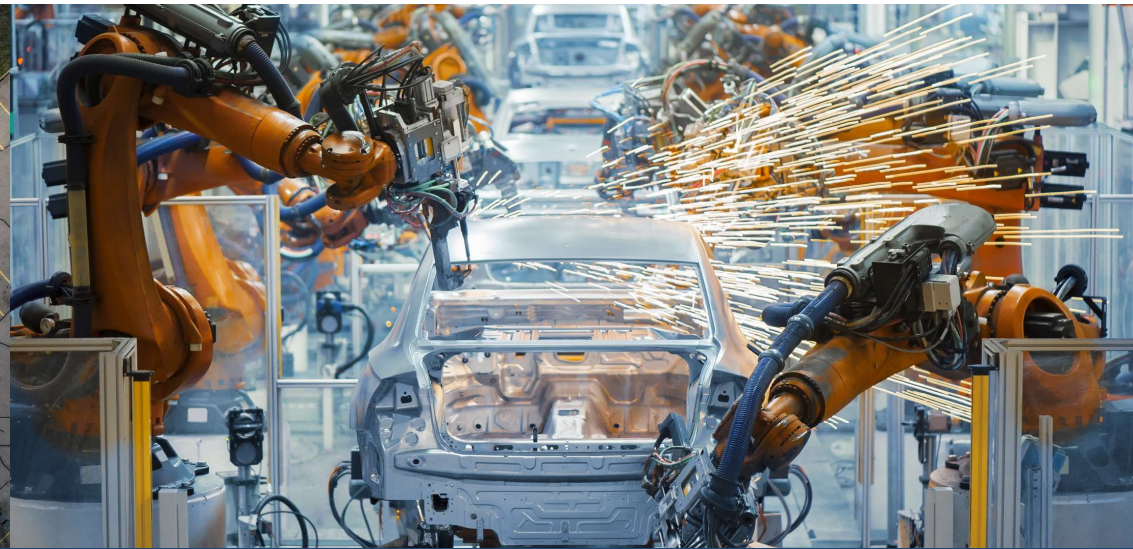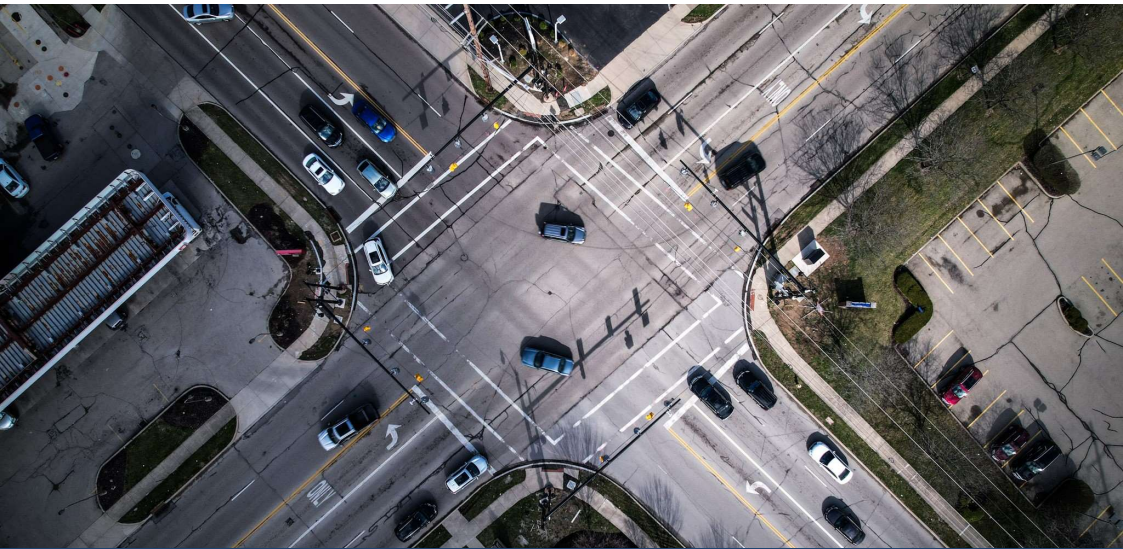# Secure Industry 4.0 with Cisco IoT

Driving Digitalisation and Securing OT Networks

Natalia Chadwick
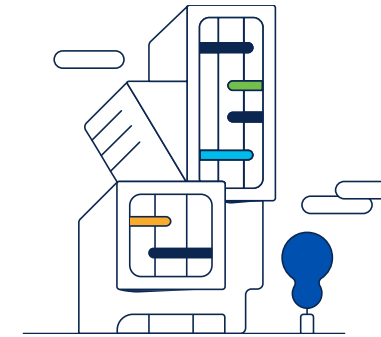IoT Channel Sales Lead – UKI & Northern Europe
April 2023

The heart of your business is the edge. And everywhere is digitizing

Only Cisco IoT solutions meet the needs of IT and operations

Industrial Grade
Purpose built for Operations

+

Enterprise IT Grade
Leverage existing knowledge and investments

- Built for harsh and outdoor environments
- Industry use-cases and certifications
- Industrial protocol support and integrations
- Machine data and control

- Industry-leading end-to-end Cisco security architecture
- Less complexity at scale: one network architecture
- Consistent commercial model – software, licensing

Cisco Catalyst
Industrial Networking

IoT Networking + Security Portfolio

Industrial Switching
1K, 2K, 3200, 3300, 3400, 3400H, 4K, 5K, 9K

Industrial Routing
IR1101, IR1800, IR8100, IR8300, CGR1120, CGR1240, CGR2010, IoT Gateways (IG21, IG21R, IG31R)

Embedded Networking
ESS, ESR, ESW, Resilient Mesh

Industrial Wireless
Cisco Ultra-Reliable Wireless Backhaul, IW6300, IW3702, IR5XX, IXM Gateway, IW9167

Industrial Cybersecurity
Cyber Vision, ISA3000 Industrial Firewall

Sensor   Sensor   Sensor

Data Control and Exchange
Edge Intelligence, IOx

Industrial Sensor Solution
Industrial Asset Vision

Management & Automation
Field Network Director, IoT Operations Dashboard, Cisco DNA Center

Cisco has led the way
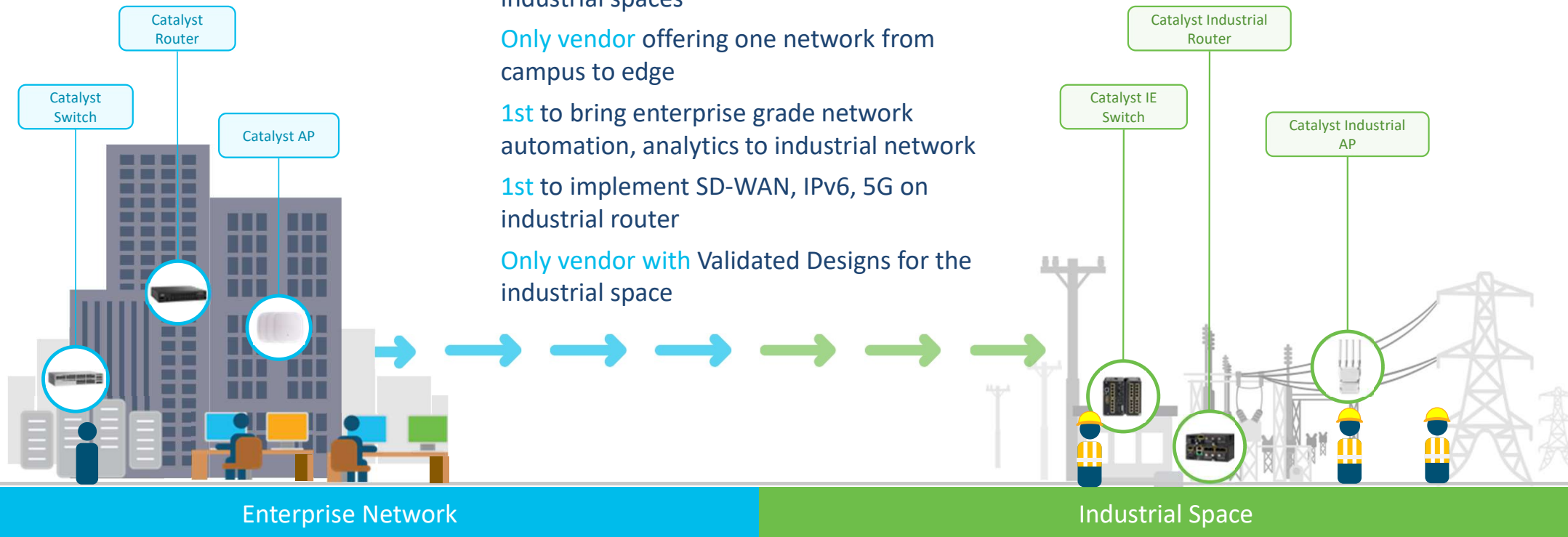## Bringing enterprise grade networking to the industrial space

1st to bring enterprise grade security to industrial spaces

Only vendor offering one network from campus to edge

1st to bring enterprise grade network automation, analytics to industrial network

1st to implement SD-WAN, IPv6, 5G on industrial router

Only vendor with Validated Designs for the industrial space

Catalyst Router

Catalyst Switch

Catalyst AP

Catalyst Industrial Router

Catalyst IE Switch

Catalyst Industrial AP

Enterprise Network

Industrial Space

OT networks can benefit from enterprise capabilities
Helping to avoid:

Less secure, unsegmented

Evolving threats

Air gapped, unsegmented or flat Layer-2 networks

Lack of asset visibility

Complexity at scale

Multiple vendors and networks

Multiple touch points
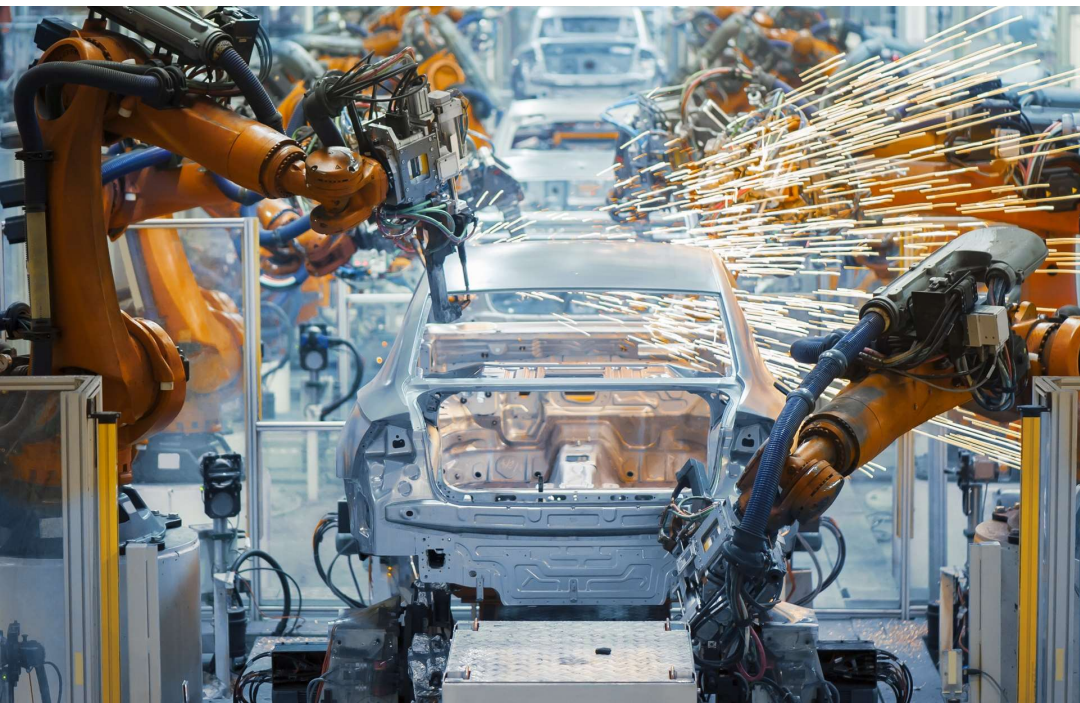
Multi-step, complex interactions

Difficulty resolving issues

Poor network visibility

Long outages due to reactive troubleshooting

Manual processes

Talent shortages compound the issue – IT/OT need enterprise capabilities to keep up

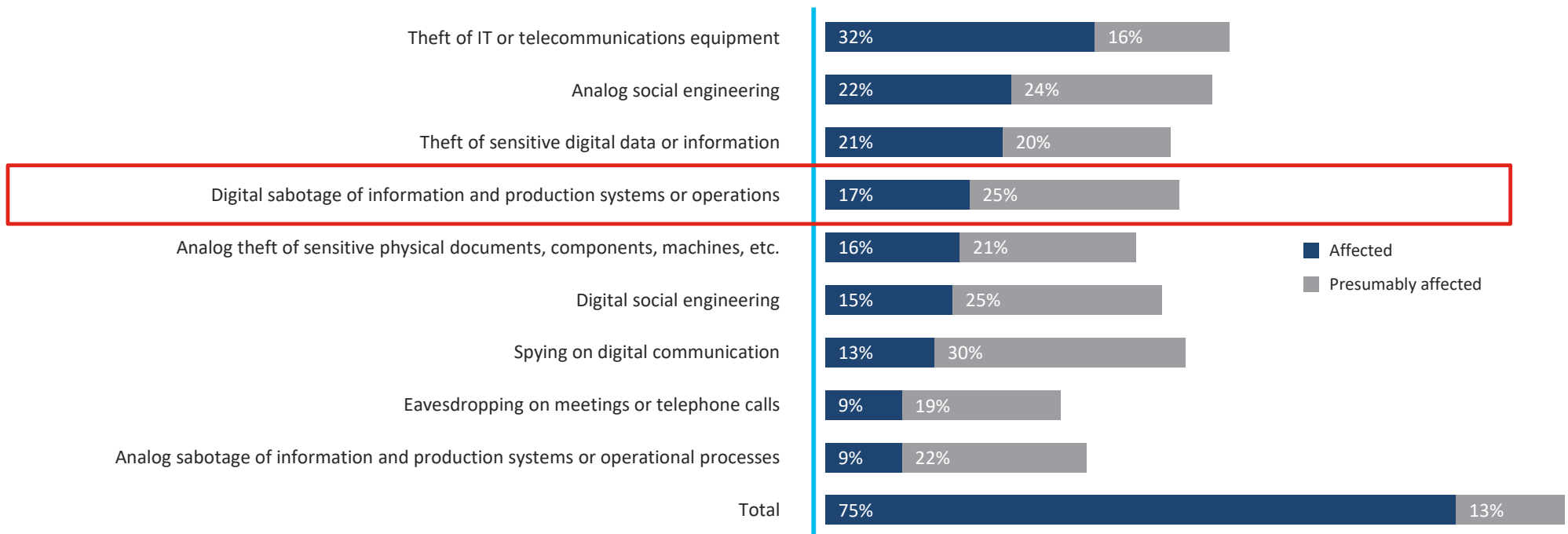# Industry digitization brings new requirements and challenges

- Seamless communications between OT, IT and Cloud
- Network uptime and reliability
- Remote access/Hybrid work
- Cybersecurity

The role of IT is expanding to help manage and secure the industrial network

Cyber Risk

A closer Look - Even outside the top news, the threat is real

Which of the following digital or analog types of data theft, industrial espionage, or sabotage has your company been affected or likely to be affected by within the last two years?

Category	Affected	Presumably affected
Theft of IT or telecommunications equipment	32%	16%
Analog social engineering	22%	24%
Theft of sensitive digital data or information	21%	20%
Digital sabotage of information and production systems or operations	17%	25%
Analog theft of sensitive physical documents, components, machines, etc.	16%	21%
Digital social engineering	15%	25%
Spying on digital communication	13%	30%
Eavesdropping on meetings or telephone calls	9%	19%
Analog sabotage of information and production systems or operational processes	9%	22%
Total	75%	13%

Legend:
- Affected
- Presumably affected

Source: www.bitkom.org | Basis: All respondents (n=1.070)

Cybersecurity is a Journey

Full Spectrum Security

Foundation Security

Minimal Security

Step-by-step journey to limit complexity and embark all stakeholders

Critical need for visibility into industrial networks

| Identifying OT assets and their communications | Troubleshooting asset configuration issues | Improving network reliability and performance | Detecting intrusions and malicious traffic | Controlling remote accesses to engineering stations |

Visibility helps improves network hygiene, operational efficiency and security

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

Visibility
Asset inventory
Communication patterns

Security
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

Context and insights that are foundational to building reliable and secure OT networks

Enlist your OT network for security

Cisco Industrial switches and gateways **see everything** that attaches to them so you can gain **visibility at scale**
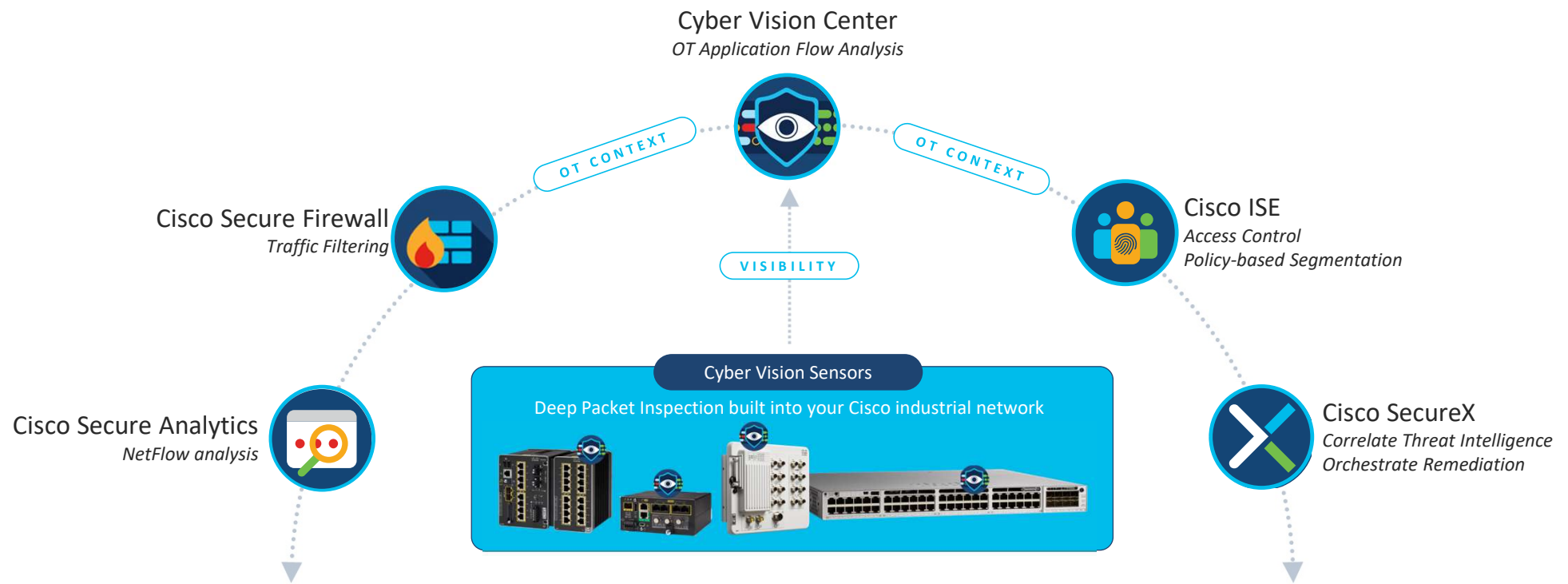
Cyber Vision Center

1 0 0 1
0 0 1
Application Flow Metadata

Cyber Vision Sensor

0 0
1 1 0

Deep Packet Inspection & Active Discovery
built into your network infrastructure

# Cyber Vision extends IT security to OT

Cyber Vision Center
OT Application Flow Analysis

OT CONTEXT

OT CONTEXT

Cisco Secure Firewall
Traffic Filtering

VISIBILITY

Cisco ISE
*Access Control
Policy-based Segmentation*

Cisco Secure Analytics
NetFlow analysis

Cyber Vision Sensors
Deep Packet Inspection built into your Cisco industrial network

Cisco SecureX
*Correlate Threat Intelligence
Orchestrate Remediation*

The broadest OT security solution on the market • Powered by Talos threat Intelligence

Foundational Components of Industrial Security
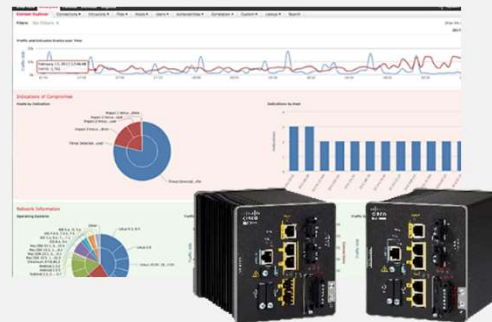

Detect

Cisco Cyber Vision
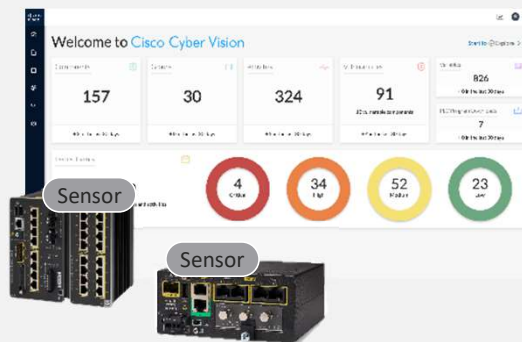
Maintain OT asset inventory

Assess industrial security posture

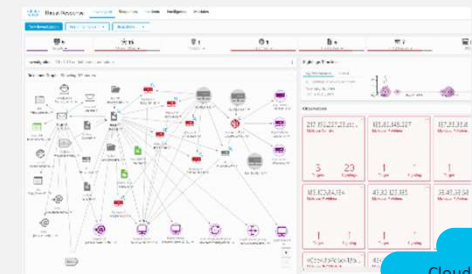Troubleshoot industrial processes

Protect

Cisco ISA3000 Firewall

Segment network and prevent threat propagation with best of breed industrial protocol IPS/IDS
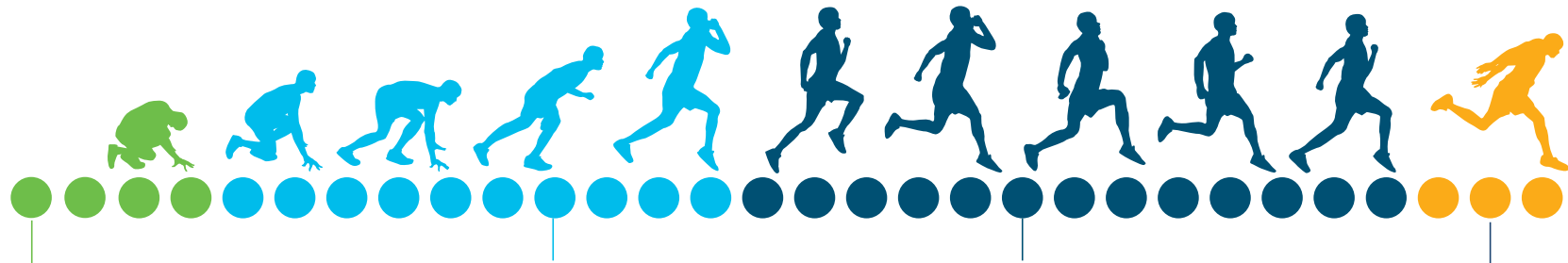
Investigate & Respond

Cisco SecureX

Enable security experts to investigate industrial threats and orchestrate response with playbooks

Powered by Cisco TALOS threat intelligence

A Complete OT Security Journey

Discover
- Catalog Asset Inventory
- Find them on the network
- Patch their vulnerabilities

Baseline & Segment
- Know who is talking to whom
- Baseline normal behavior
- Create segments based on communication patterns

Detect
Get alerts on violation to the baseline

Enforce
Automate enforcement to quarantine misbehaving assets

Cyber Vision
Vulnerability Detection

ISE - Centralized Segmentation Policy

Cyber Vision Anomaly detection

Cisco Stealthwatch

Firepower IPS
Zone Segmentation

Firepower/Cyber Vision
Intrusion Detection

Firepower NGFW

TrustSec
Micro Segmentation

AMP / Threat Grid Malware
Detection

Zero Trust Architecture

TALOS Threat Intelligence

Multi-Factor Auth

Only Cisco can support IT and Operations
Accelerate industrial digitization

Best of enterprise and industrial networks

Single architecture

IT teams - support operations without retraining

Ruggedized for any environment

Bringing IT & OT Security Together

Market leading industry expertise

#1 in market share across enterprise and industrial networking

Decades of experience

Resources to ensure success

Cisco Validated Designs

Award-winning dev program

CX services

330 specialized partnerships globally