrial Cyber Security

ForeScout

Joint Solution for OT Network Security, Visibility and Control

Today more than ever, industrial environments are of critical concern when it comes to cyber security protection. Indegy and ForeScout provide critical visibility and security into the IT and OT devices on industrial networks.

The Challenge

Unlike IT networks, Industrial Control Systems lack a proper foundation of visibility and security controls. Most devices don't require authentication, making it difficult to prevent unauthorized access or changes to critical devices. In addition, there are no event logs or historical data to help with event detection and response. Without this proper foundation of visibility and control, added challenges emerge in managing assets, detecting threats, and managing systems configurations in OT environments.

Managing IT and OT Assets in Industrial Networks

Since industrial networks lack access controls to restrict the activities of unknown devices connected to the network, new unmanaged connected devices can potentially introduce threats into these sensitive environments.

The lack of automated asset discovery and management is also at the root of many operational incidents resulting from contractors, integrators or employees working on the wrong assets. Such incidents could result in severe operational disruptions.

In addition, an unmanaged asset inventory is harder to support and maintain since it is not always clear which assets should be upgraded or patched, or which spare parts are needed. What's more, an accurate inventory is essential to meet regulatory and compliance mandates.

Existing solutions fall short.

Traditional IT

- No coverage of OT assets for vulnerability and configuration
- No visibility into the unique patterns and protocols of ICS attack traffic

Network only OT solutions

- Blind to local maintenance modifications
- Lack context of endpoint state during attack
- Inability to gather reliable patch levels

THE SOLUTION

The joint Indegy® - ForeScout® solution offers visibility and security for industrial networks, enabling security professionals to effectively detect and mitigate threats to the safety, reliability and continuity of industrial processes. The monitored devices include traditional operating systems such as MS Windows or Linux based systems, as well as mobile devices, OT and IOT devices.

KEY BENEFITS

- Threat Detection & Mitigation that combines behavioral anomalies with policy-based detection.
- Asset Tracking that goes as far as dormant devices and as deep as PLC backplane configurations.
- Vulnerability Management that tracks and scores patch & risk levels of ICS devices.
- Configuration Control that tracks all changes to code, OS & firmware regardless if done through the network or locally.
- Enterprise visibility to ensure that all data collected integrates to your single pane of glass.

Detecting Threats to Operational Environments

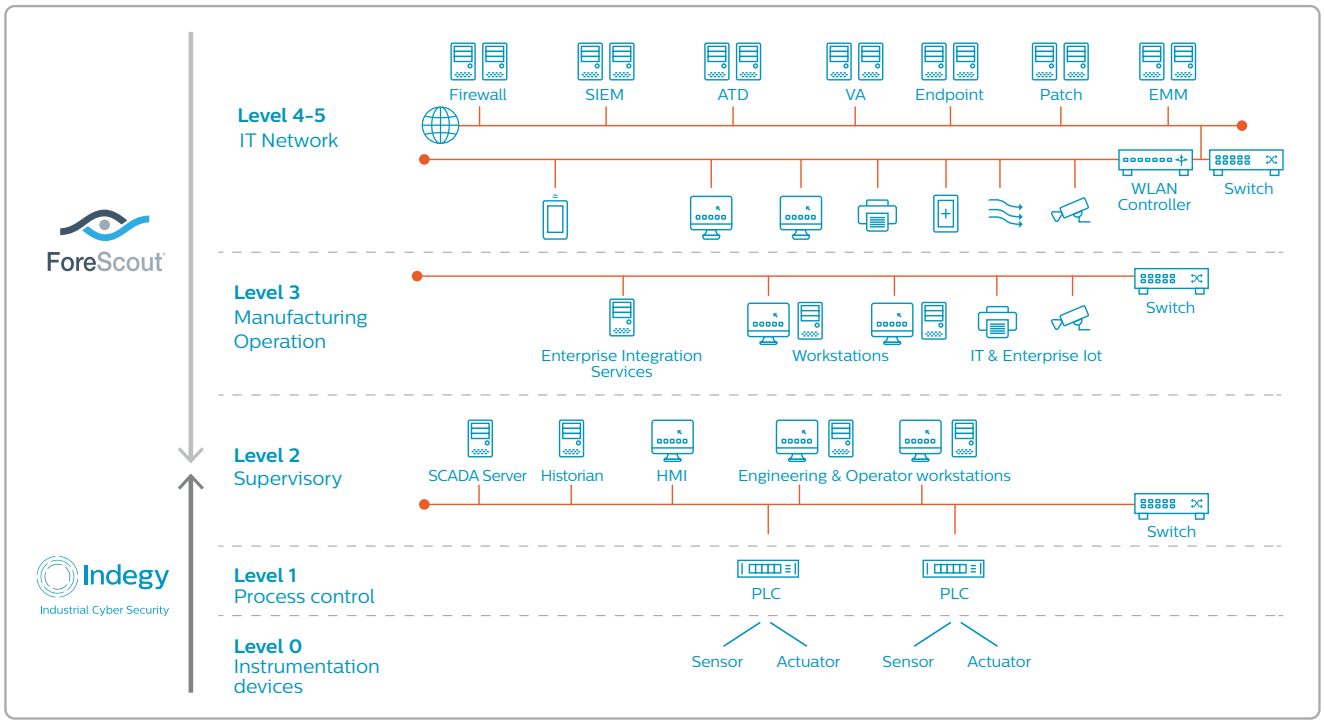
As more and more industrial networks are connected to corporate environments and cloud services, risk exposure increases. Since ICS environments are very different from IT environments, and use proprietary protocols, IT security solutions like firewalls and intrusion detection solutions (IDS) lack the technologies needed to detect threats. In addition, the critical control devices lack event logs, so tracking operational and security events is nearly impossible.

Validating Configurations and Managing Changes

The configuration settings of controllers directly impact the industrial processes they manage. Any unauthorized change to the code, configuration or firmware can result in down time, severe disruptions or damaged equipment. Without the historical information of past configurations, it is also impossible to restore a controller to a previously known good configuration after an incident.

The Joint Solution

The Indegy-ForeScout joint solution enables industrial organizations to manage IT and OT devices: While ForeScout covers devices in layers 3, 4 and 5 of the Purdue Model, Indegy covers layers 0, 1 and 2. Together, the solutions deliver visibility and control, while enabling incident detection, incident response and effective mitigation.



Use Case #1:

Consolidated IT-OT Asset Discovery and Management

The joint solution automatically discovers IT, IoT and OT devices and provides a consolidated view of the assets across IT and OT environments. It continuously updates the asset inventory to ensure accurate, up-to-date asset management; ForeScout real-time visibility into all enterprise IT and IoT assets while the Indegy Security Suite discovers networked controllers (PLCs, RTUs and DCS controllers) and other ICS devices. Together, the solutions provide visibility into device properties, classification, configuration and network context in a single-source-of-truth asset repository.

Use Case #2:

Real-Time OT Threat Detection

The Indegy Security Suite identifies threats to OT networks and sends real-time alerts to the ForeScout console, providing organizations with a consolidated view of alerts across IT and OT environments. The integrated solution extends threat detection capabilities to include:

- Reconnaissance activity in OT networks
- Malware propagation across the network
- Unauthorized or abnormal communications
- Unauthorized attempts to read controller configuration, setting or code
- Attempts to change critical controller configuration, code or firmware

Visibility is key for security: you can't protect what you can't see...

Use Case #3:

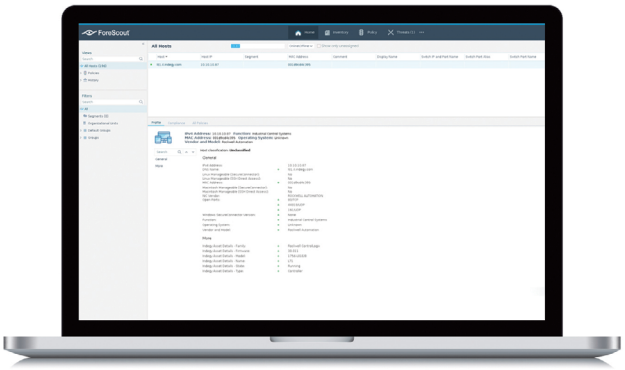
Configuration Validation and Change Management

Both Indegy and CounterAct perform deep endpoint inspection without an agent on the devices. This enables organizations to capture in real-time changes to IT devices, IOT devices and level 2-3 OT devices, including industrial controllers, and supports the implementation of change management processes across the entire organization. Historical information about previous configurations is kept in case there is a need to restore a device to a previously known good configuration.

Use Case #4:

Addressing Compliance Regulations and Security Frameworks

Compliance with industry regulations and security standards like NIST, NERC, ISO/IEC 27001 and similar frameworks worldwide requires effective, automated asset discovery and ongoing management of the asset inventory. The Indegy and ForeScout joint solution enables organizations to simplify compliance efforts and automates reporting across their enterprise IT, IoT and OT environments.



Consolidate views of all IT and OT assets

The Indegy and ForeScout solutions work together to offer extended visibility and security to industrial networks. Using this joint offering, operators can mitigate security threats and achieve a safer and more reliable environment, protect it from operational disruptions and assure zero down time.