CISCO Partner
Gold Certified

Visibility equals Defense vol.4: An IoT story

Elias Aggelidis, Technical Director ICT

Industry 4.0 Security Topics

- Growth and Challenges
- What's Different With IoT / OT versus IT
- How IT Managers Can Deal With IoT / OT

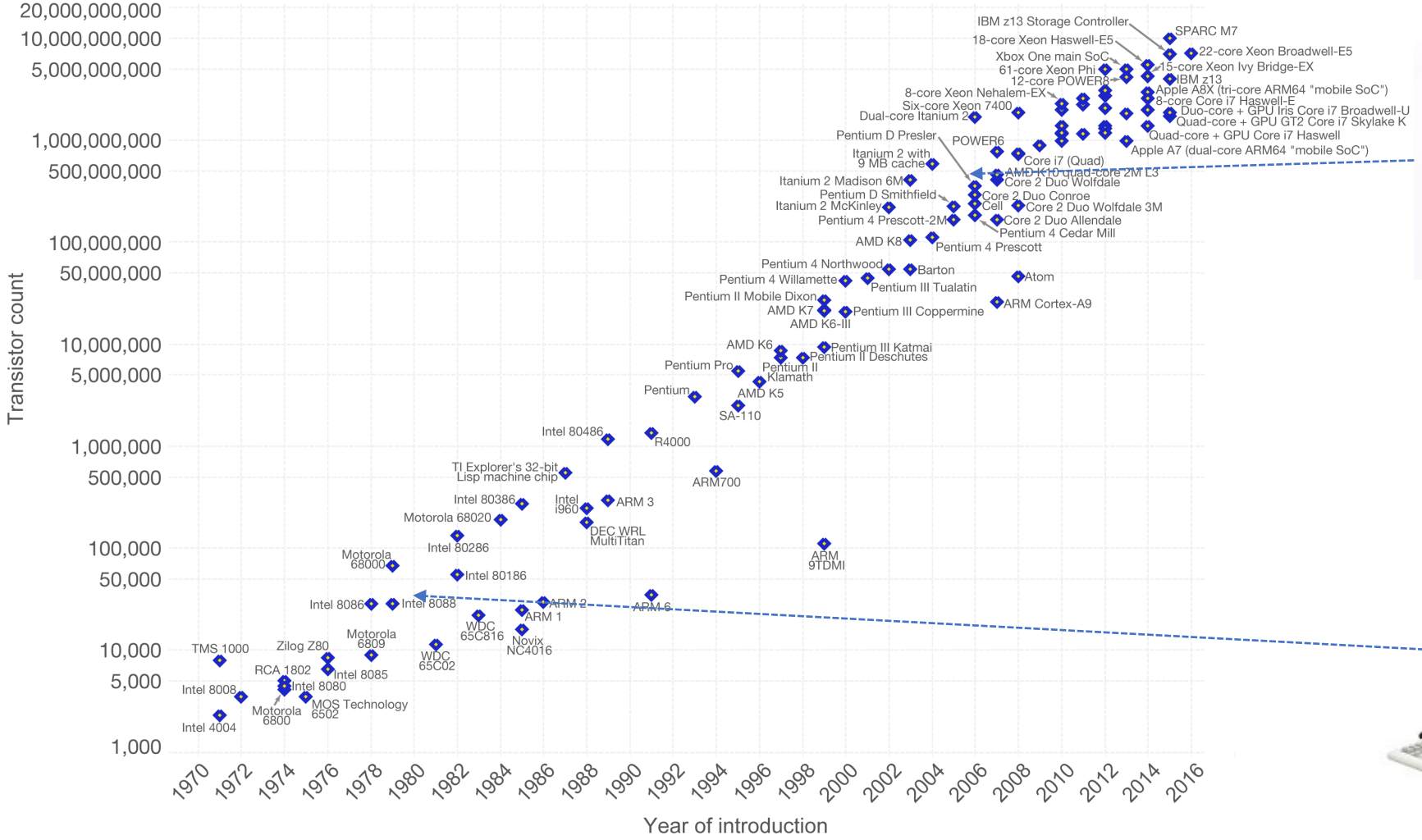
Industry 4.0 Security Topics

- Growth & Challenges

Moore's Law – The number of transistors on integrated circuit chips (1971-2016)

Our World in Data

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are strongly linked to Moore's law.

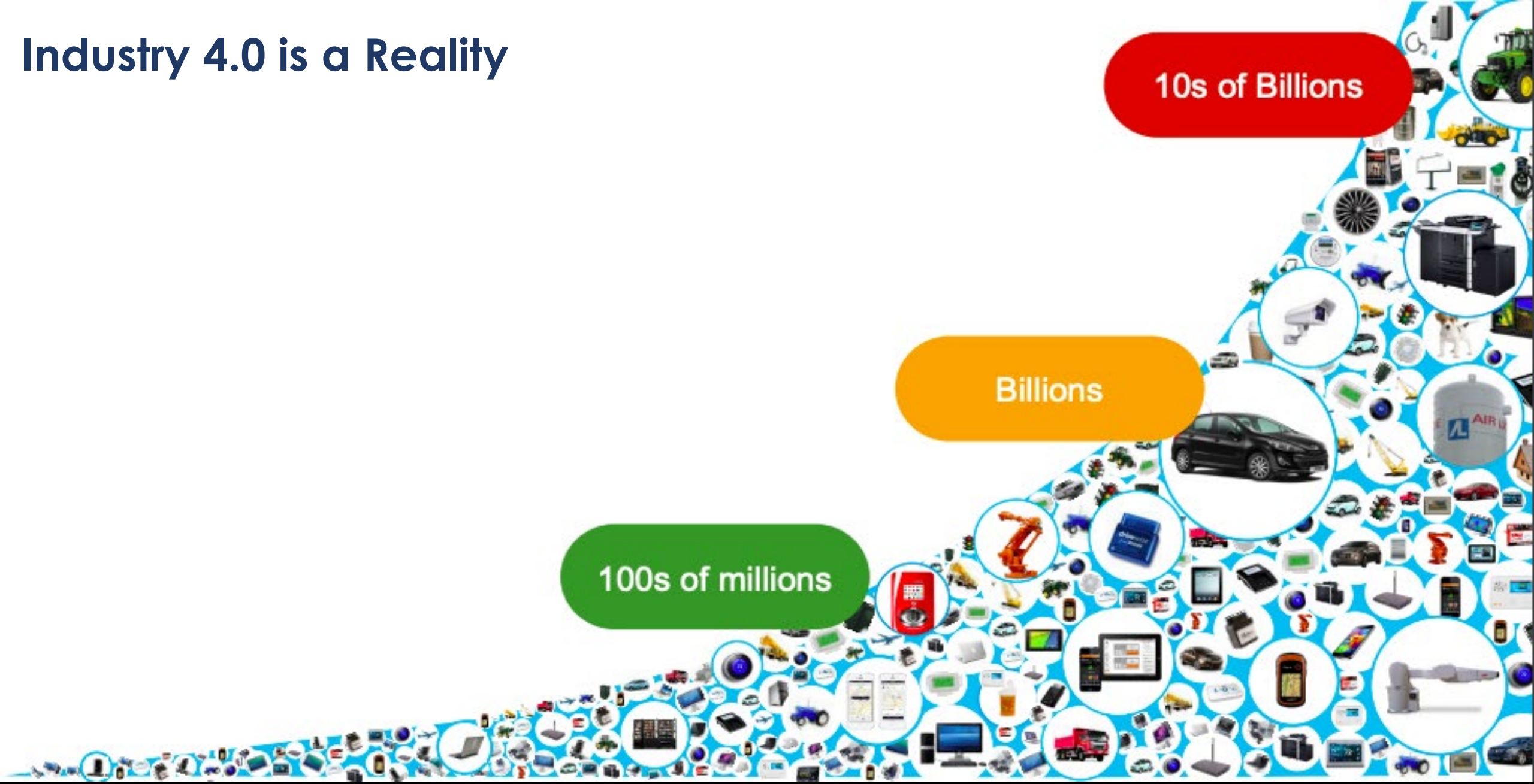


Pi Zero
15,70 euro
270M transistors

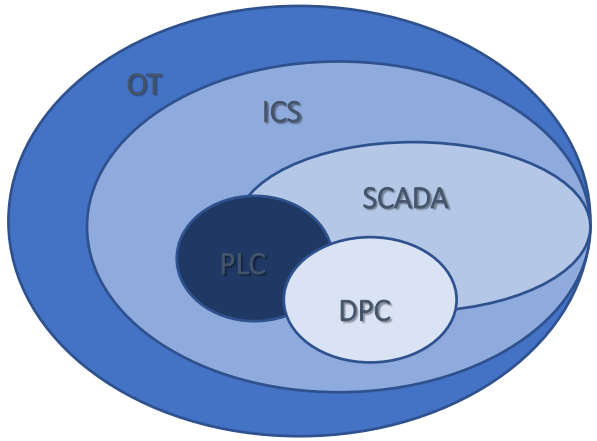
IBM PC 5150
$1565
($4313 today's rate)
29K transistors

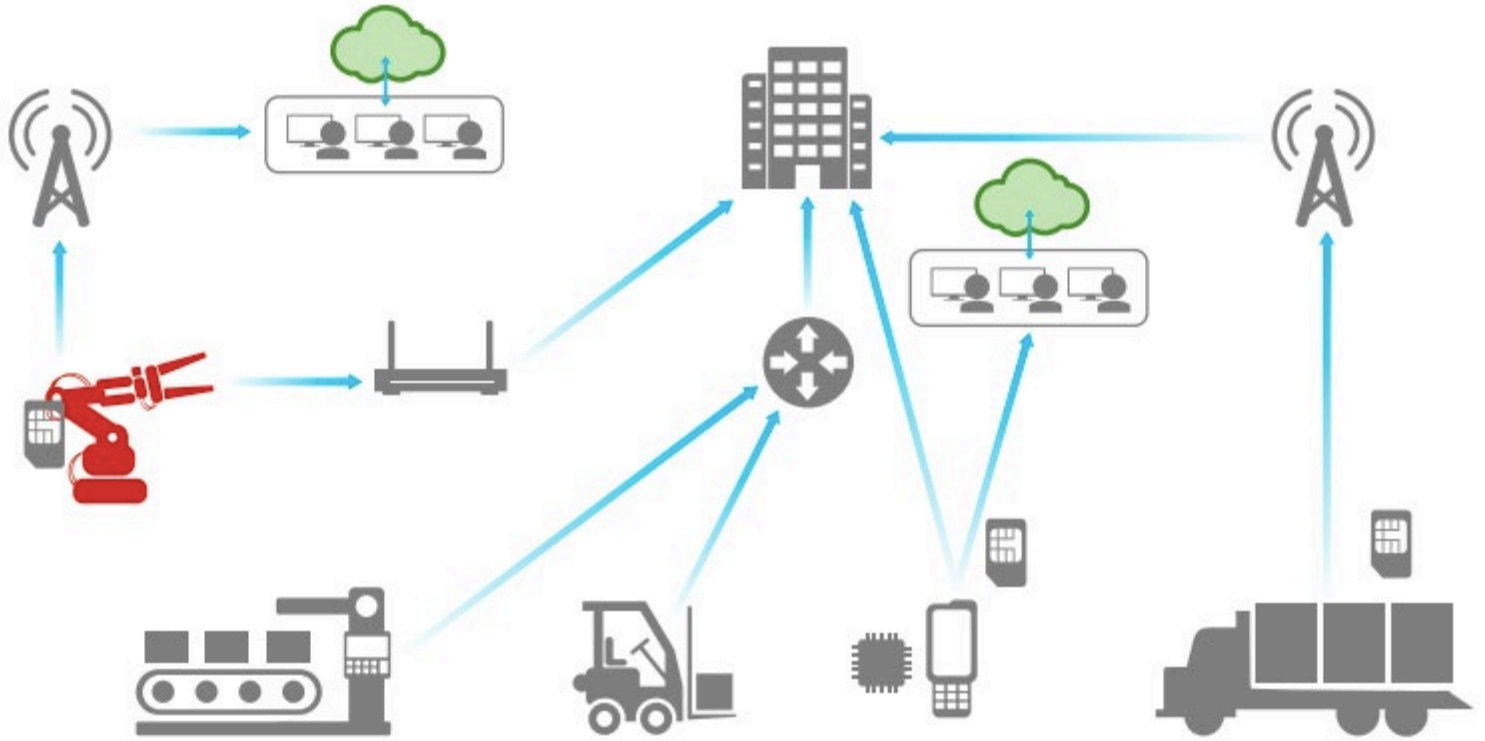
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Industry 4.0 is a Reality



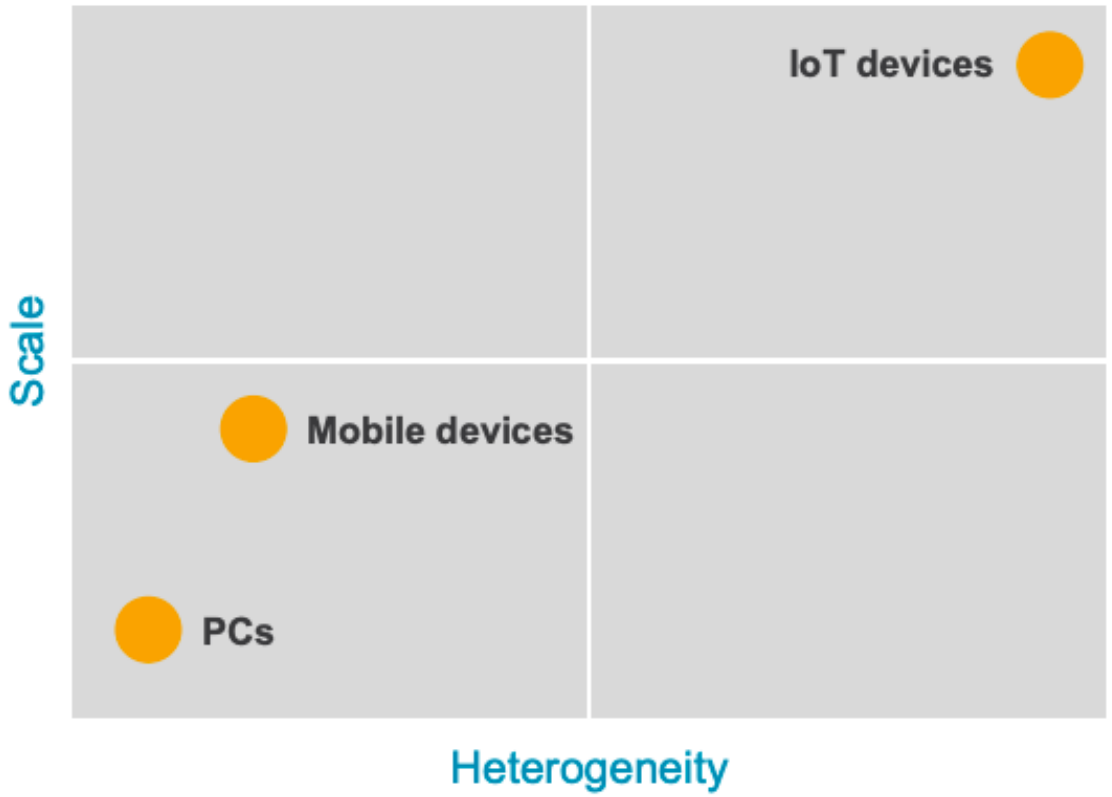
Industry 4.0 in Action Within Manufacturing





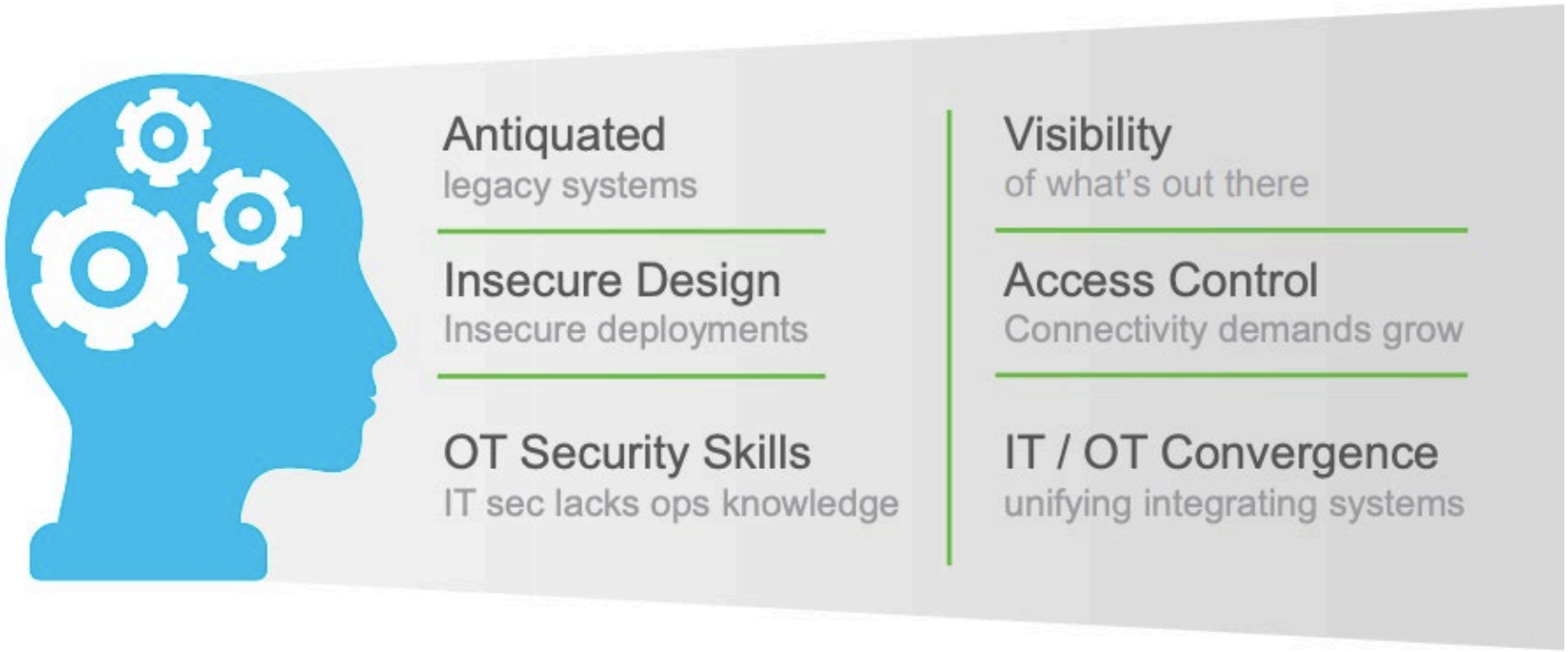
ICS = Industrial Control System
PLC = Programmable Logic Controller
DPC = Discrete Process Control Systems
SCADA = Supervisory Control and Data Acquisition

Industry 4.0 Devices Introduce New Challenges



- Devices not all greenfield
- Highly heterogeneous and massive scale
- Traditional IT approaches don't work

Industry 4.0 Devices Introduce New Challenges



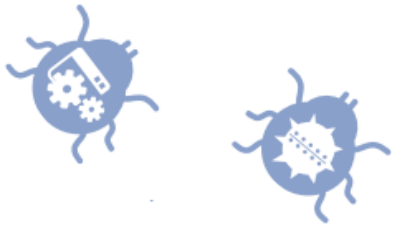
Industry 4.0 Devices Introduce New Challenges

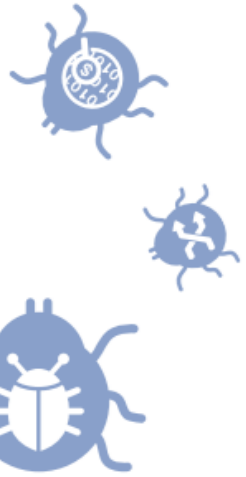
Automation vendors still ship updates on **EOL Windows platforms**

Vulnerabilities found in industrial systems
rose **2400%** from 2009 to 2015

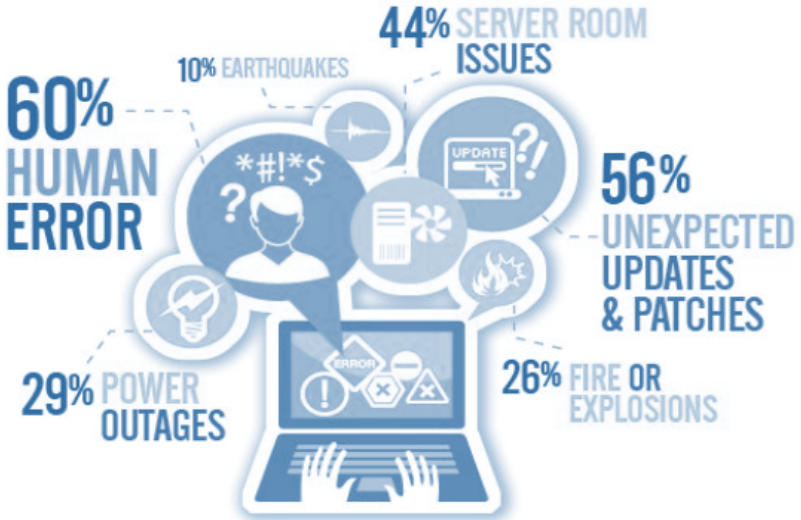
The most common ethernet based OT protocol
lacked authentication till Fall of 2015

Yet ethernet in manufacturing grew
96% the three years before



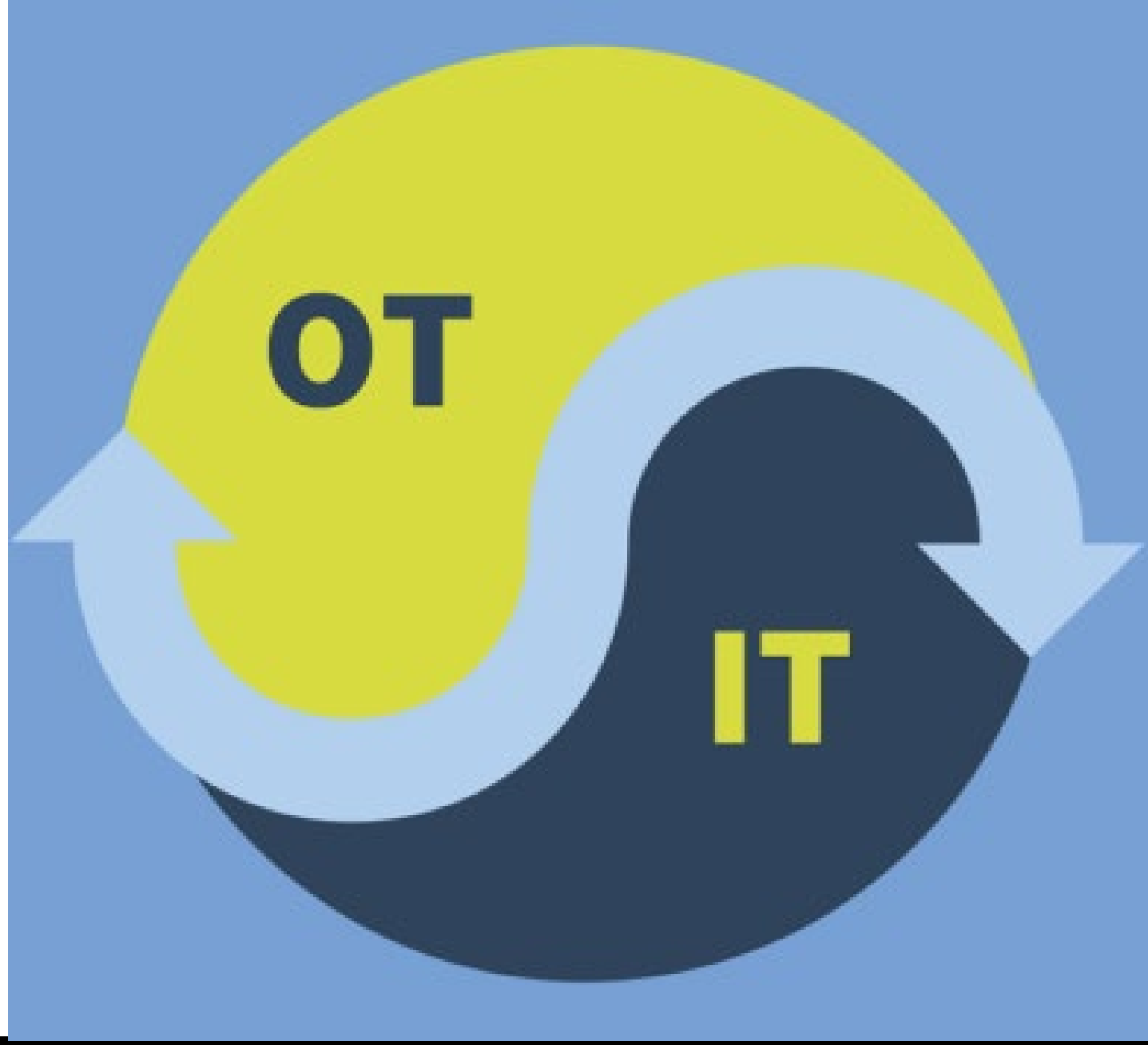


Challenges
are not
always
malicious

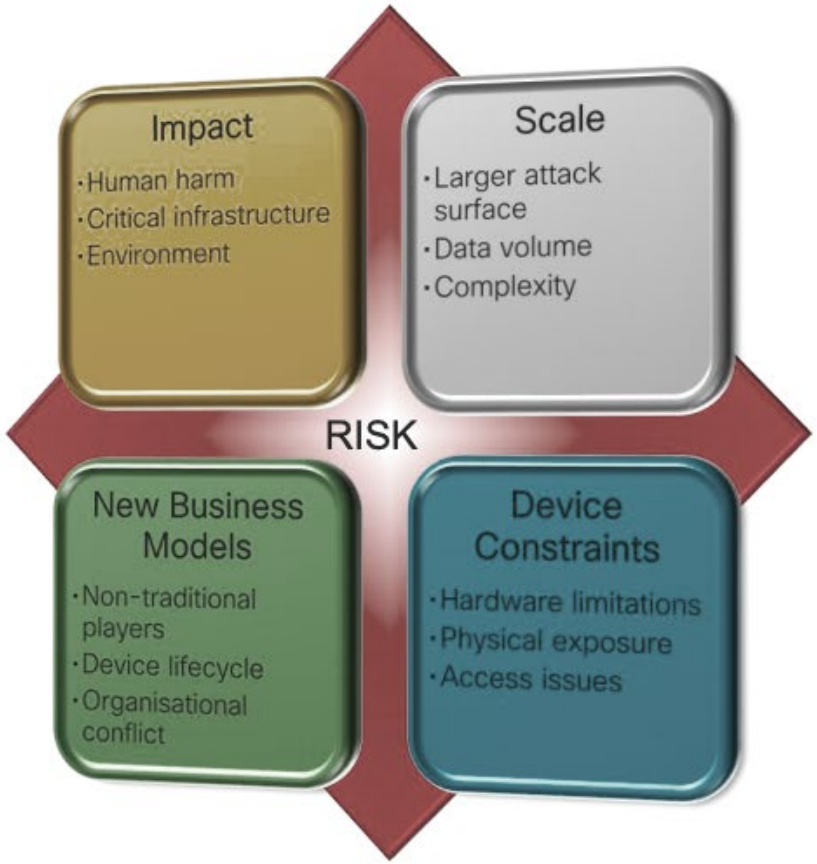


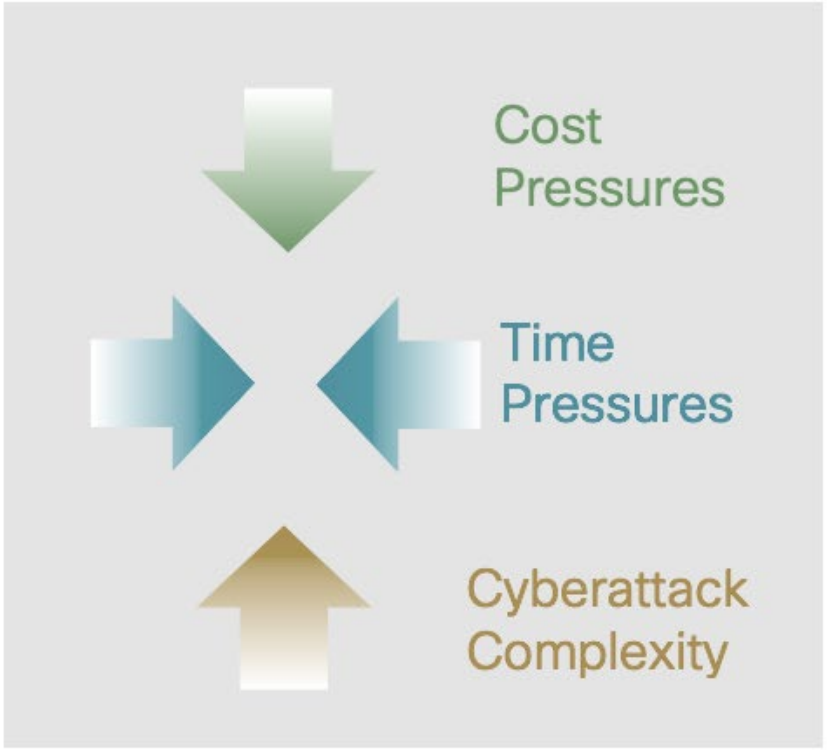
Industry 4.0 Security Topics

- What's Different With IoT / OT versus IT



Differences between IoT/OT and IT





Industry 4.0 affects Real World

- IoT/OT is not just computers, it is things
  - Big Things
  - Critical Things
  - Potential for impact is an entirely new scope and scale

- Things generate data
  - Aggregation and correlation of data
  - Telemetry

Scale

- Average Devices per IT person is ~1:200
- Scaling to IoT numbers and keeping staff numbers the same means that is about 1:1,000,000
- Data volume is scaling along with it, and data security has to scale as well
- Security data (data captured, monitored, events alerts) is growing too
- Non-heterogenous environments

Changing Business Landscape

- Manufactures may not be used to providing ongoing updates
- With inbuilt connectivity comes maintenance and patching requirements
- Devices may have long lifetimes, and support may not be there
- Ownership issues, Uptime expectations
- Businesses are being forced to change engagement models

Device Constraints

- Battery, CPU, capacity, size… cost…
- Likely no footprint, trust anchor etc.
- We used to lock computers up to keep them secure
  - "if an attacker has physical access, your system is already compromised"
- Onsite support not necessarily easy ….

Industry 4.0 Security Topics

- How IT Managers Can Deal with IoT/ OT

IoT Threat Defense

Visibility & Analysis

Detect anomalies, block threats, identify compromised hosts

ISE/TrustSec
Next Generation FW

Segmentation

Extensible, scalable segmentation to protect IoT devices and threat containment

Umbrella
Stealthwatch
ISE/TrustSec
Cognitive Threat Analytics
AMP

Remote Access

Secure third-party access with control and visibility

AnyConnect

Services

Reduce risk, design, deploy and respond to incidents while protecting the business - (SOCs)

Design
Assess risk
Incident response

IoT Threat Defense

IoT Threat Defense also analyzes network traffic entering and exiting your organization to:

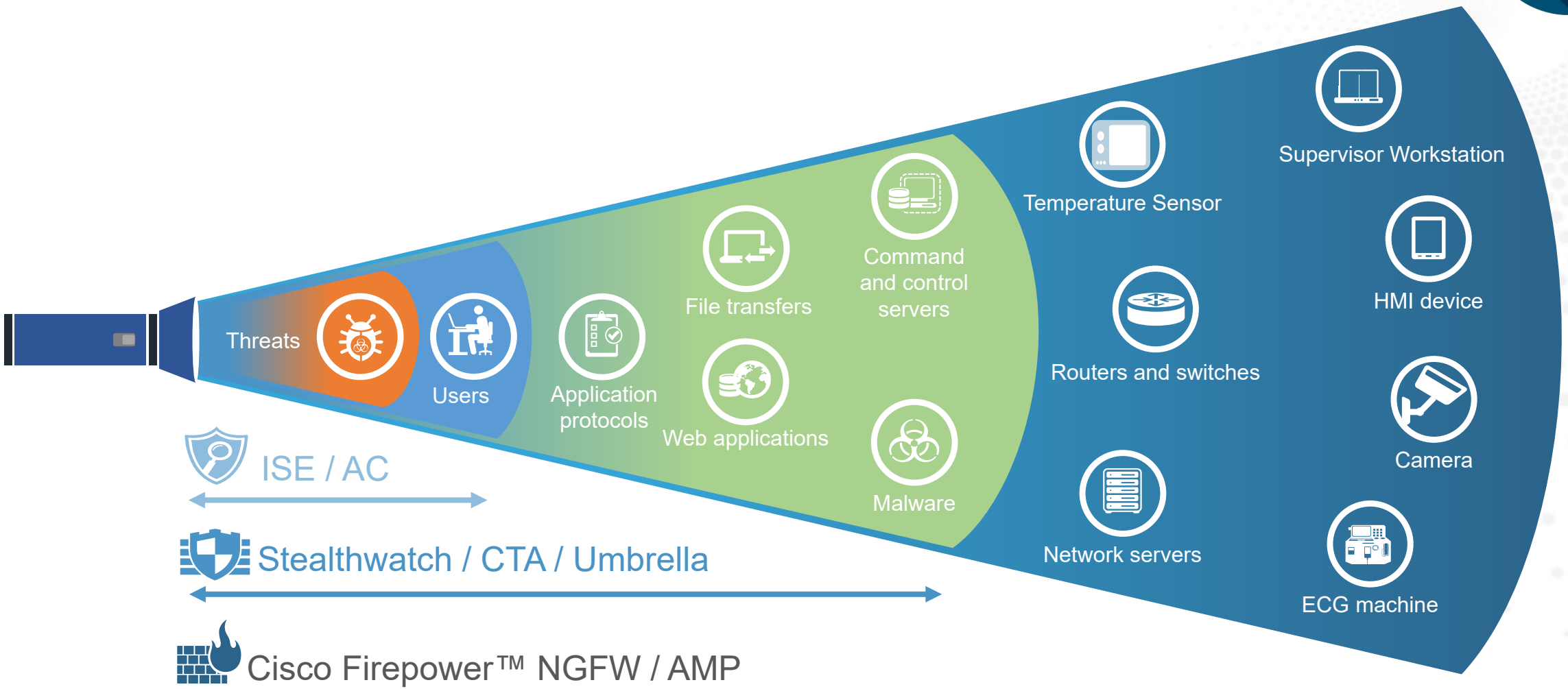
Detect anomalies

Block attacks

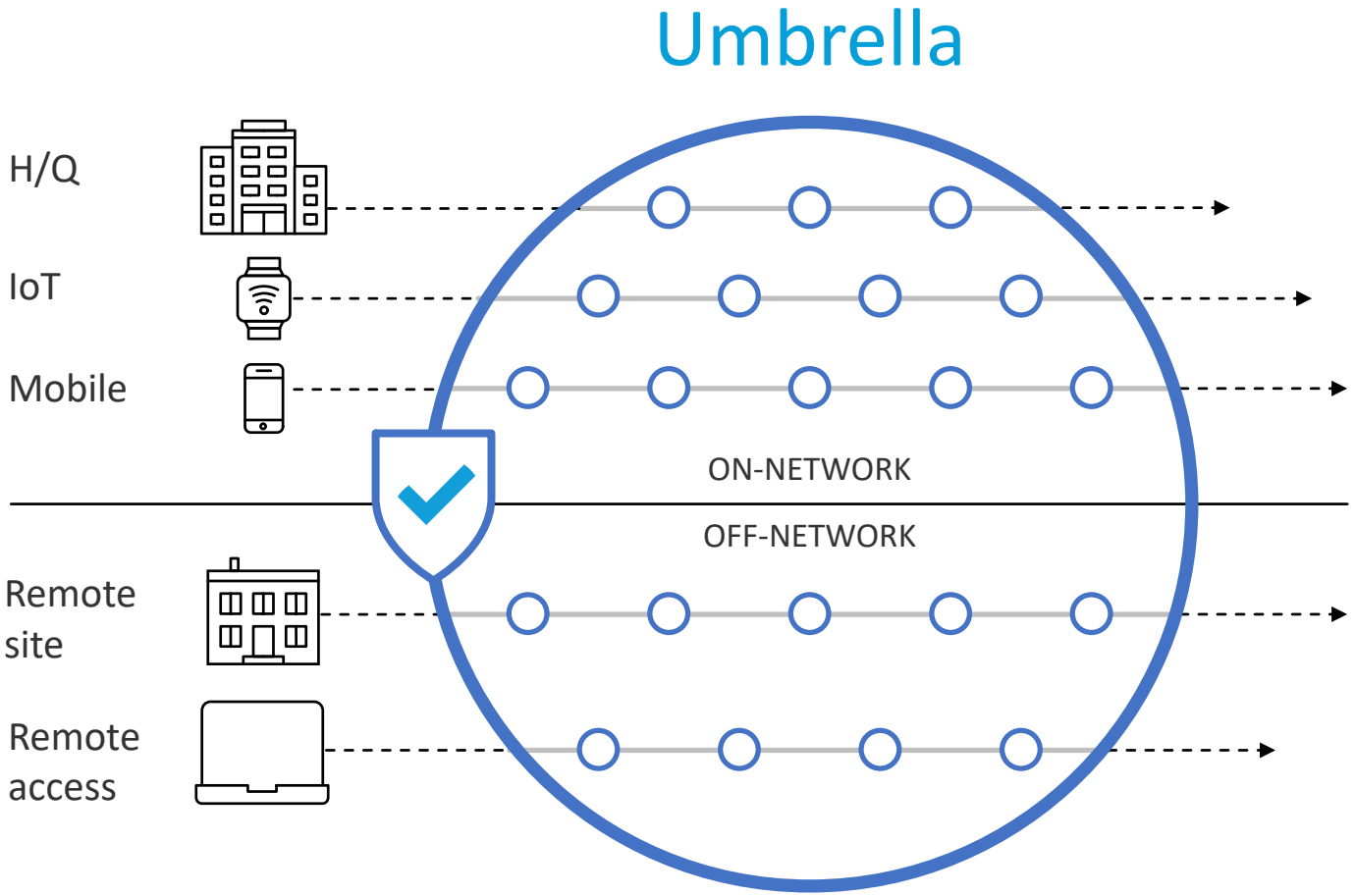
Identify compromised devices

IoT devices security-aware safety

Gaining more insight with increased visibility



Visibility and protection for all activity, anywhere



Visibility outside of your network

All locations

Any device on your network

Roaming laptops

All ports and protocol

Extensible, scalable segmentation

IoT Threat Defense also helps with segmentation by:

Protect inbound and outbound communications and from each other

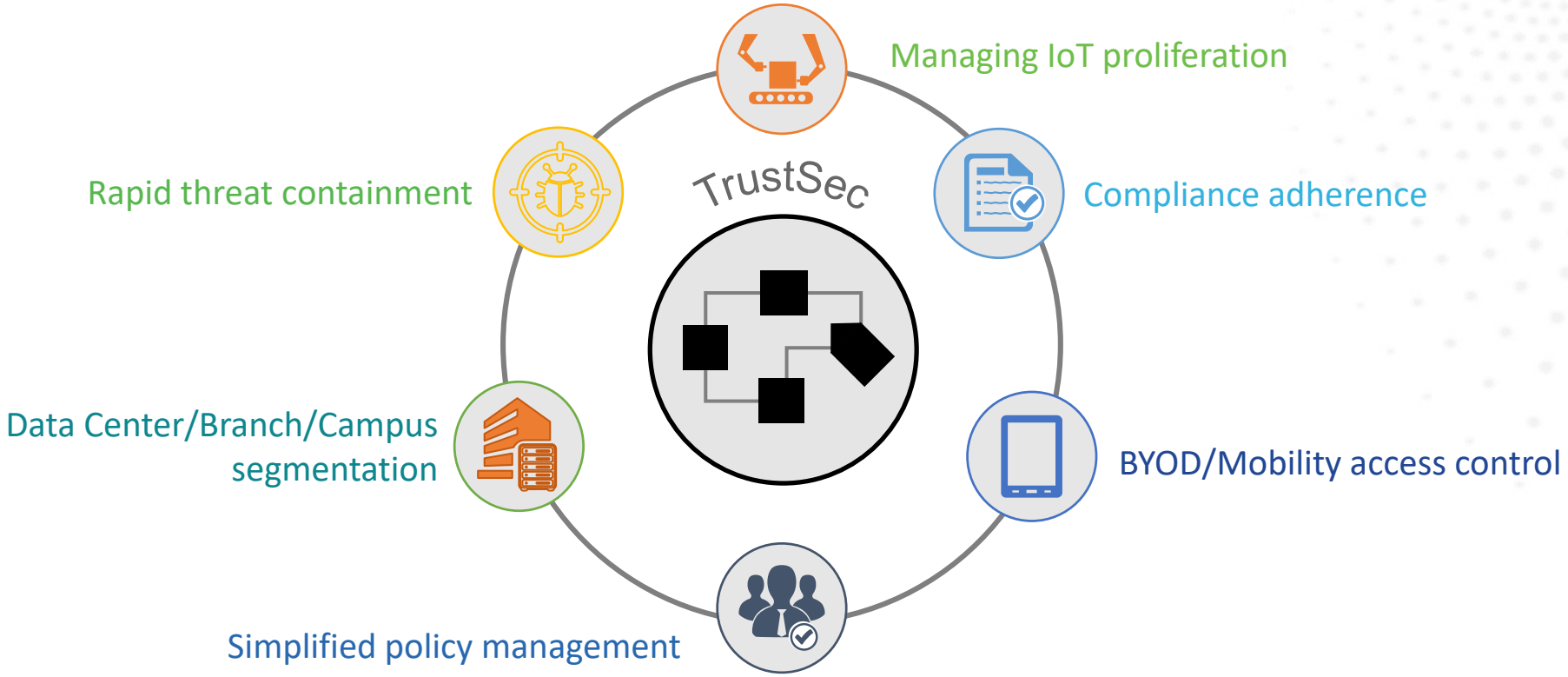
Management

Segment Infrastructure based on role and policy

Compliance and best practice

Cisco evolves network segmentation

Can be used for



Secure remote access between sites and between organizations

Remote vendor support

Defense vulnerabilities

Visibility at risk

Security Services for IoT Threat Defense

Assess and Manage Risk

- Security Network Penetration Assessment
- Security Network Architecture Assessment
- Customized Network Penetration Testing
- Privacy impact assessments
- Automation & Control System Risk Assessment (for OT)
- Network Device Security Assessment

Readiness to Adopt IoT Threat Defense

- Security Segmentation Services
- Deployment Services for:
  - AMP for Endpoint
  - Firepower (NGFW)
  - Stealthwatch
  - ISE
- Incident Response Services

Improved Ability to Resolve Issues Quickly

- Solution Support for Network Security
- Learning@Cisco for IoT training
- SecureOps for industrial automation and control system environments

CYBER A
RE:ACTION

CISCO

NOZOMI NETWORKS

Nozomi feeding Algosystems' Next Gen SOC

- GARTNER COOL VENDOR
- SUPPORTING MORE THAN 300,000 DEVICES
- MORE THAN 1,000 INSTALLATIONS
- DEPLOYMENTS IN 5 CONTINENTS
- INDUSTRY'S MOST ACTIONABLE RESEARCH AND TOOLS ON TRITON AND GREYENERGY
- STRATEGIC PARTNER OF:

CISCO IBM Security Schneider Electric


Nagios XI
Hypermap
About This Map
Nagios XI
Home Dashboard
ALGOSYSTEMS
THE PATH FORWARD
Current Threat Activity
www.algosystems.gr
CYBER A
RE:ACTION

ALGOSYSTEMS

Τομέας Πληροφορικής & Επικοινωνιών

ICT Division

Thank You!

Algosystems S.A., Λ. Συγγρού 206, 176 72 Καλλιθέα (Αθήνα) 206 Sygrou Avenue, 176 72 Kallithea (Athens)

Τηλ. /Tel. (+30) 210 9548000 Fax: +(30) 210 9548099 E-mail info@algosystems.gr www.algosystems.gr