



The bridge to possible

# Extending Zero Trust for Workplace to Industrial IoT

Securing the workplace in industrial networks

Tuan Nguyen  
Security Specialist  
July 2023



## Extending Workplace Zero Trust to Industrial Settings



Endpoint  
Visibility



Endpoint  
Compliance

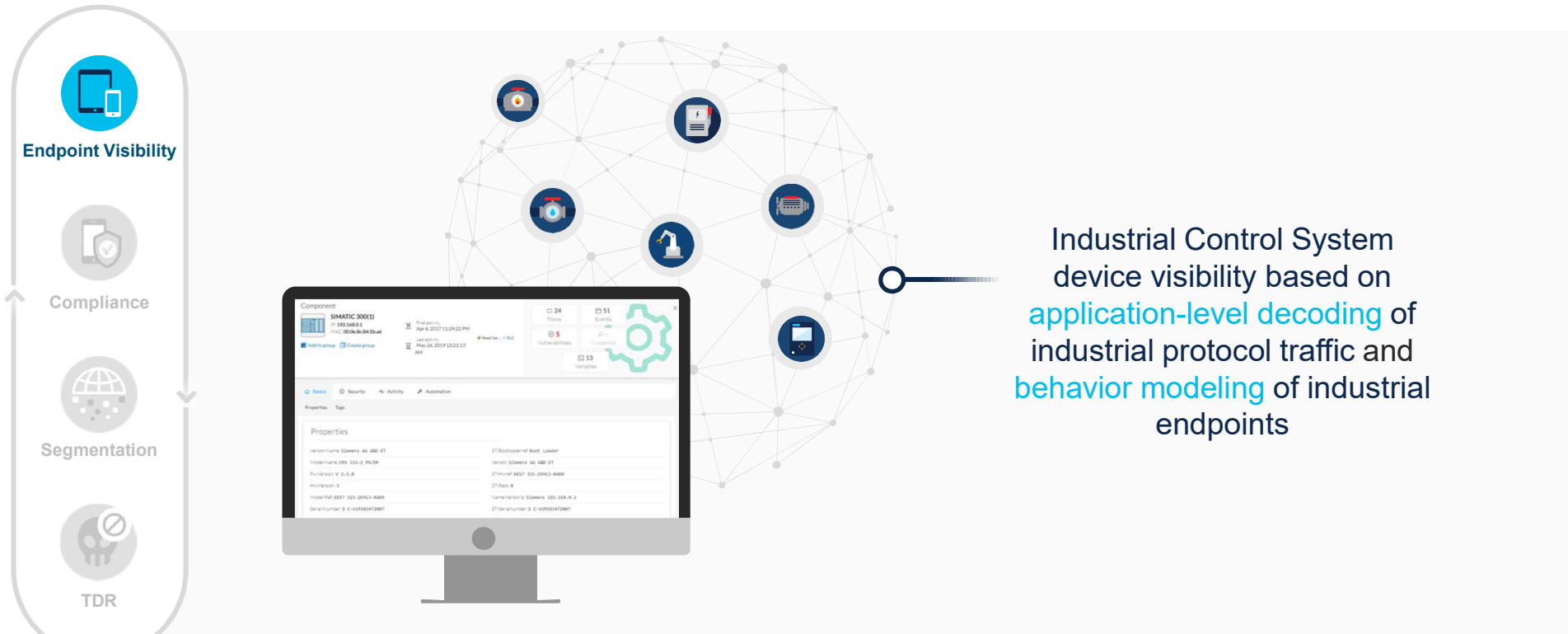


Network  
Segmentation

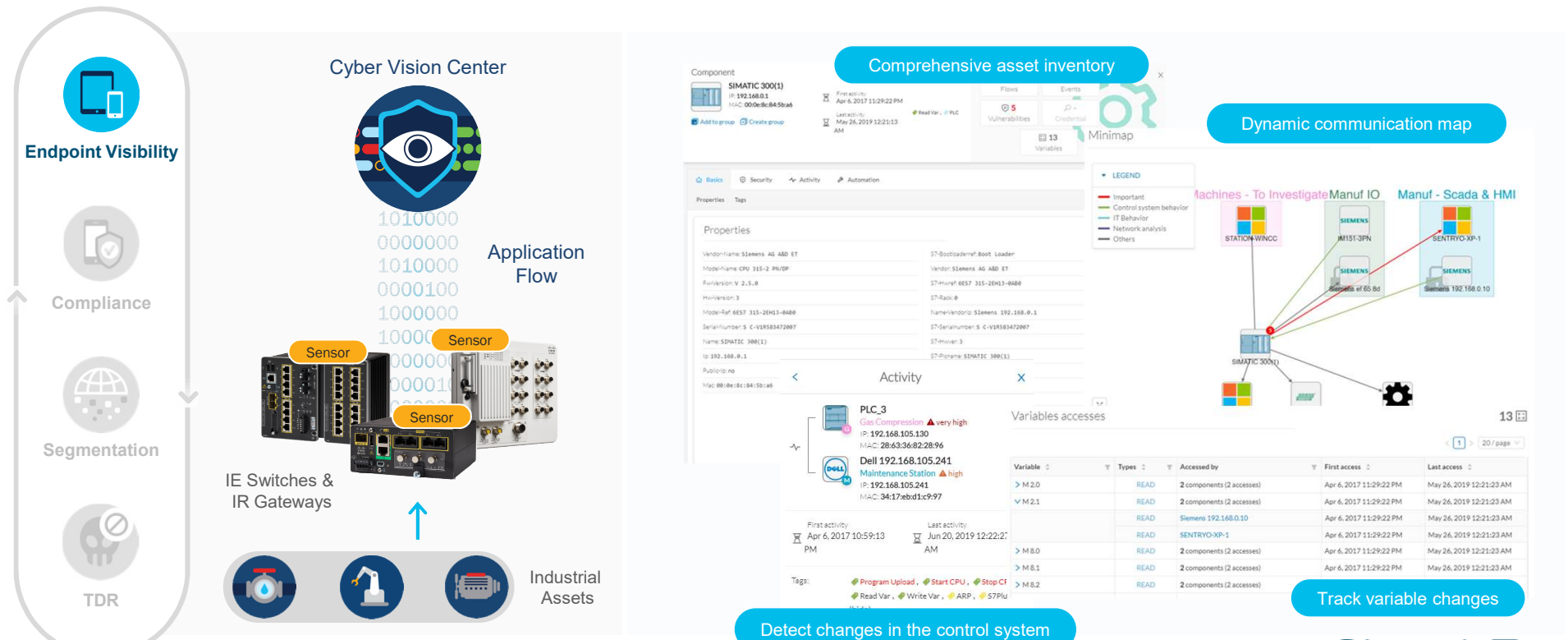


Threat Detection  
& Response

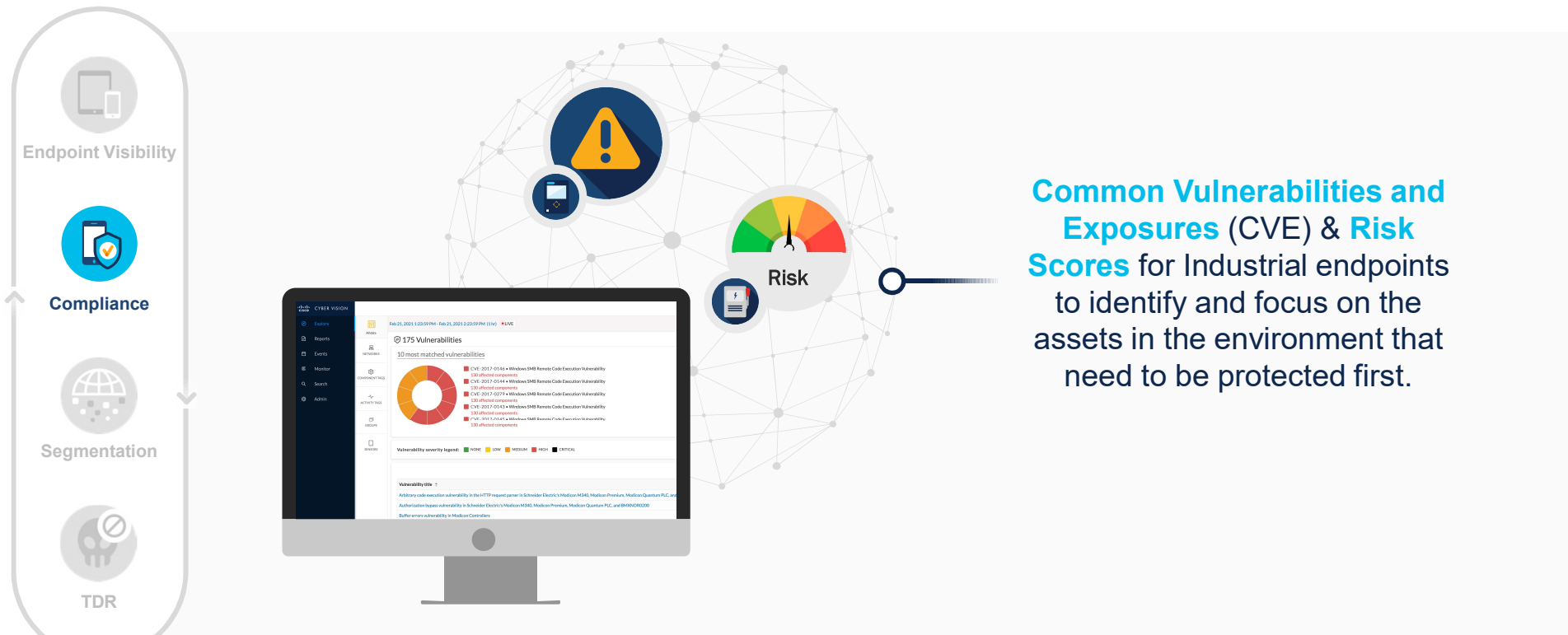
# Industrial Endpoint Visibility



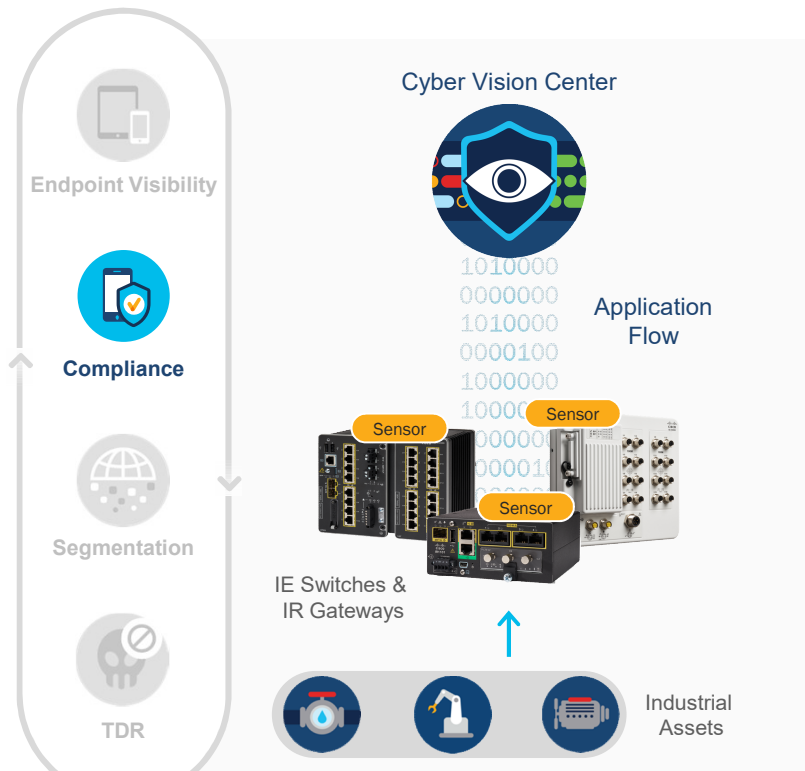
# Industrial Endpoint Visibility with Cyber Vision



# Endpoint Compliance for Industrial Endpoints



# Industrial Device Vulnerability Detection



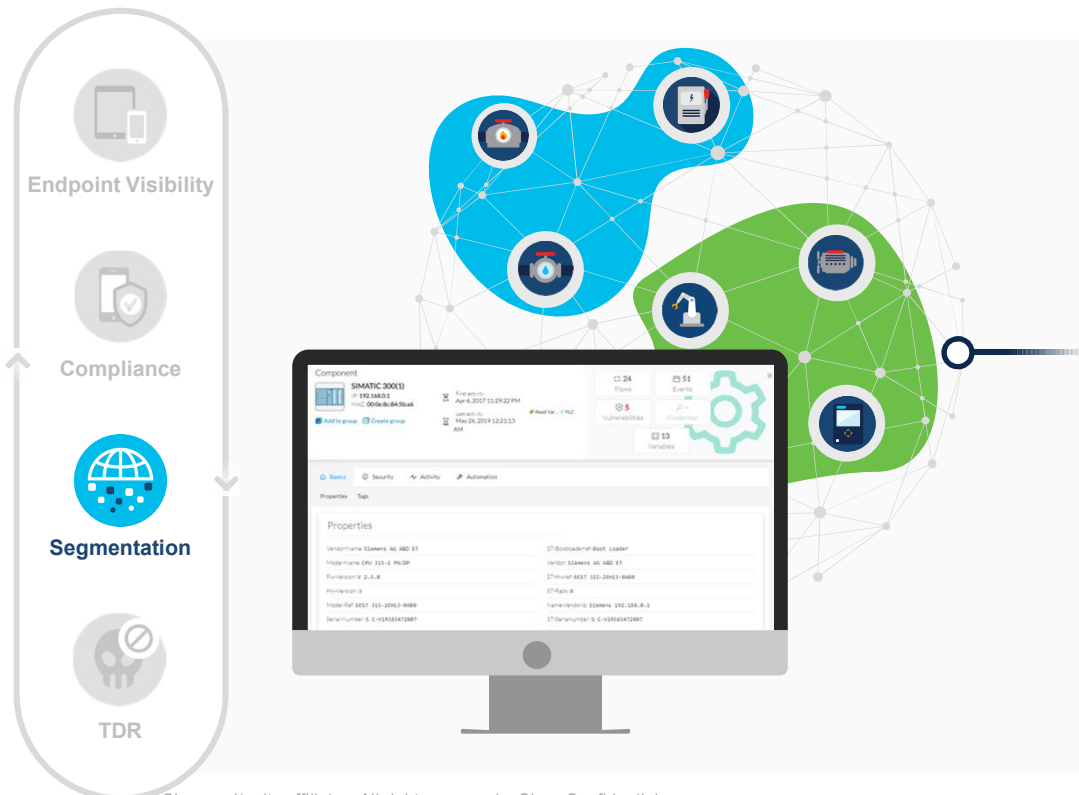
The screenshot shows the Cyber Vision interface for a specific subnet (192.168.1). It displays a summary of 73 vulnerabilities, a donut chart showing the distribution of severity levels, and a table of the most matched vulnerabilities. The table includes columns for vulnerability titles, CVE IDs, CVSS scores, and the number of affected components.

Vulnerability title	CVE	CVSS score	Affected components
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFNET Discovery and Configuration Protocol	CVE-2017-2680	6.5 (v)	3 components
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	7.5 (v)	3 components
Denial-of-Service Vulnerability in Profnet Devices	CVE-2019-10936	7.5 (v)	3 components
Yokogawa CENTUM BKHSimcore Stack Based Buffer Overflow Vulnerability	CVE-2014-0783	9.0 (v)	2 components
Yokogawa CENTUM BKFSim_vh1cLevel Buffer Overflow - Packet Storm	CVE-2014-3888	8.3 (v)	2 components
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032	5.9 (v)	2 components
Yokogawa CENTUM BKESimcore Stack Based Buffer Overflow Vulnerability	CVE-2014-0782	0.0 (v)	2 components
Vulnerabilities in SIMATIC 1200 and SIMATIC 57-1500 CPU Families	CVE-2019-10943	7.5 (v)	2 components
Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities	CVE-2017-6034	9.8 (v)	2 components

The interface also shows a 'Vulnerability severity legend' with categories: NONE, LOW, MEDIUM, HIGH, and CRITICAL. A summary box indicates '9 Total vulnerable components for 192.168.1 subnet'.

Cyber Vision matches device attributes against **built-in vulnerability database** curated by Cisco Security Teams to easily identify vulnerable components

# Segmentation



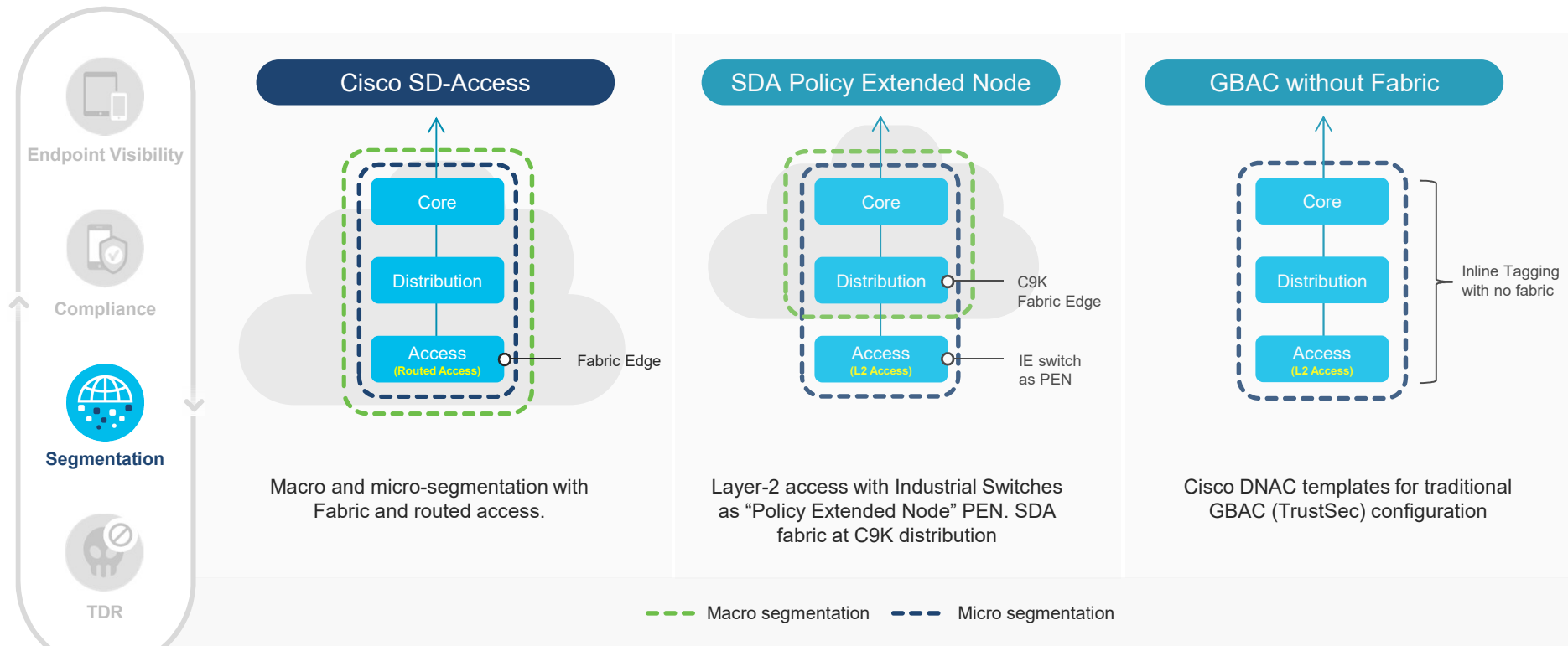
View application relationships to **group endpoints into zones** and **identify conduits** in Cyber Vision

Enable OT users to **dynamically map zones to scalable group tags** of pre-defined TrustSec policies built by IT in ISE

Visualize **traffic activity between scalable groups** in DNAC policy analytics

**Deploy group segmentation policy with confidence** once you are comfortable with the observed network behavior using DNAC Day-n templates

# Segmentation Architectures





# Identify Zones and Conduits

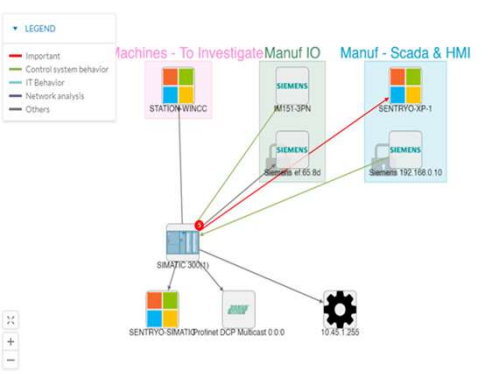
Endpoint Visibility

Compliance

Segmentation

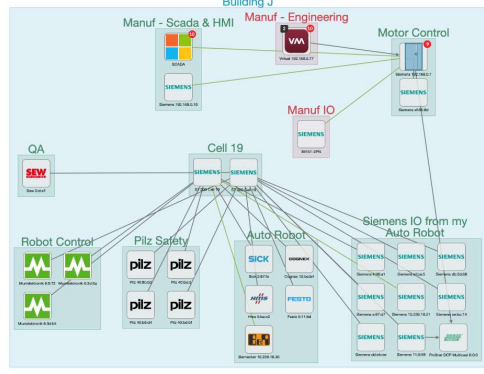
TDR

### Identify Application Relationships

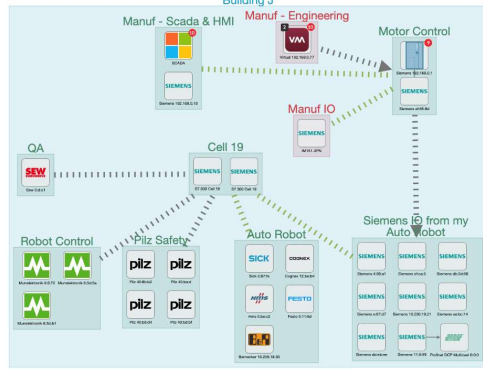


machines - To Investigate Manuf IO Manuf - Scada & HMI

### Group endpoints into Zones



### Visualize Conduits between Zones



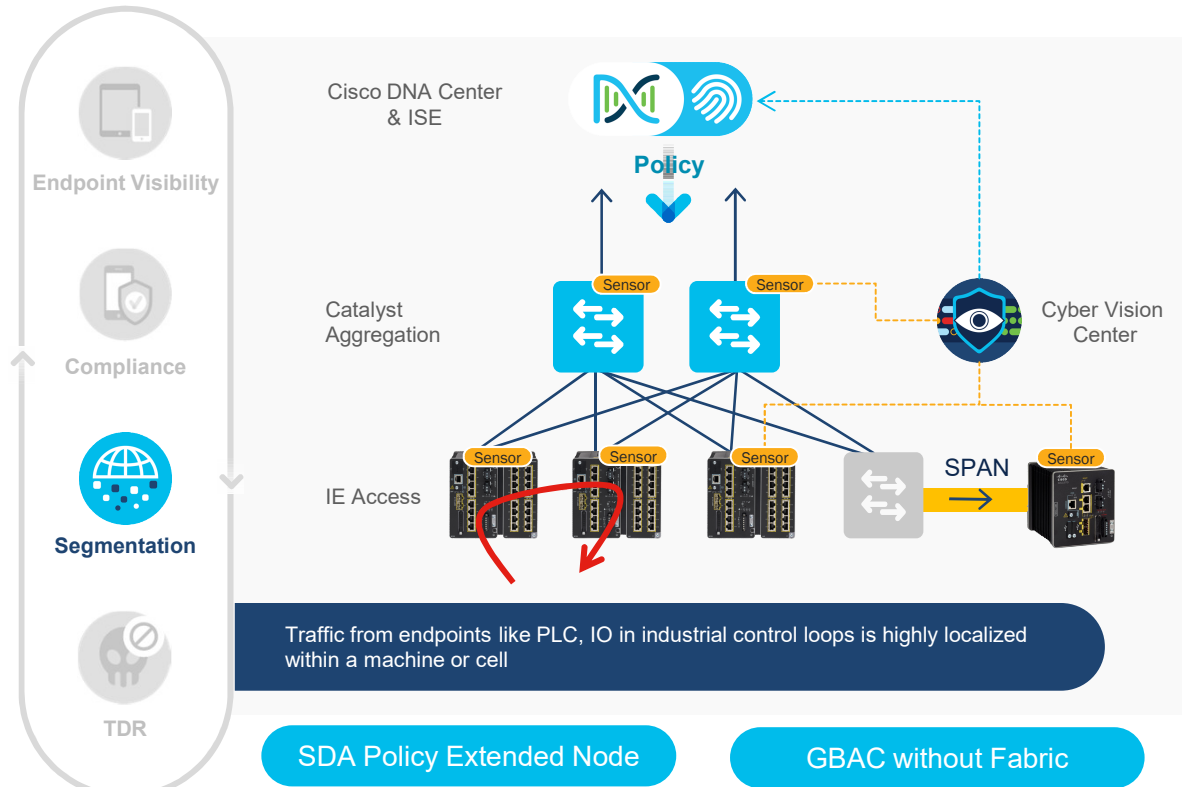
Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

Users can leverage these application relations to group endpoints to match the industrial processes they represent

The traffic flows can be aggregated into conduits which can be used to inform segmentation policies

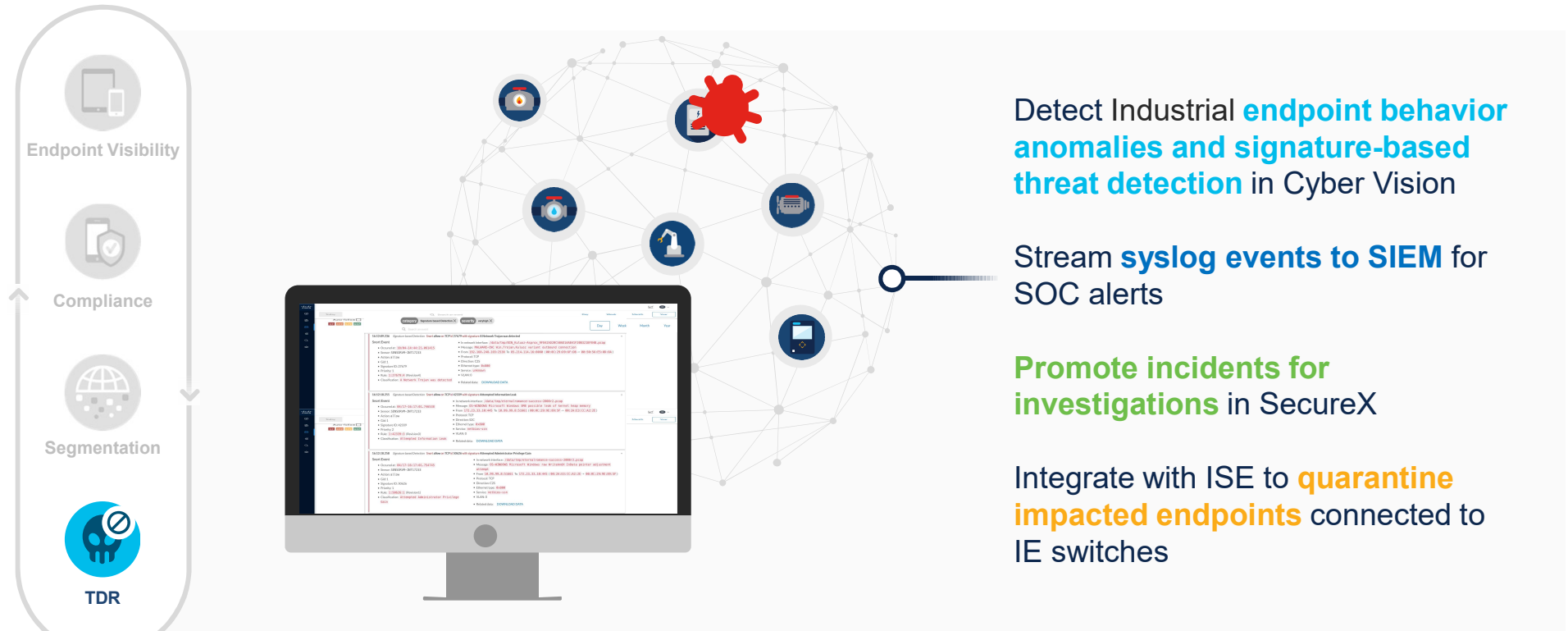
# Bringing it all Together

## Segmenting with Visibility & Policy Analytics



1. Discover endpoints and visualize application relationships in **Cyber Vision** to help inform creation of TrustSec group-based segmentation policies in **DNAC Access Control Application**
2. Endpoint grouping in Cyber Vision triggers pxGrid updates and results in dynamic assignment of SGTs in ISE
3. Visualize group-based network behavior using NetFlow traffic in **DNAC Policy Analytics**
4. Deploy segmentation policy with confidence using **DNAC Day-n templates** once you are comfortable with the observed network behavior

# Threat Detection & Response





The bridge to possible