

Cisco **Cyber Vision** identifies your Operational Technology (OT) assets, their characteristics, and their communication patterns by passively capturing and decoding industrial application flows. This ultra-safe approach can be enhanced with active discovery that sends requests in the semantics of the specific ICS protocol at play.

Benefits:

Gain OT visibility at scale: Easily identify all industrial devices and their communication patterns. Cyber Vision is embedded in your industrial network.

Understand your OT security posture: Reduce the attack surface. Cyber Vision highlights devices that need immediate attention and suggests solutions.

Improve operational efficiency. Reduce downtime and improve efficiency. Cyber Vision monitors OT events, identifies network problems, and helps you troubleshoot issues faster.

Extend IT security to OT: Converge your security practice. Cyber Vision feeds your IT security tools with rich details on OT devices and events.

Vulnerability Detection: Identify known asset vulnerabilities so you can patch them before they are exploited.

Risk Scoring: Asset risk scoring based on impact and likelihood to help you improve compliance.

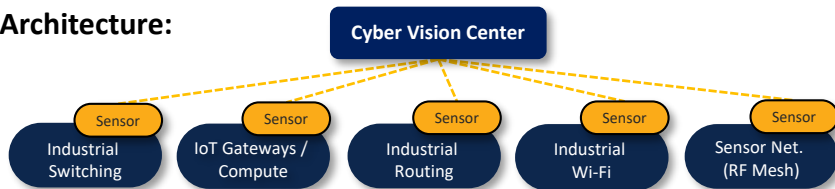
Anomaly Detection: Detect attempts to modify OT assets with behavioral analytics, create baselines to detect deviations.

Intrusion Detection: Detect intrusions with snort IDS and Talos intelligence.

Conversation Starters:

- How do you know your IDMZ is effectively protecting your OT domain?
- Do subcontractors have unauthorized remote access to your assets?
- Do you know if you are missing critical security patches?
- Are there decommissioned assets still connected to your network?
- Can you track unwanted asset modifications such as variable changes or program uploads?
- Can you identify which industrial machines use outdated software and are you able to detect malware and other threats to these machines?

Architecture:



Solutions:

Cyber Vision Center options:

- **Hardware Appliance:** USC based server with hardware RAID
- **Software Appliance** (virtual): VMWare ESXi & Hyper-V VHD
- **Cloud Appliance** (virtual): Amazon Web Services (AWS) & Microsoft Azure

Cyber Vision Sensor options:

- **Network Sensors:** Embedded in networking for simple highly scalable deployment
 - Cat [IE3300](#), [IE3400HD](#), [IR1101](#), IR8300 & 9300/9400, [Stratix 5800](#)
- **Hardware Sensor:** Capturing traffic on any switch with a single hop SPAN
 - [IC3000](#) Industrial Compute (DPI via SPAN to support brownfield)
- **On-Center Sensor:** Existing SPAN infrastructures or collect traffic within datacenter.

Licenses: (CV-LICENSE)

Essentials:

Inventory:

- Device inventory
- Identify communication patterns
- Generate inventory reports

Vulnerability:

- Identify device vulnerabilities
- Generate vulnerability reports

Activities:

- Track control system events
- Generate device activity reports

Restful API:

- REST API interface

Advantage: (Essentials package + the following)

Security Posture:

- Device Risk Scoring

Intrusion Detection (IDS):

- Snort IDS on supported sensors
- Talos community signatures

Behavior Monitoring:

- User-created baselines for asset behaviors
- Alerts on deviations

Advanced integration:

- pxGrid integration with [ISE](#)
- Firewall Mgmt ([FMC](#)) Host Attribute integration
- SIEM Integration – [Splunk](#), [IBM QRadar](#)
- [ServiceNow](#) OT Management integration

IT vs OT:

IT Security = Cybersecurity	➔	OT Security = Safety
IT networks are segmented	➔	OT networks are flat
IT devices are modern and controlled	➔	OT devices can be 10-20+ years old
IT attacks can be well identified (virus, DoS...)	➔	OT attacks look like legitimate data to ICS
IT cares about Confidentiality and Availability	➔	OT cares most about Throughput and Uptime

Resources:

[SalesConnect](#)
[Ordering Guide](#)

[User Guides](#)
[Data Sheets](#)

[At-a-Glance](#)
[PoV Guide](#)

[Selling Guide](#)
[Protocol support](#)
[Overview/Demo](#)

[Guided Demo](#)
[IoT Security](#)
[Public page](#)