tenable

De-mystifying Active Query in OT networks

Dominic Storey
Principal OT architect,
EMEA

INDUSTRIAL CYBERSEC FORUM

First law of security

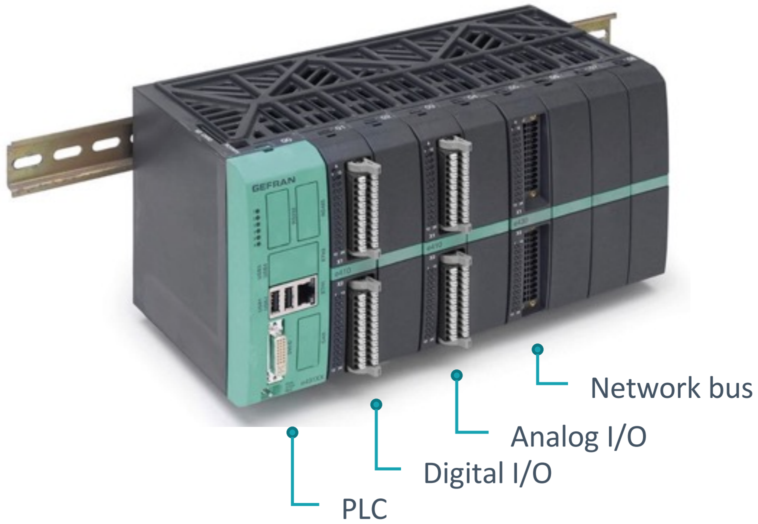
Thou cannot protect what thou dost not know

OT Dogma

Dogma yes, but rooted in truth.
The controller problem

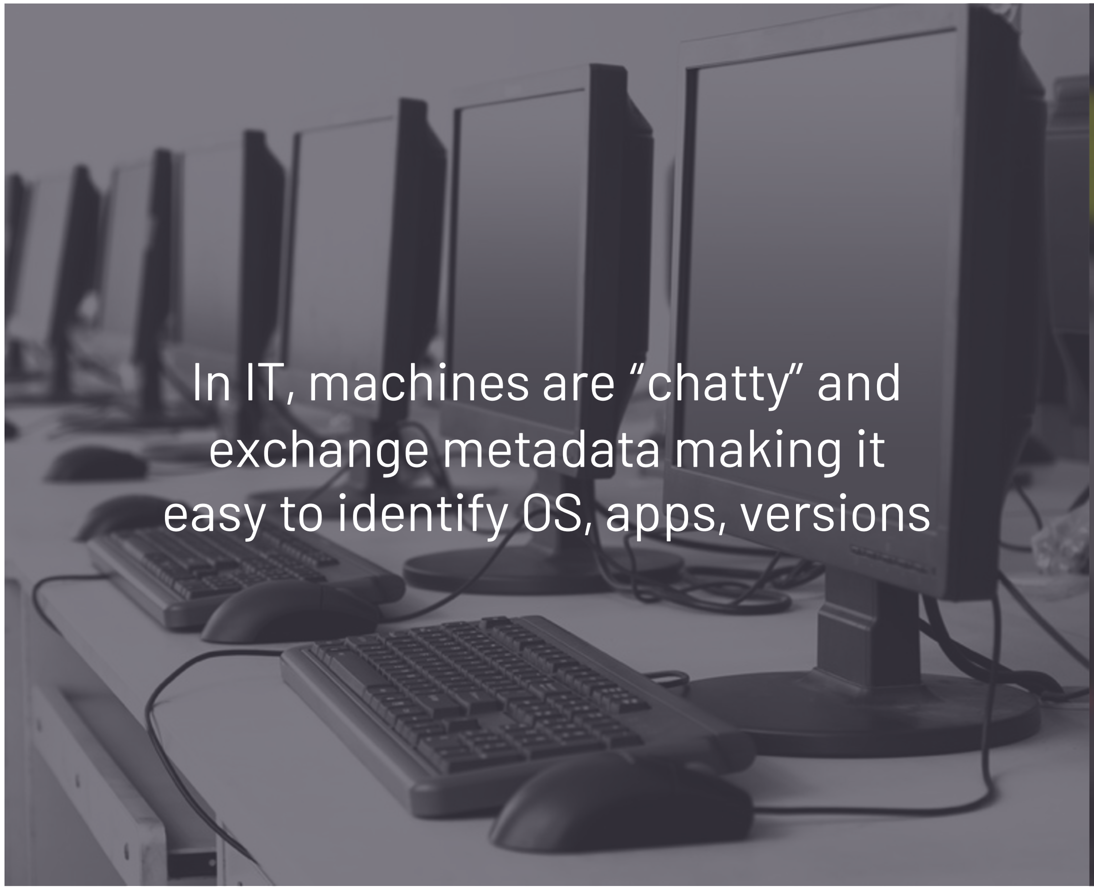
- Long field life
- Can be sensitive to scans
- Controls critical systems
- Consequences on failure

$ ♡ 🐟

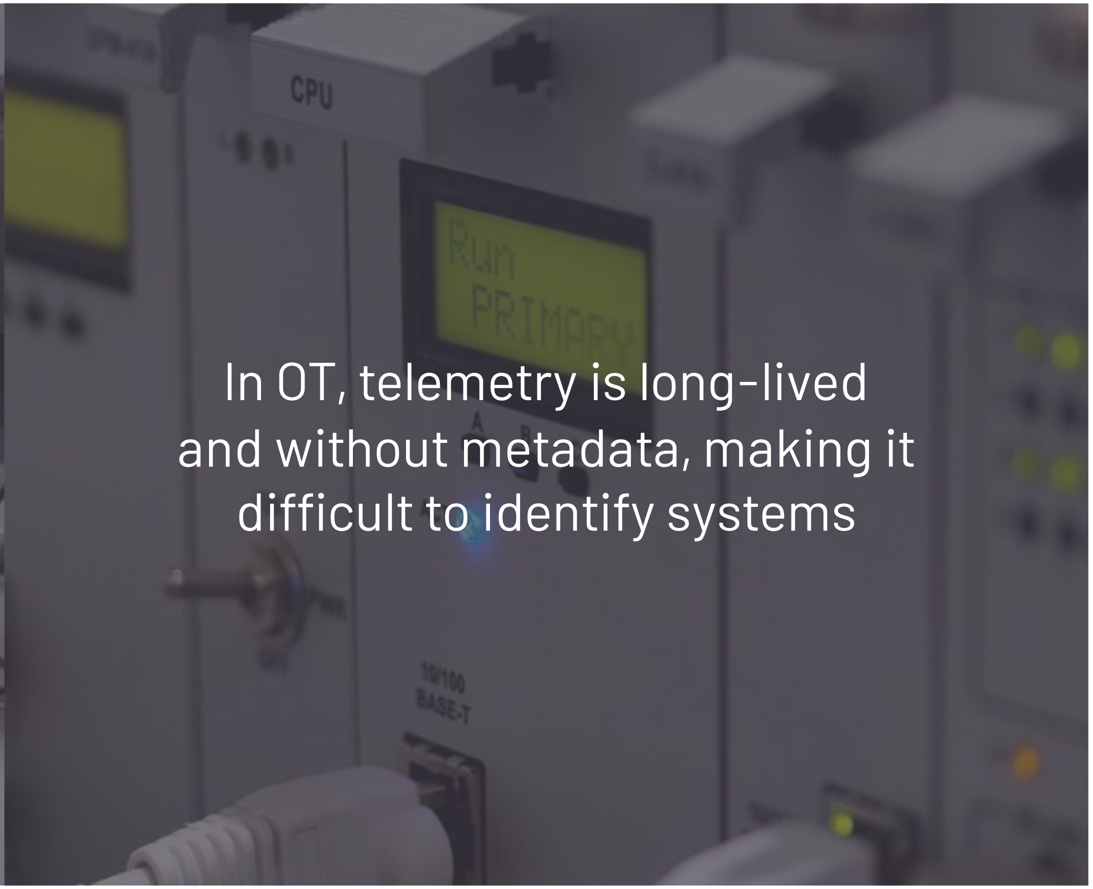


So just listen

There's a problem with that

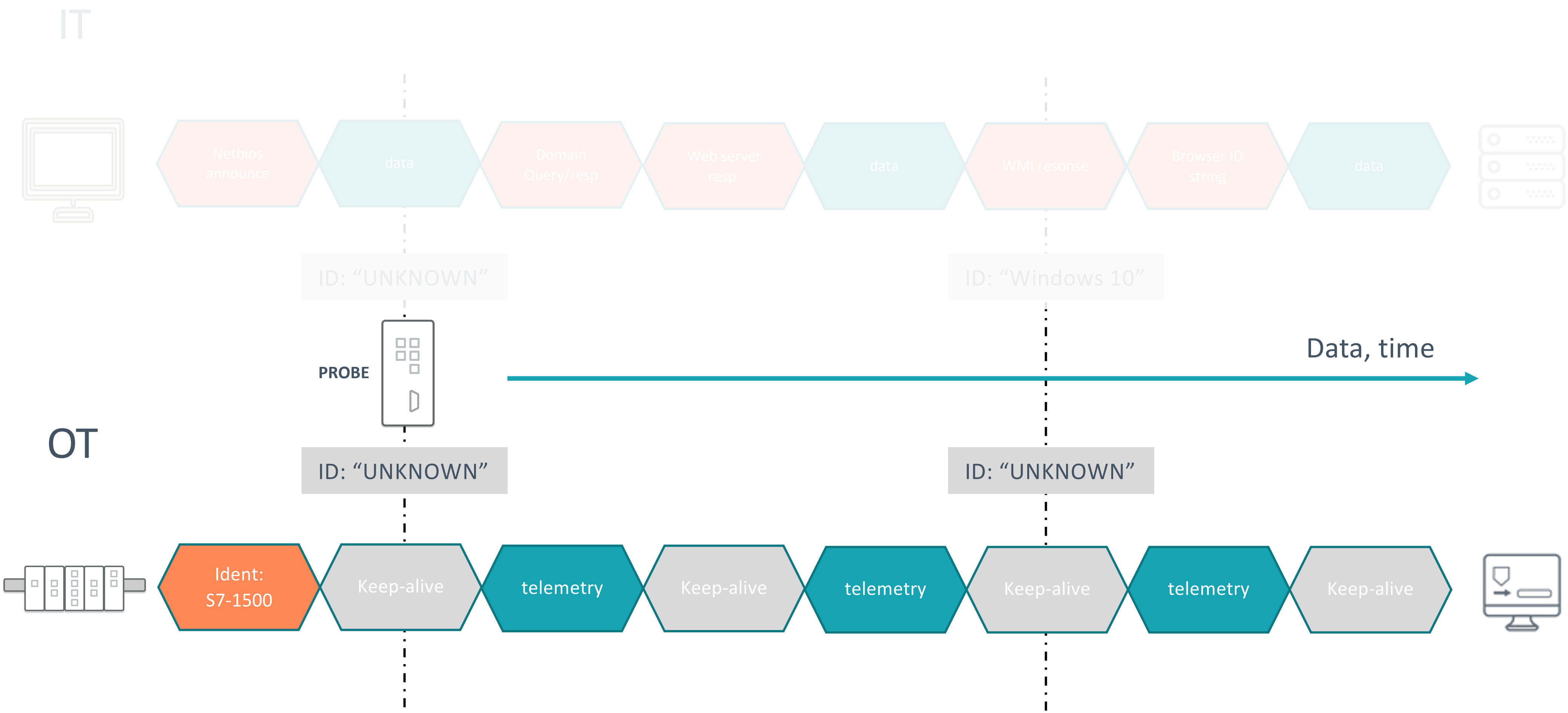


In IT, machines are "chatty" and exchange metadata making it easy to identify OS, apps, versions

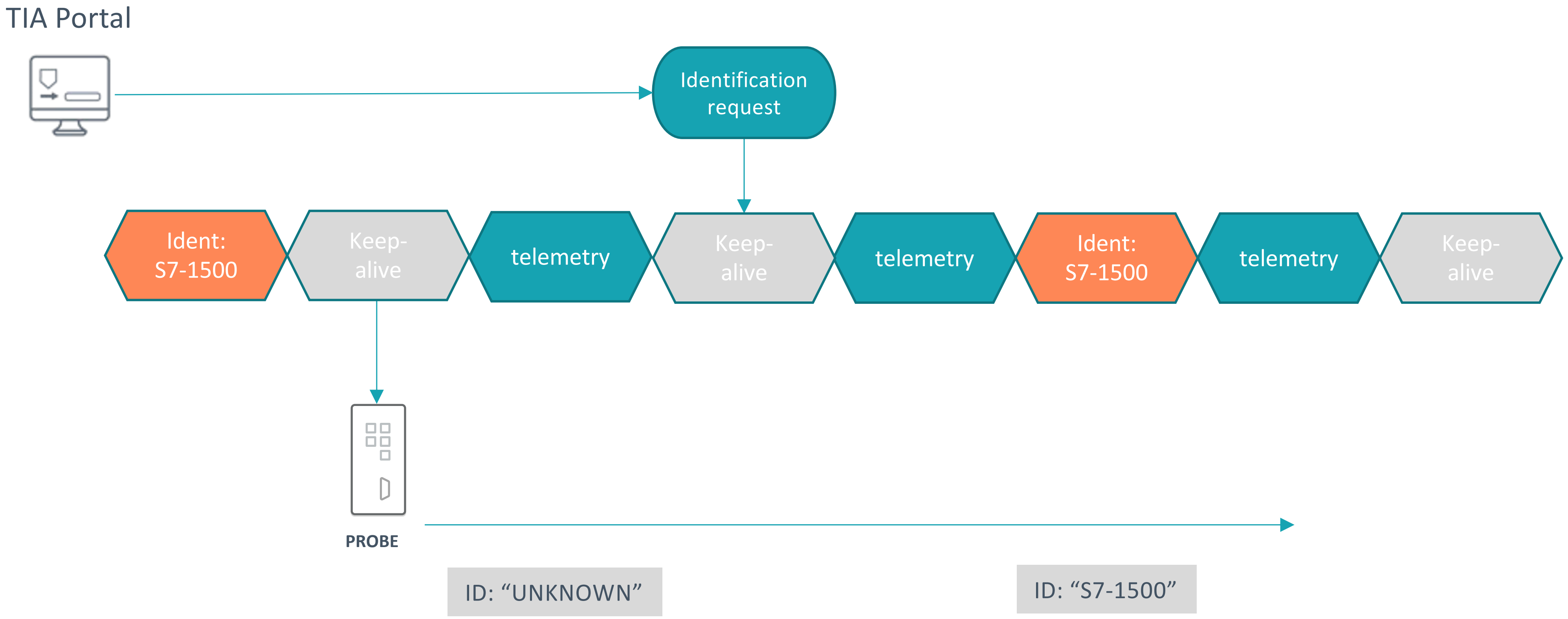


In OT, telemetry is long-lived and without metadata, making it difficult to identify systems

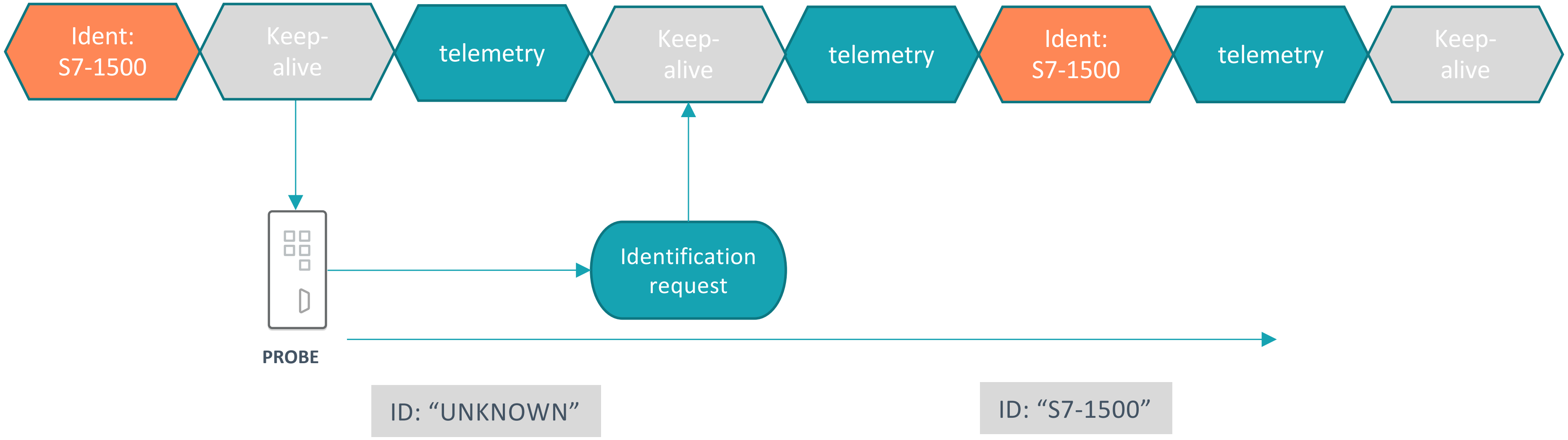
The problem is in the traffic



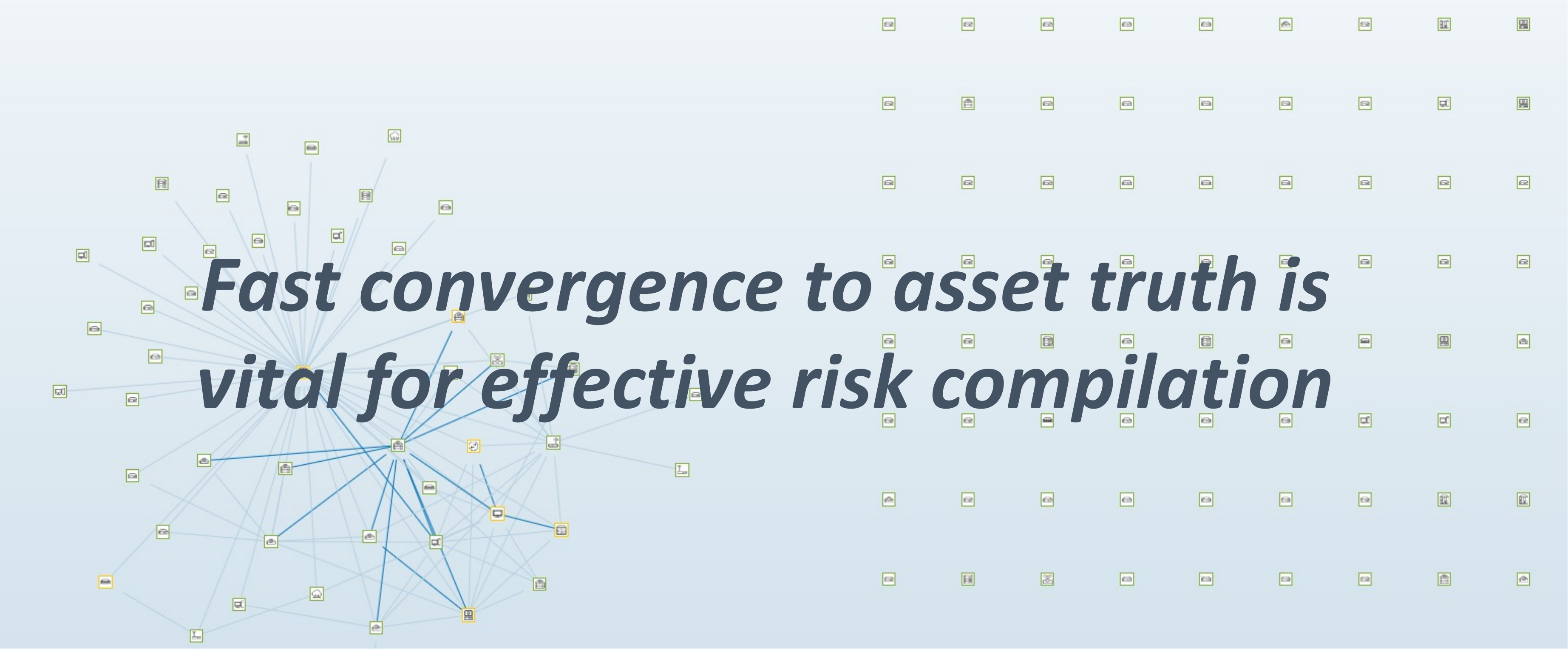
Controller vendors use active query



So why not use this method ourselves?



Many OT devices don't talk until spoken to



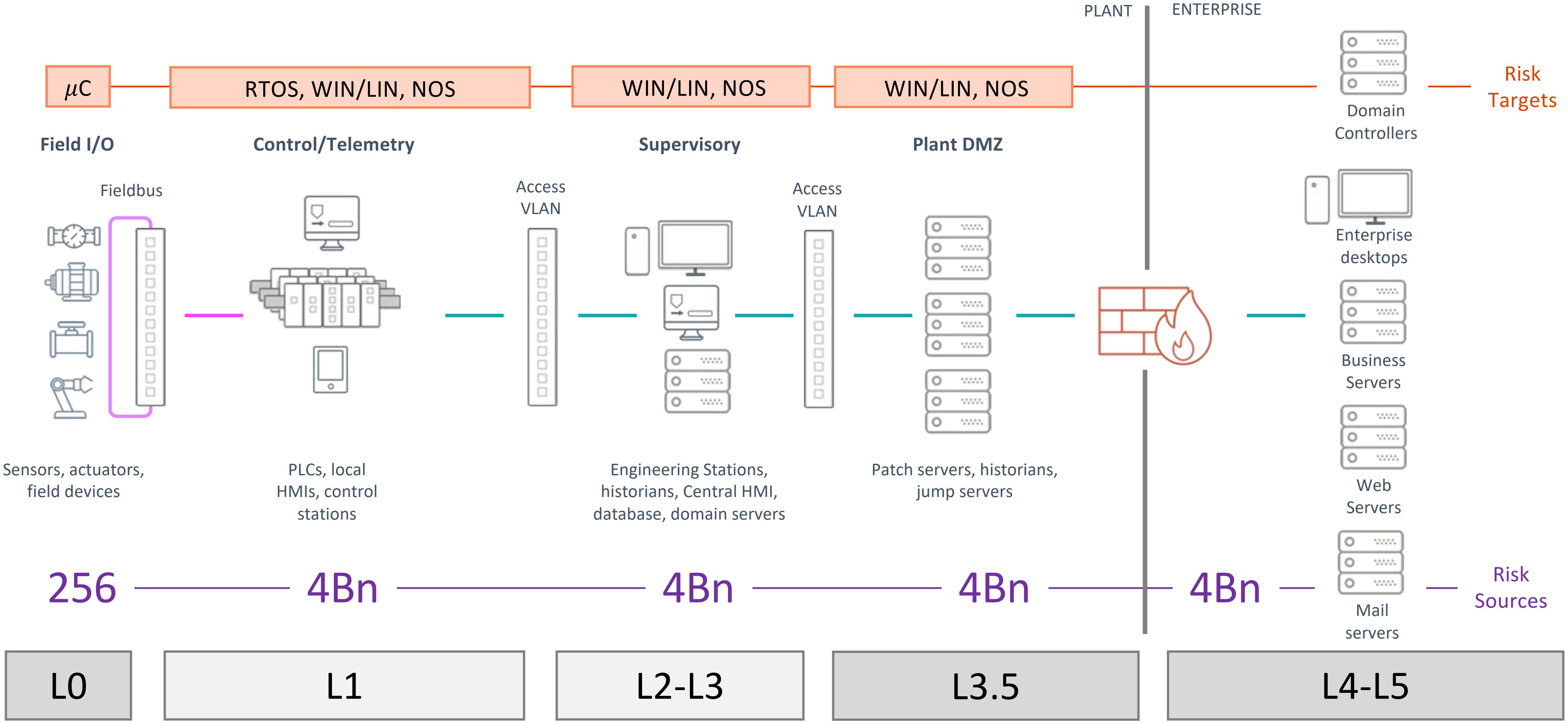
Fast convergence to asset truth is vital for effective risk compilation

Visible to passive monitors

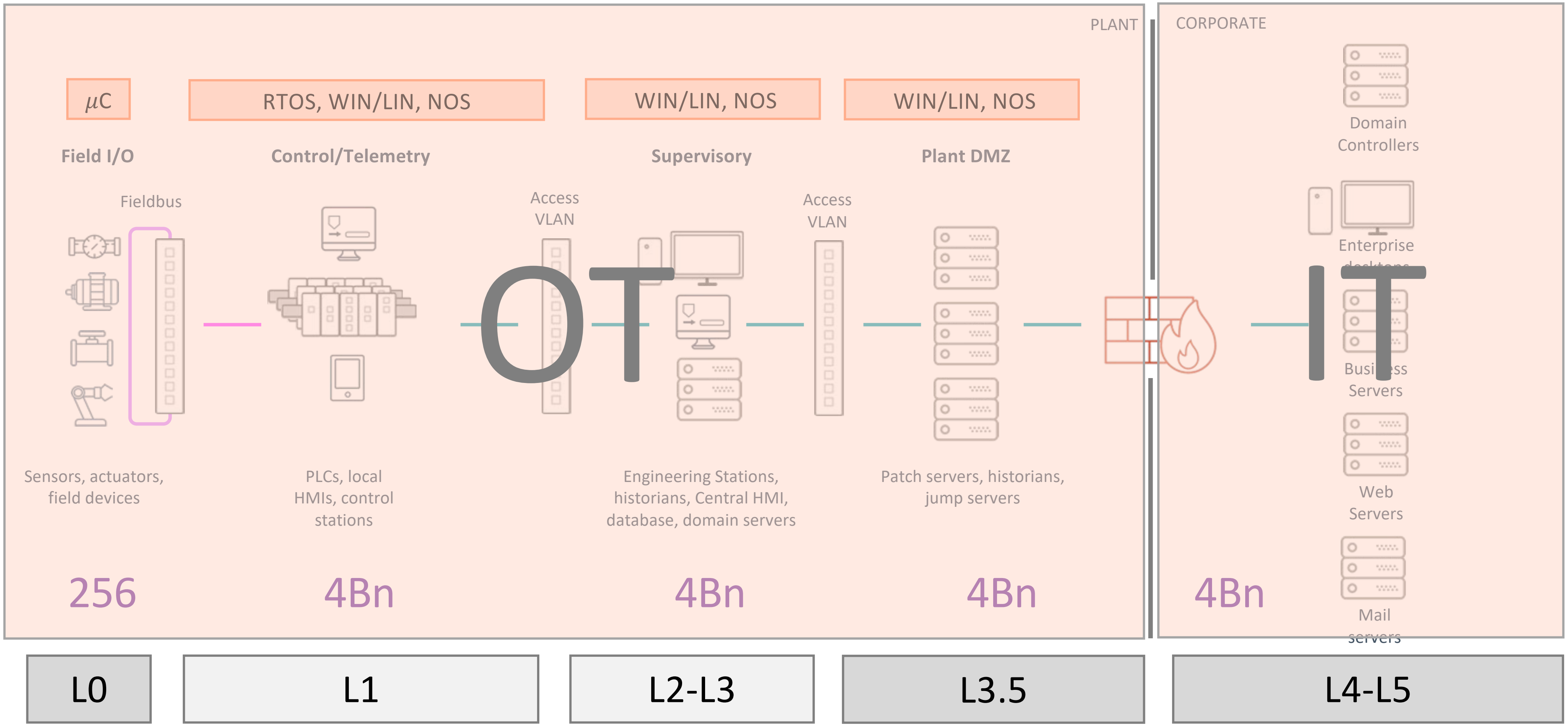
Invisible to passive monitors

Let’s think more deeply about this issue

Some thoughts about risk



Perceived IT/OT demarcation



PLANT

CORPORATE

μC

RTOS, WIN/LIN, NOS

WIN/LIN, NOS

WIN/LIN, NOS

Field I/O

Control/Telemetry

Supervisory

Plant DMZ

Fieldbus

Access VLAN

Access VLAN

Domain Controllers

Enterprise desktops

Business Servers

Web Servers

Mail servers

OT

IT

Sensors, actuators, field devices

PLCs, local HMIs, control stations

Engineering Stations, historians, Central HMI, database, domain servers

Patch servers, historians, jump servers

256

4Bn

4Bn

4Bn

4Bn

L0

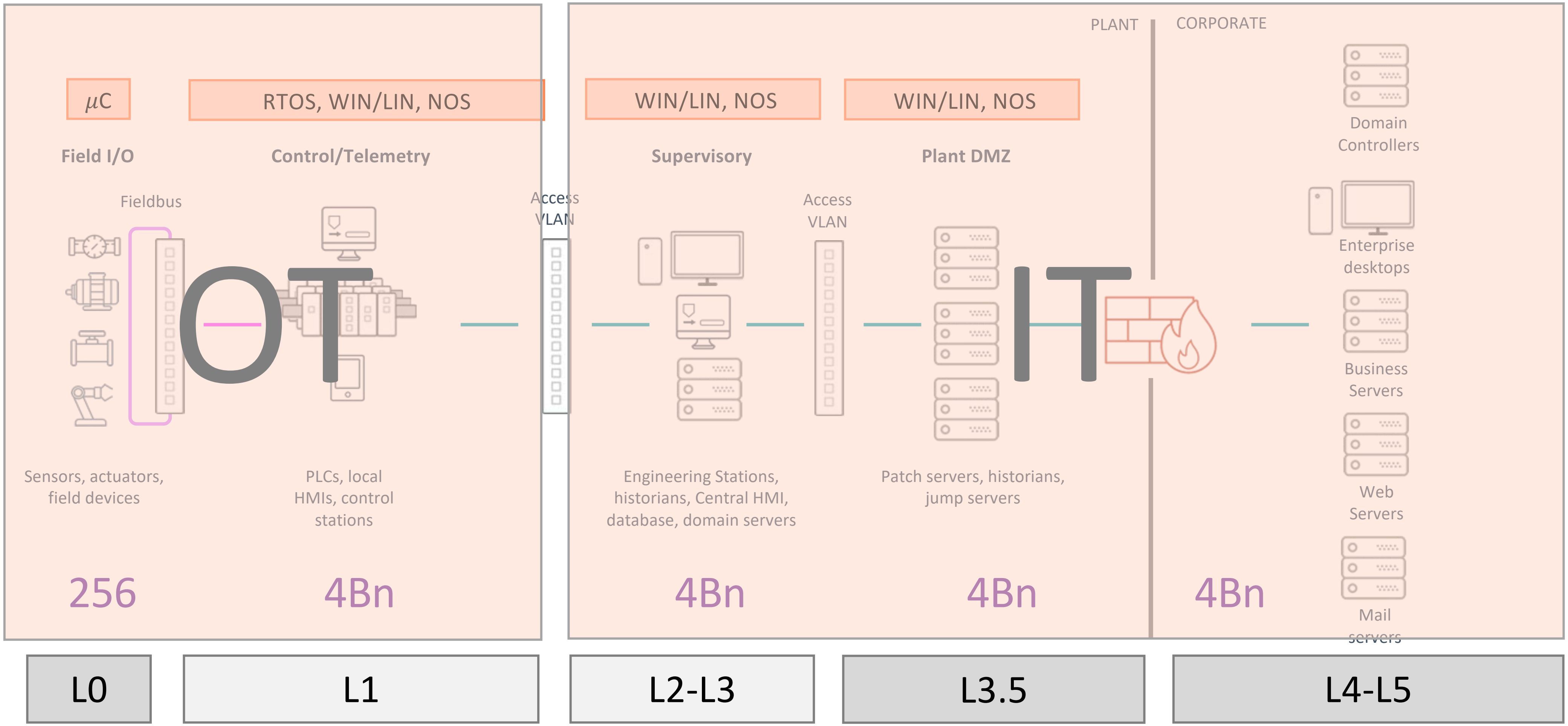
L1

L2-L3

L3.5

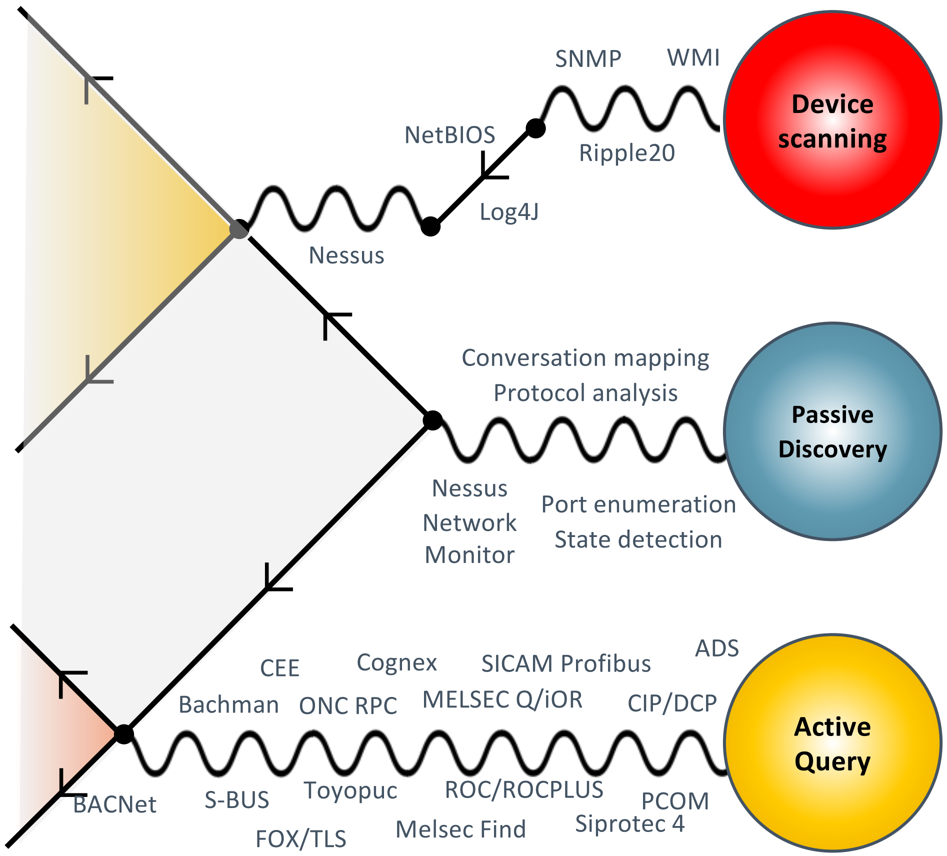
L4-L5

The reality.
(we can use this)

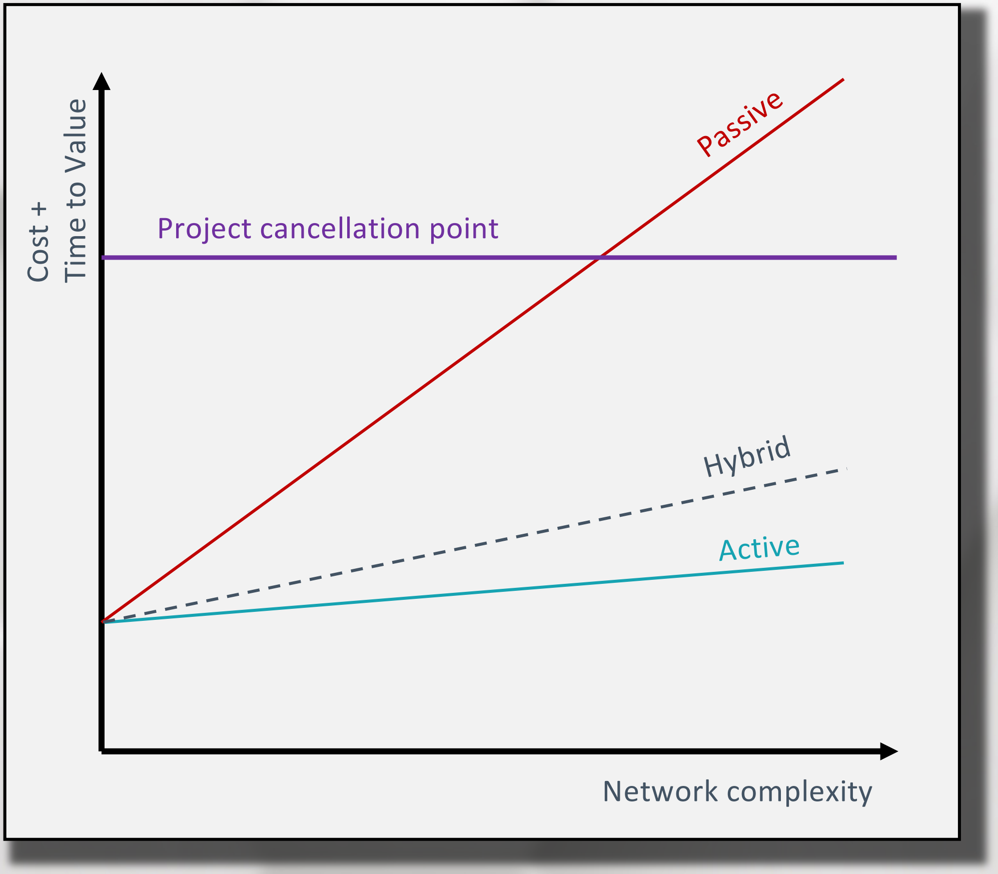


Hybrid Discovery

PURDUE	OPERATING SYS.
LEVEL 5 ENTERPRISE	WIN / LIN VM / SERVER
LEVEL 4 E.R.P.	WIN / LIN VM / SERVER
LEVEL 3 SITE OPERATIONS	WIN CLIENT ENGINEER STN
LEVEL 2 SUPERVISORY	EMBED. WIN/LIN HMI
LEVEL 1 CONTROL	RTOS / LINUX CONTROLLER/RTU
LEVEL 0 PHYSICAL PROCESS	EMBEDDED / NONE FIELD DEVICE



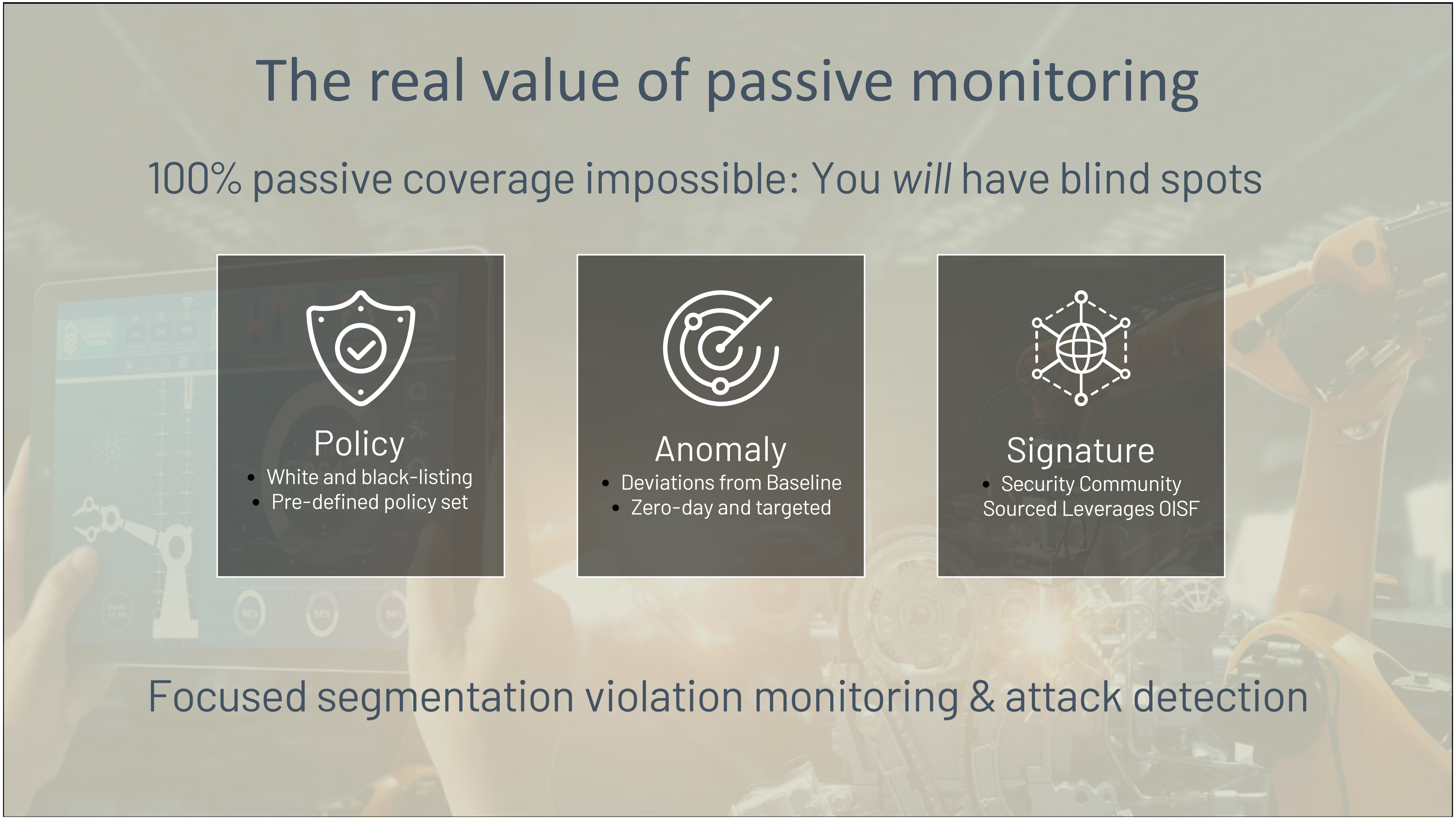
Asset convergence time (T_A) and time to value (T_V)



- **Passive Detection** costs are linked to mirroring costs, which scales unfavorably with segmentation complexity
- **Active query** costs are favorable (layer-3 technology, principally dependent on firewall requirements)
- **Hybrid** configurations can be configured to set the line anywhere between fully passive or fully active.
- **Cancellation** occurs when cost or time-to-value limits are exceeded

The real value of passive monitoring

100% passive coverage impossible: You *will* have blind spots



Policy

- White and black-listing
- Pre-defined policy set

Anomaly

- Deviations from Baseline
- Zero-day and targeted

Signature

- Security Community Sourced Leverages OISF

Focused segmentation violation monitoring & attack detection

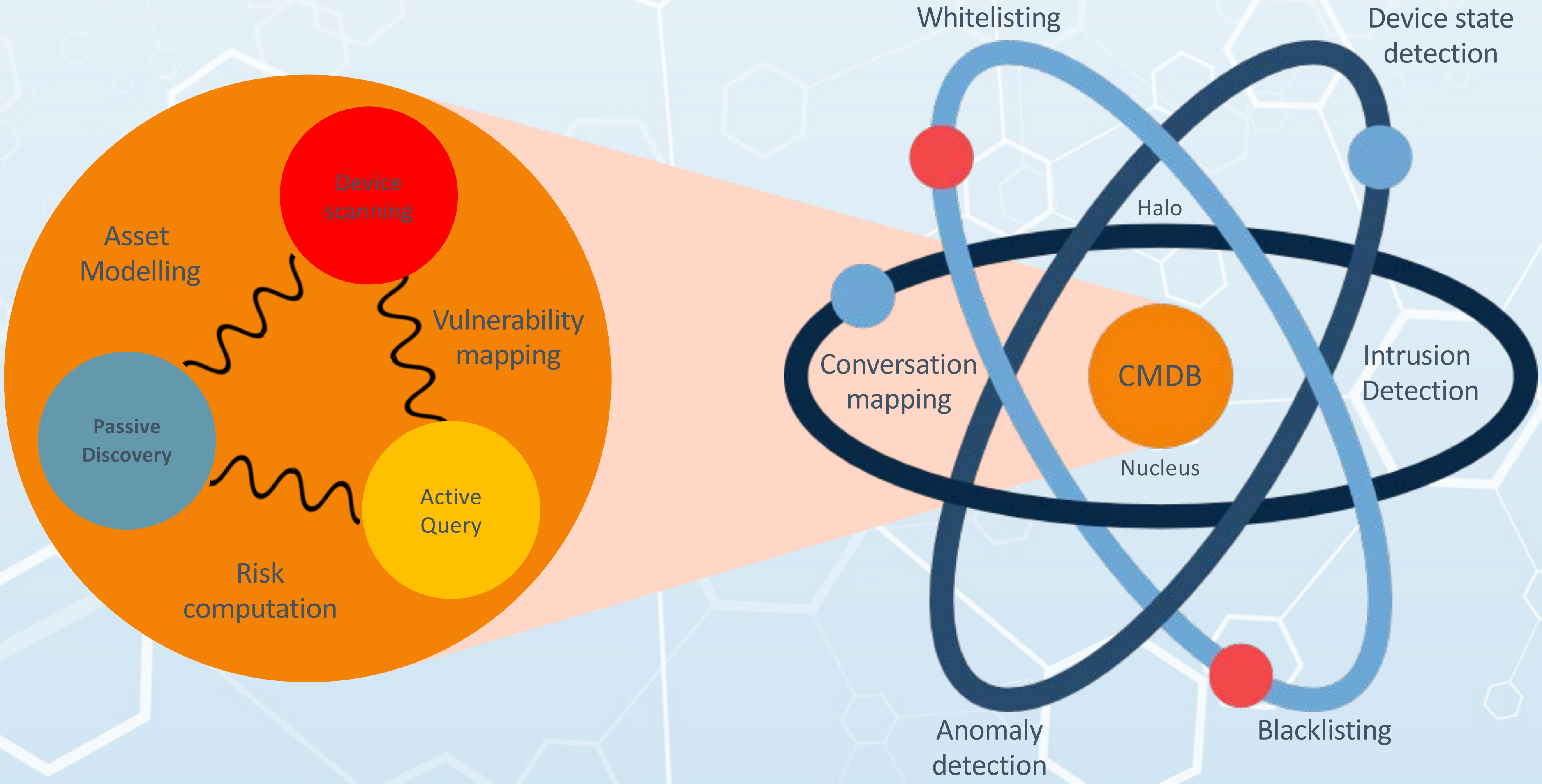
Stage your deployment for guaranteeing success

- **Stage I - Immediate success:** Active query to acquire asset map for proactive maintenance
  - Establish inventory and initial vulnerability map by running discovery and initial asset enrichment
  - Faster deployment even when you spend extra time validating active query methods
- **Stage II – Continuing success:** Build out Passive detection to track real-time events.
  - Turn on IDS, anomaly and configuration tracking to enhance value to the business

Getting Buy-in

(hint)

Offer a solution with heart and halo



Active discovery delivers better data

Identify

Assets communicating on the network

Discover

Devices which are not active or communicating

Classify

HMI, Historian, Router, PLC, Server, Switch

Collect

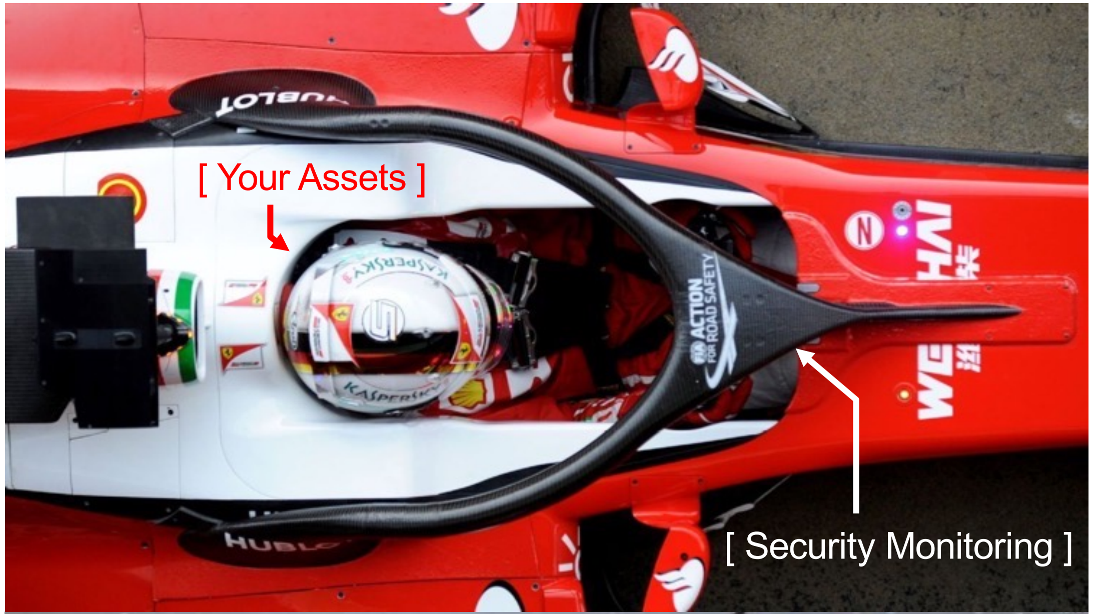
Patch, Hotfix levels, Firmware, Users, PLC Backplane

Track

Full configuration change control including devices

Halo value add

- Protect controllers lacking authentication protocols
- Protect against network-based compromise
- Protect against human error
- Detect and respond to device failure

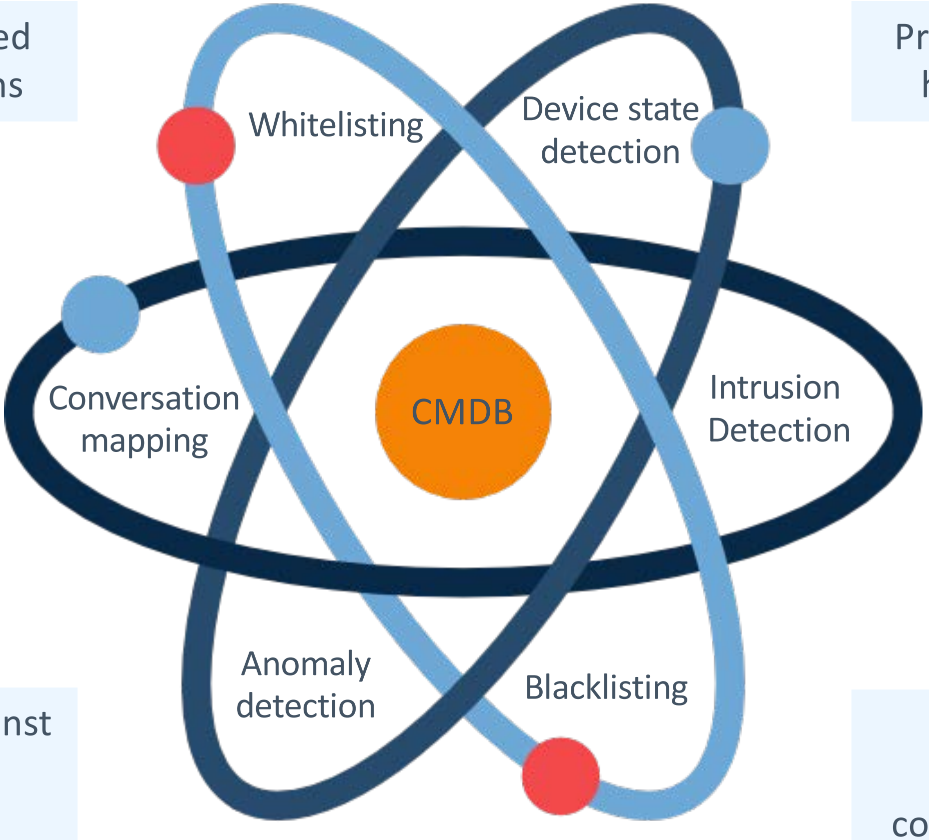


[Your Assets]

[Security Monitoring]

MARK THOMPSON/GETTY IMAGES EUROPE/GETTY IMAGES

Example: The Tenable.ot Halo



Codifies intended communications

Protects against human error

Aids reliability analysis and Reveals systemic dependencies

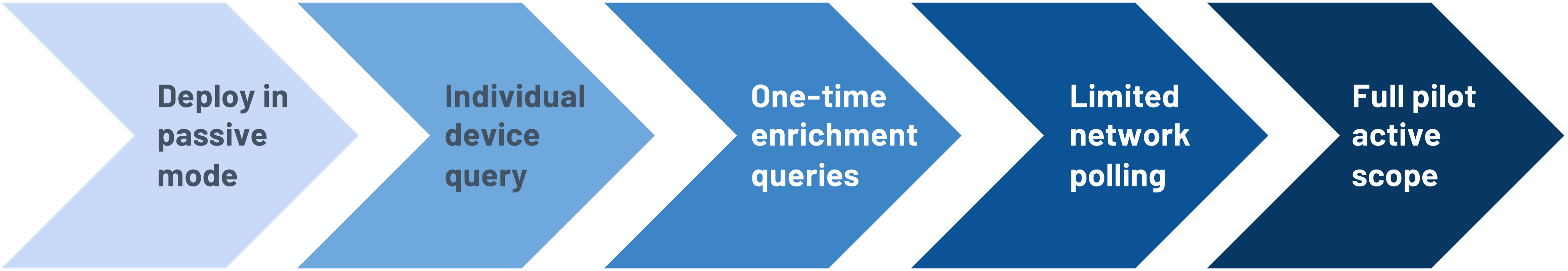
Protects against known threats

Protects against unknown threats

Alerts on unintended communications

VALIDATING ACTIVE QUERY

Small scale pilot



Deploy in passive mode

Individual device query

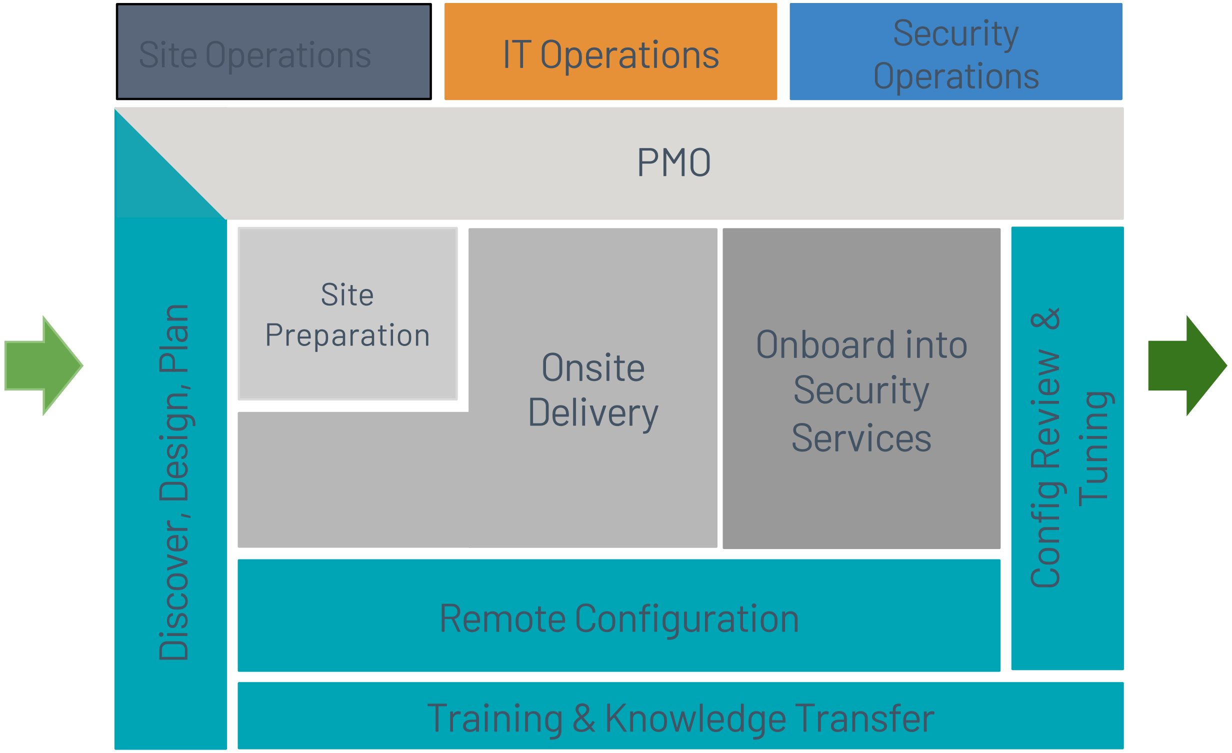
One-time enrichment queries

Limited network polling

Full pilot active scope

FACT: Our customers make 100,000+ active queries *every day.*

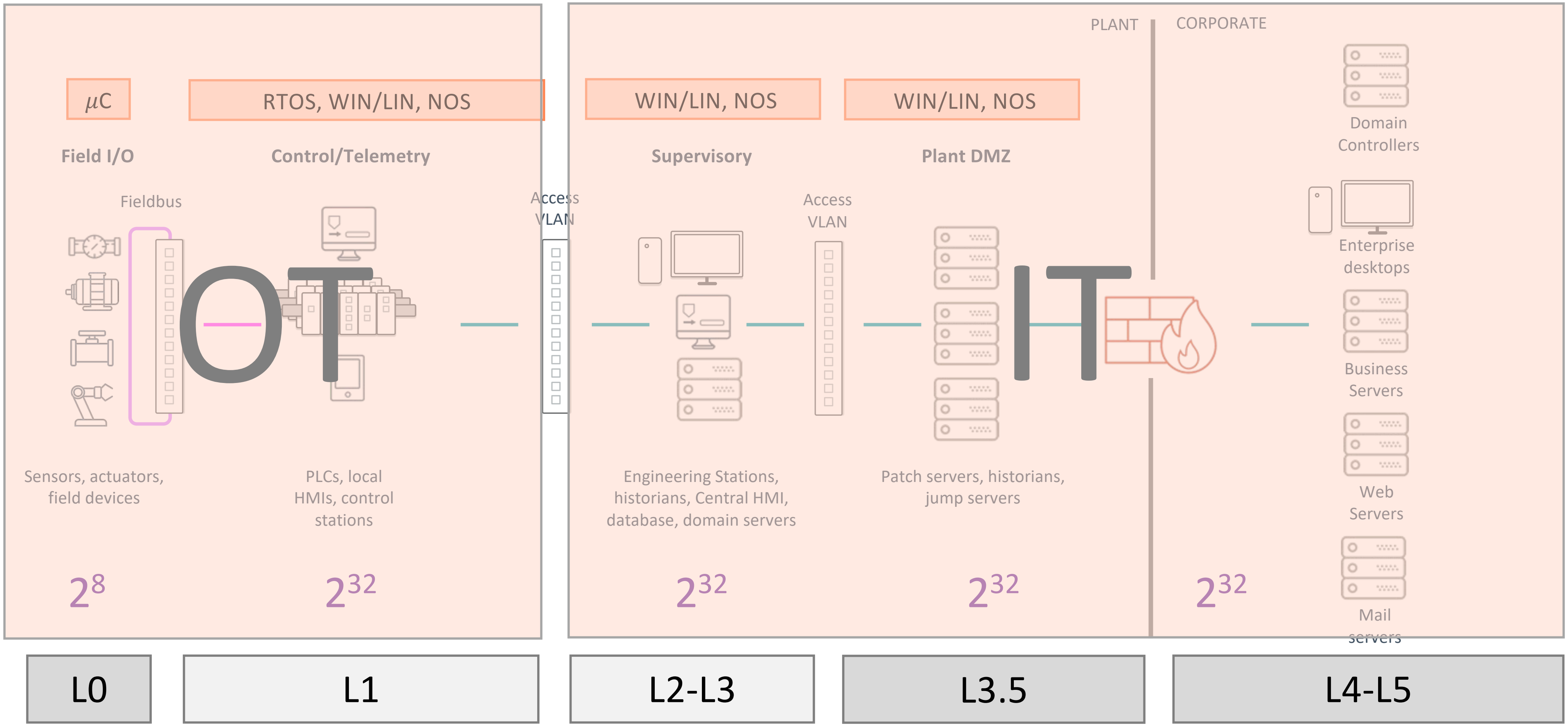
Scaling to implementation



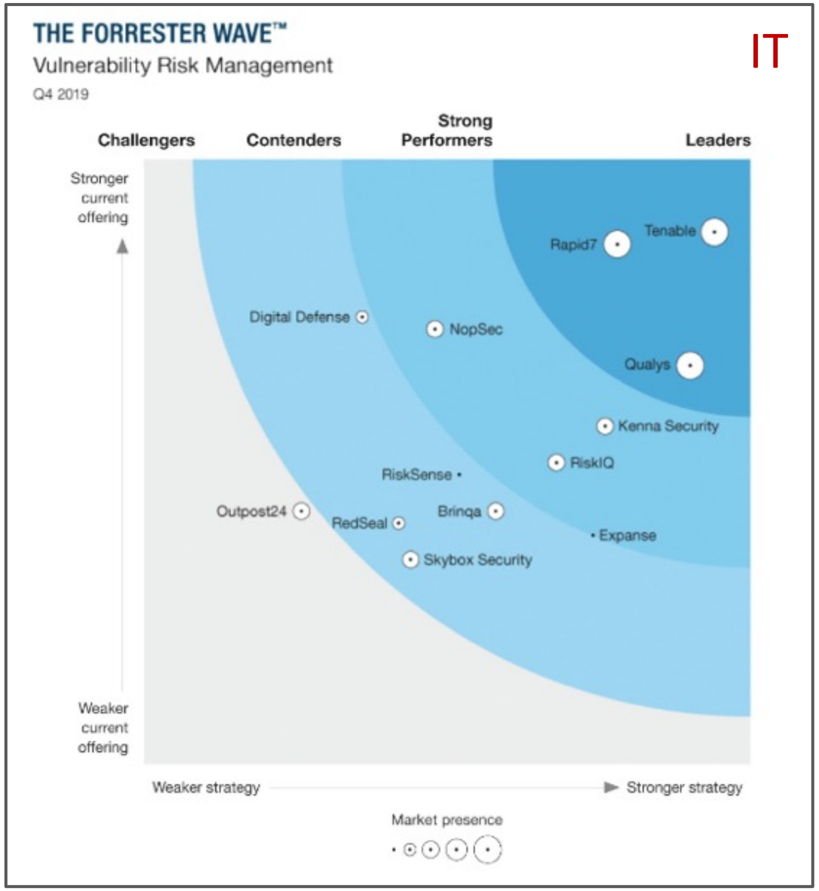
MSSP/SOC SVCs

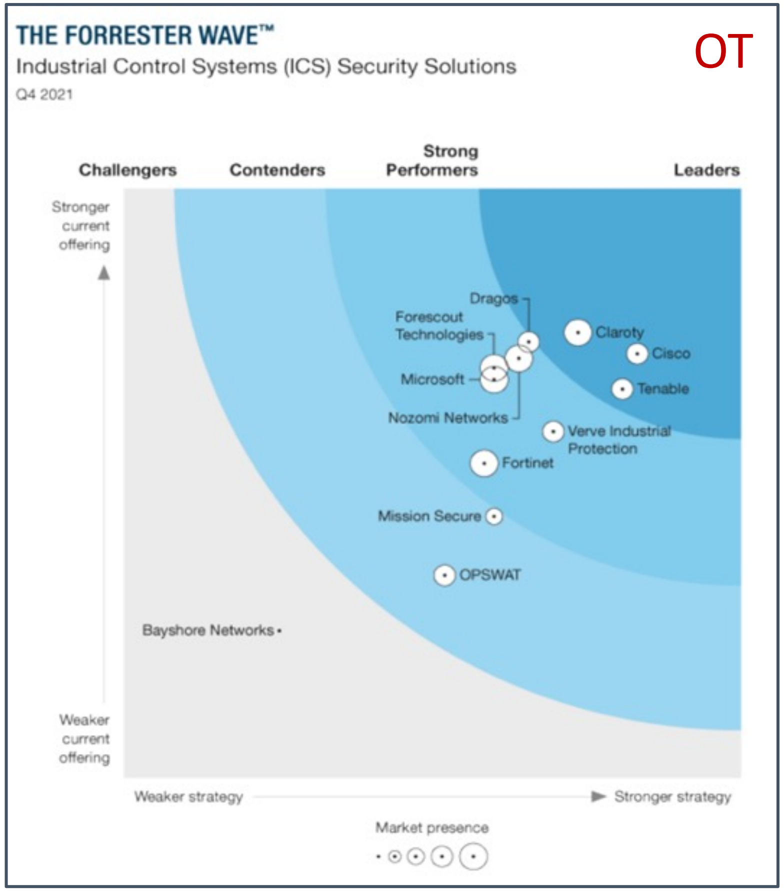
Last thoughts

If your world looks like this



Choose a solutions vendor who is leader in both IT & OT





Questions?

dstorey@tenable.com