inetum. realdolmen Positive digital flow

inetum. realdolmen Positive digital flow

SIEMENS

IT

Convergence

OT

MORE THAN

**27 000**

CONSULTANTS

2019 (Pro Forma)

**€ 2.3**

BILLION

IN REVENUE

**26** COUNTRIES

FRANCE, SPAIN, PORTUGAL, BELGIUM, MEXICO, LUXEMBOURG, POLAND, MOROCCO, ROMANIA, SWITZERLAND, BRAZIL, TUNISIA, COLOMBIA, COTE D'IVOIRE, PERU, USA, ANGOLA, CAMEROON, SINGAPORE, ENGLAND, UAE, RP OF PANAMA, CHILI, COSTA RICA, DOMINICAN REPUBLIC, ARGENTINA

**6**

ACTIVITIES

+ CONSULTING
+ APPLICATION & INFRASTRUCTURE SERVICES
+ SYSTEM INTEGRATION (Business Solutions, ERP, CRM, PLM...)
+ OUTSOURCING
+ VALUE ADDED RESELLING
+ SOFTWARE:
  - 4 vertical solutions :
    *Local governement, Insurance, Healthcare social, Retail*
  - Transverse Solutions
    *Time Management (Chronotime)*
    *DDM (Business Document)*

**MORE**

+ Proximity-Intimacy-Agility
+ Industrialisation-Automation
+ Innovation-Business

**5**

VALUES & PRINCIPLE OF ACTION

**SOLIDARITY**
We have a united entrepreneurial spirit.

**AMBITION**
Our local power fosters our global success.

**EXCELLENCE**
Our culture of excellence is a product of our daring.

**ENGAGEMENT**
We grow but stay close to our clients.

**INNOVATION**
We are constantly co-inventing the technology based business of our customers

# inetum.

Positive digital flow

**6** INNOVATION CENTERS

PARIS, NANTES, LYON, GHENT, LISBON, MADRID

Casablanca & Warsaw in 2021

**GROUP ALLIANCES**

SAP, Microsoft, Oracle, Salesforce

AWS, IBM, Sage, HRAccess

PTC, Siemens, Dassault

**21** SERVICE CENTERS

**APAC** *(Macau)* ▪ **BRAZIL** *(São Paulo)* ▪ **COLOMBIA** *(Bogota)* ▪ **FRANCE** *(Lille, Lyon, Meudon, Nantes, Toulouse)* ▪ **INDIA** *(Pune)* ▪ **MOROCCO** *(Casablanca)* ▪ **POLAND** *(Warsaw-Poznan-Lublin)* ▪ **PORTUGAL** *(Lisbon-Covilha-Bragança)* ▪ **ROMANIA** *(Bucarest-Constanza)* ▪ **SPAIN** *(Alicante-Bilbao)* ▪ **TUNISIA** *(Tunis)*

**10** GROUP PRACTICES

DIGITAL BANKING ▪
DIGITAL INSURANCE ▪ DIGITAL RETAIL ▪
DIGITAL UTILITIES ▪ E-HEALTHCARE ▪
INDUSTRY 4.0 ▪ SMART CITIES ▪
DIGITAL TELECOM ▪
DIGITAL TRANSPORT ▪
SMART DATA & AI ▪

**7**

BUSINESS SECTORS

- FINANCIAL SERVICES
- INDUSTRIES
- PUBLIC-HEALTHCARE
- TELECOM-MEDIA-TECHNOLOGIES
- ENERGY-UTILITIES-CHEMICALS
- RETAIL-CONSUMER GOODS
- TRANSPORTATION-TRAVEL-SERVICES

PARIS SAINT-GERMAIN

HANDBALL

**SPONSOR**

Inetum is Top Sponsor of Paris Saint-Germain Handball

October 2020

V. 14/10/2020

For more information: **inetum.world**

# A positive digital flow: key challenges in industry?

inetum. realdolmen
Positive digital flow

## Future Proof ICT

- How to support our business departments in a **cost efficient** and **agile (& secure)** manner?
- How do we ensure **technology adoption** and create a digital mindset?

## Employee Experience

- How to realize an ultimate **digital customer experience?**
- How to accomplish a post-COVID **workforce strategy** and engaging employee experience?
- How to close the **digital skills gap** of our workers?

## Customer Centricity

- How to get a **360-customer view** and a deep understanding of our customer needs?
- How to realize an ultimate **digital customer experience?**

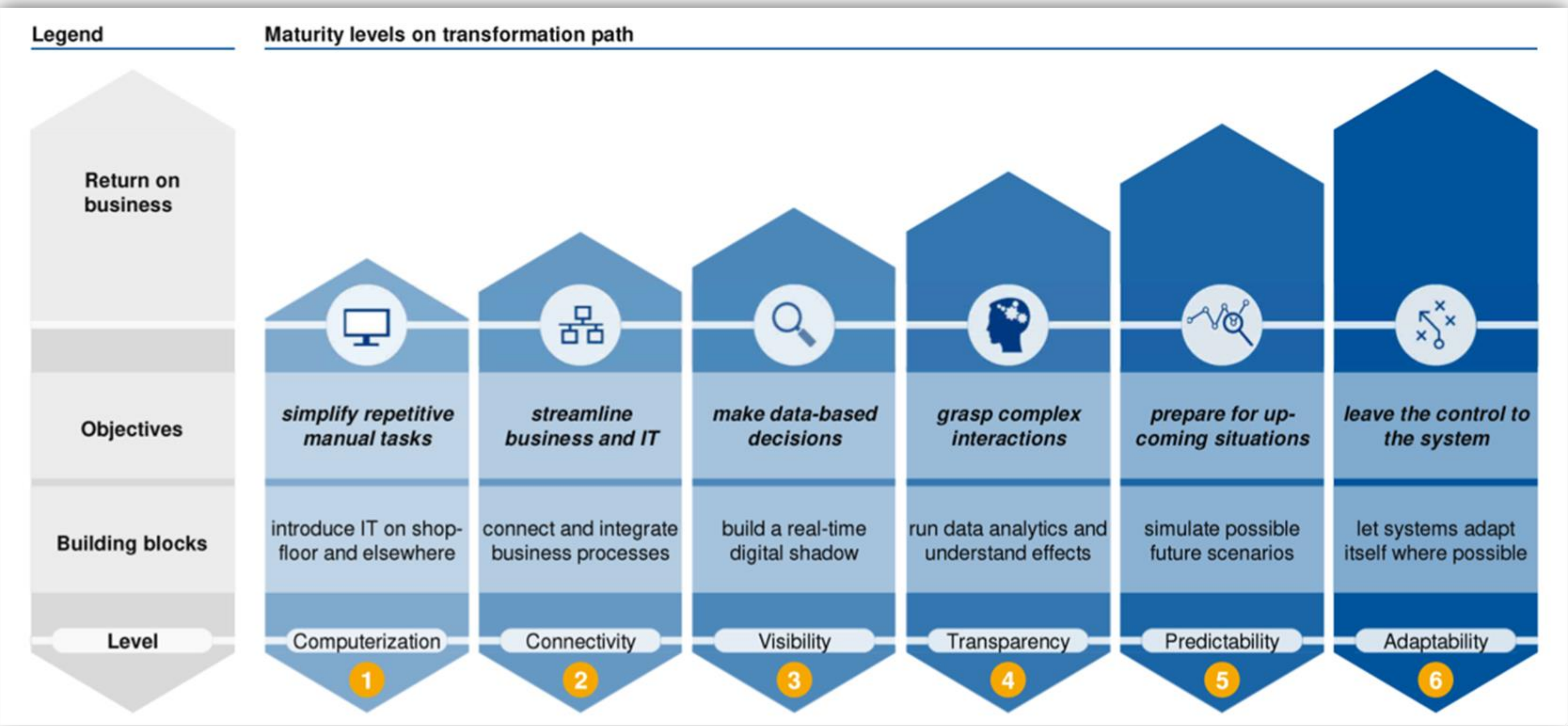
## Product & Service Innovation

- How to design new innovative products and services?
- How to develop new disruptive, **data driven business models**?

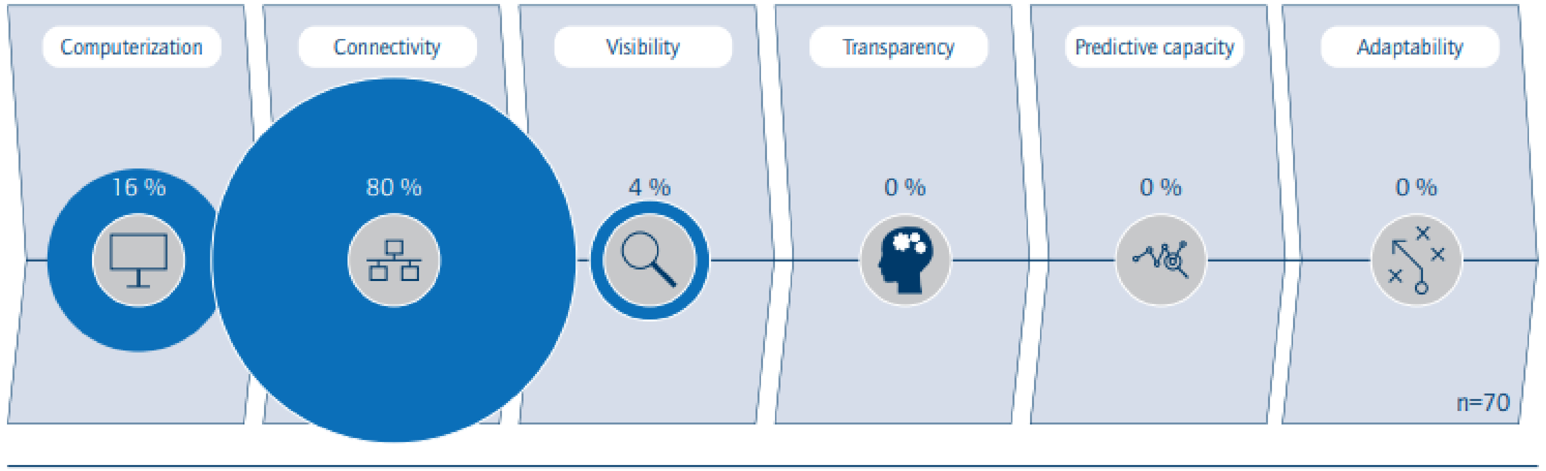
## Manufacturing Excellence

- How to increase **quality and process control**?
- How to increase production **efficiency**: OEE & asset utilization?
- How to minimize **ecological** footprint?
- How to keep up with increasing regulation and **compliancy?**

# From connected to cognitive manufacturing !



| Legend | Maturity levels on transformation path | | | | | |
|---|---|---|---|---|---|---|
| Return on business | | | | | | |
| Objectives | *simplify repetitive manual tasks* | *streamline business and IT* | *make data-based decisions* | *grasp complex interactions* | *prepare for up-coming situations* | *leave the control to the system* |
| Building blocks | introduce IT on shop-floor and elsewhere | connect and integrate business processes | build a real-time digital shadow | run data analytics and understand effects | simulate possible future scenarios | let systems adapt itself where possible |
| Level | Computerization | Connectivity | Visibility | Transparency | Predictability | Adaptability |
| | 1 | 2 | 3 | 4 | 5 | 6 |



# Your Input

Vulnerability

Cyber Criminals

External Access

Outdated OT Infrastructure

Defense in Depth

Network segmentation

Firmware Updates

Virus Updates / Patches in OT

Compatibility IT/OT SW

Version Management

System Hardening

IT Monitoring of OT

Collaboration IT/OT

Knowledge

# Agenda

**01** Intro IT-OT Convergence

**02** Benefits

**03** Challenges

**04** Best practices

**05** Getting started

# The convergence of OT & IT

Components, functions & expectations

| OT | IT |
|---|---|
| Operational Technology | Information Technology |
| Critical infrastructure for manufacturing | Critical infrastructure for data processing |
| Machinery, control systems, equipment, monitoring, … | Storage systems, computing, business applications,.. |
| Availability, integrity & confidentiality | Confidentiality, integrity & availability |
| Control engineer, Plant manager, COO, … | System engineer, IT architect, CIO, business analyst, … |

# The convergence of OT & IT

Components, functions & expectations

INDUSTRIAL GRADE

EMC Robust

Fast Connect (steel plugs)

Fan-less

…

PROFINET

PROFISAFE

PROFIENERGY

MODBUS

…

Easy Diagnostics

Easy Configuration

Easy Replacement

…

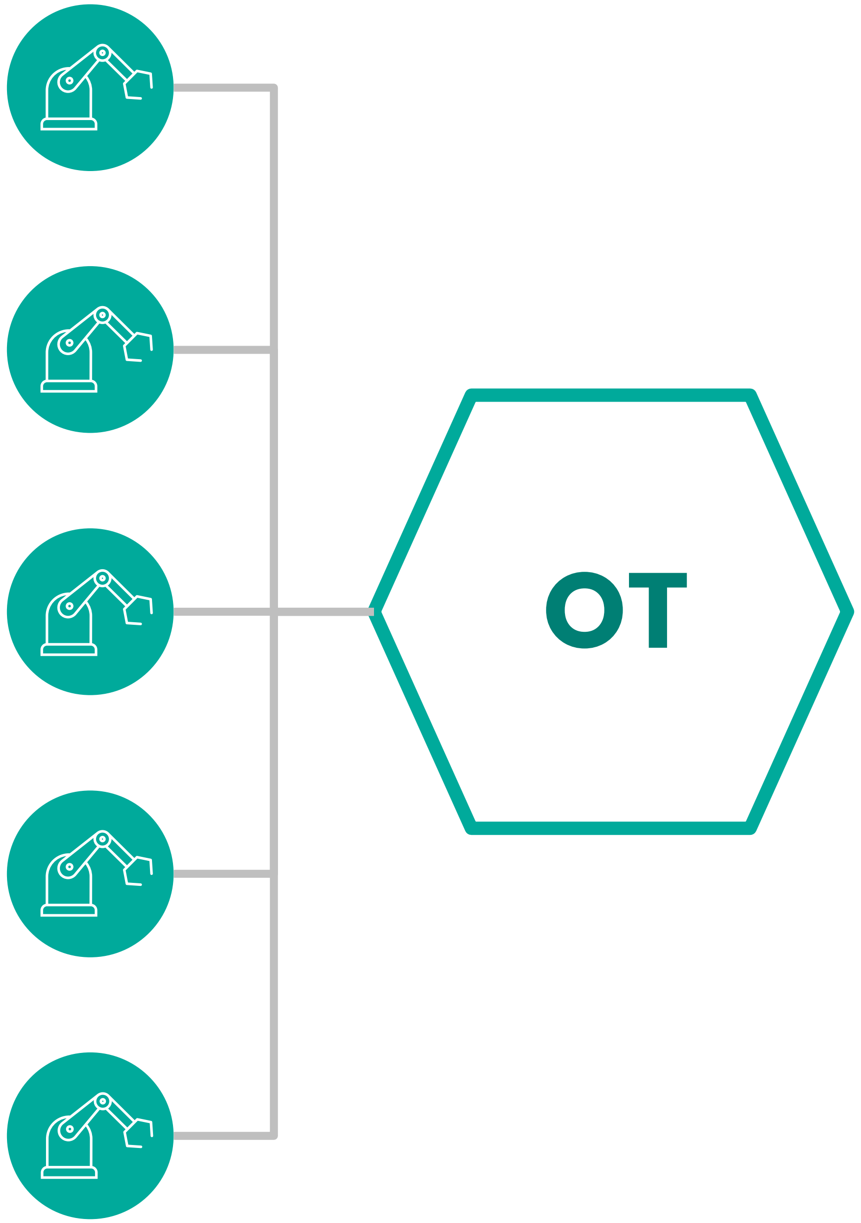
Operational Technology

Critical infrastructure for **manufacturing**

Machinery, control systems, equipment, monitoring, …

**Availability**, integrity & confidentiality

Control engineer, Plant manager, COO, …



inetum realdolmen
Positive digital flow

# Benefits of OT & IT convergence

### CONTROL

Enables more direct control and complete monitoring of complex systems

### SILO

Less siloed IT & OT departments and more shared expertise

### REGULATIONS

Improved compliance with regulatory standards

### ASSETS

More efficient asset management across both environments

### DATA

Decision making improves due to having access to real life data insight

### AVAILABILITY

Improved availability through preventive maintenance and enhanced security

# Benefits of OT & IT convergence

### CONTROL

Enables more direct control and complete monitoring of complex systems

### REGULATIONS

Improved compliance with regulatory standards

### DATA

Decision making improves due to having access to real life data insight

### SILO

Less siloed IT & OT departments and more shared expertise

### ASSETS

More efficient asset management across both environments

### AVAILABILITY

Improved availability through preventive maintenance and enhanced security

# Data driven applications will be the main driver for further productivity increases in manufacturing – Use case driven

OEE analysis & improvements

Predictive Maintenance

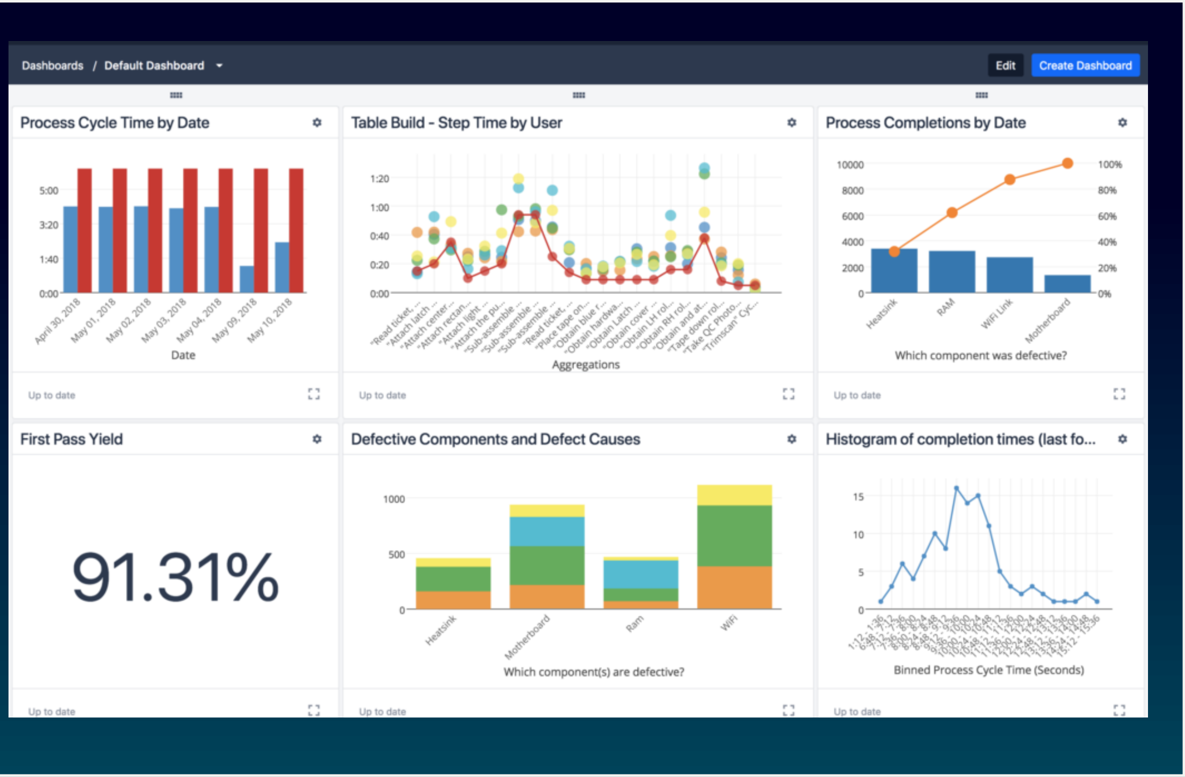
Energy Management

Inventory Management

Service Management

…

## Application



Complete data management and access (analog-, image-data & further)

Standardized data integration – of any source

Standardized system inter-connection to MES/ERP/BI

## Asset, component and sensor data

More data

More assets

More connectivity

More governance

More security risks

IT/OT Cross Collaboration

IT/OT Process Alignment

More attack surface

More unpatched devices

More security risks

Less visibility and asset management

More lateral movement

# Security strategies & best practices

### Security Roadmap

Benchmark your security maturity and define needed actions to minimize risks

### Asset Management

Know what you have means you know what to protect

### Network Segmentation

Avoid lateral movement by dividing the network

### Network Access Control

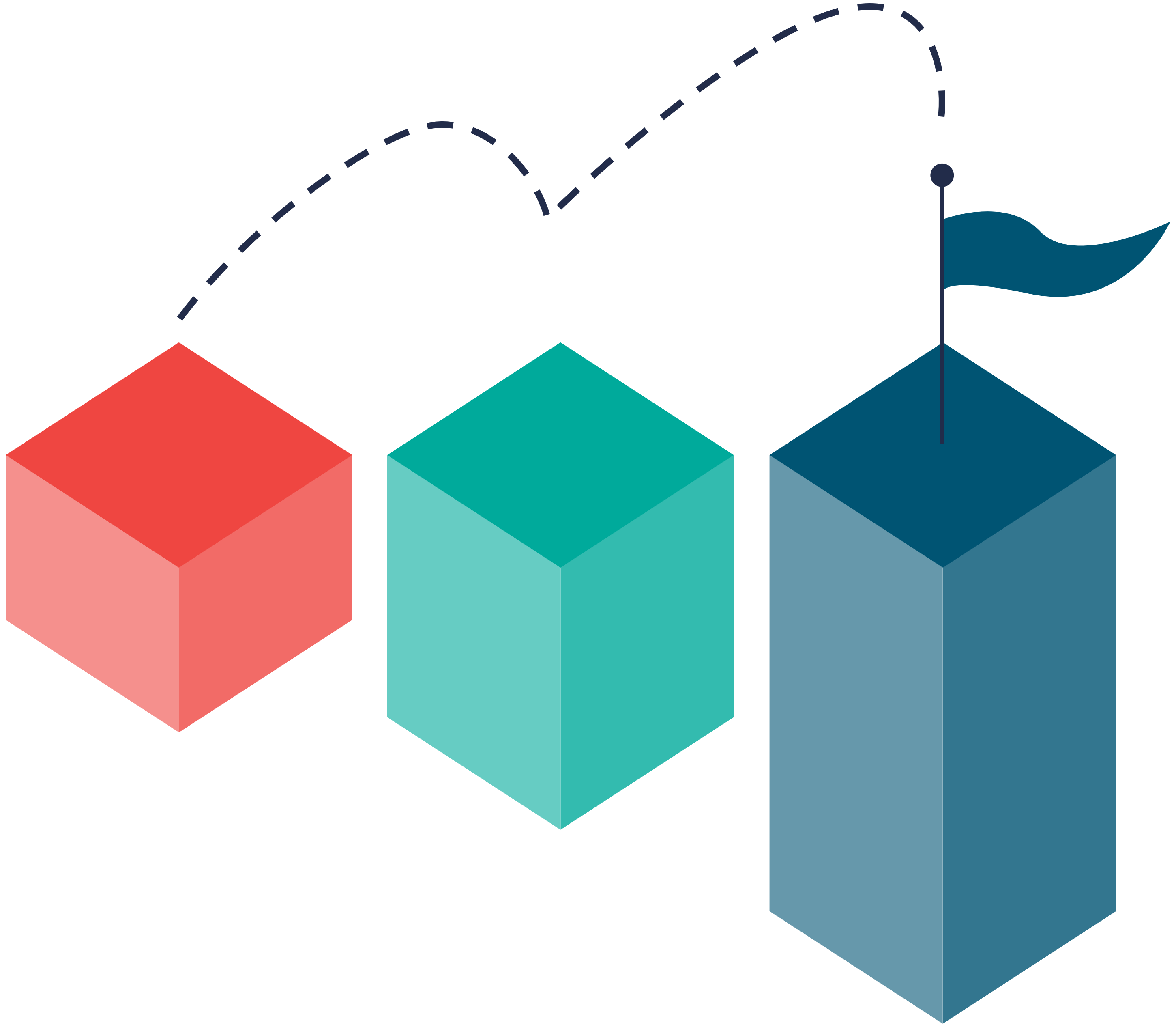
Gain control on which devices can do what on your network

# Security Roadmap

Assess current security maturity and describe recommendations to reduce risk

## “From here to there”

- Where are you today?
- How do you align with industry standard security frameworks?
- Where do you want to go?
- How will we get there?
- What budget must be foreseen?
- What’s the user impact?



## Roadmap outcome

- Identify potential risks
- Insight on level of security maturity
- Prioritized actionable recommendations
- Budget estimation per recommendation

inetum realdolmen
Positive digital flow

# Security Roadmap

Assess current security maturity and describe recommendations to reduce risk

| ID | Topic |
|---|---|
| 1 | Inventory and control of hardware assets |
| 2 | Inventory and control of software assets |
| 3 | Data protection |
| 4 | Secure configuration of hardware assets and software |
| 5 | Account management |
| 6 | Access Control Management |
| 7 | Continuous Vulnerability Management |
| 8 | Audit Log Management |
| 9 | Email and web browser protections |
| 10 | Malware defenses |
| 11 | Data Recovery |
| 12 | Network infrastructure management |
| 13 | Network monitoring and defense |
| 14 | Security awareness and training |
| 15 | Service provider management |
| 16 | Application software security |
| 17 | Incident response management |
| 18 | Penetration testing |

Actions that form a set of best practices that mitigate the most common attacks against systems and networks

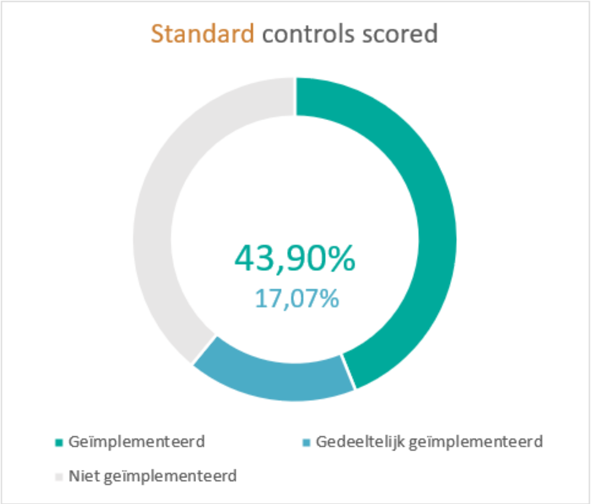
STANDARD

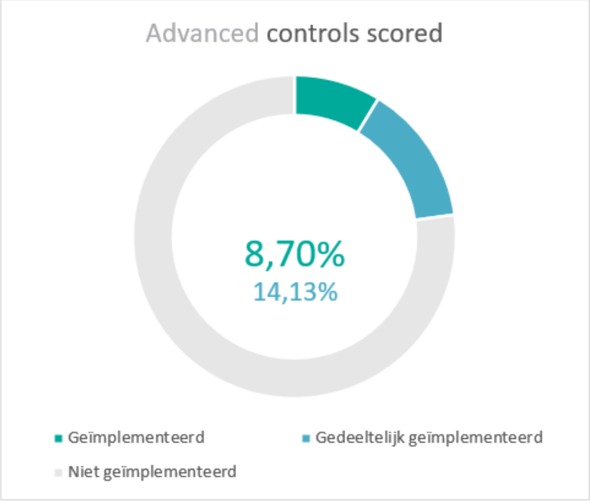
ADVANCED

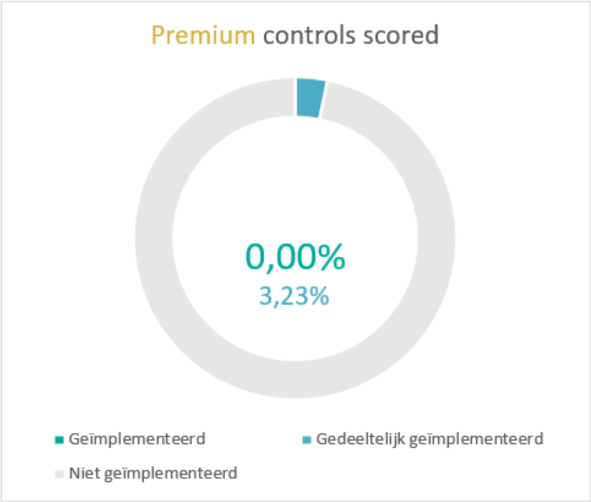
PREMIUM

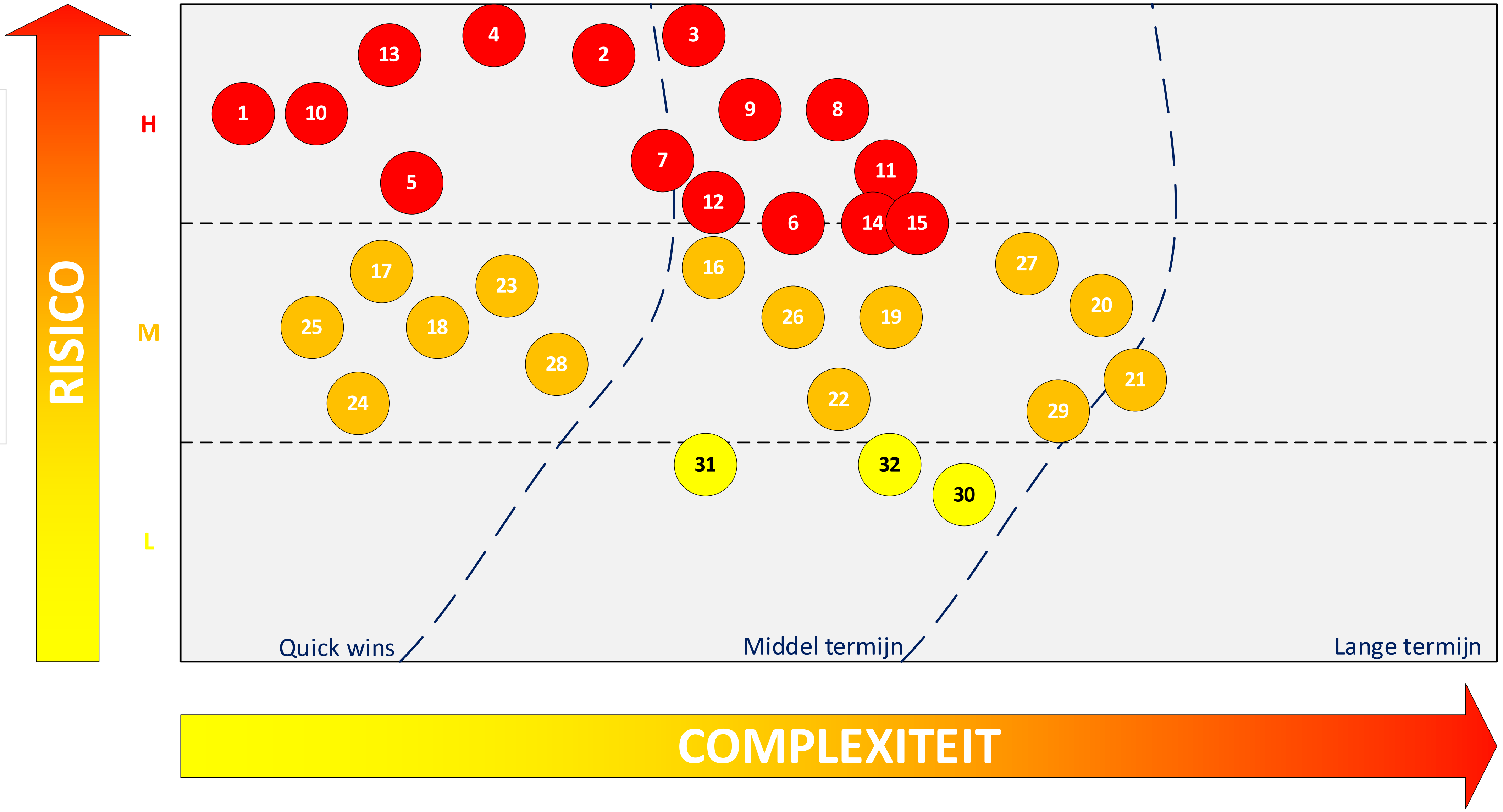
# Security Roadmap

Assess current security maturity and describe recommendations to reduce risk







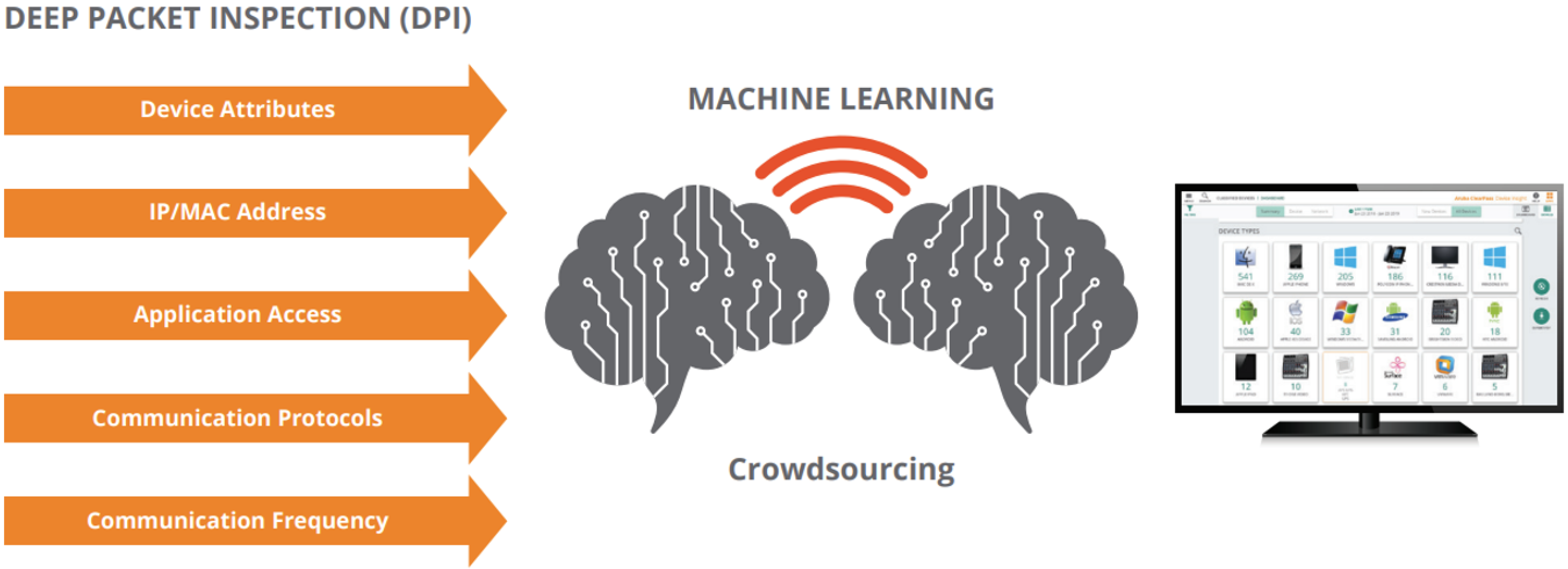


# Asset Management

Know what you have, to know what you need to protect

## CLEARPASS DEVICE INSIGHT

**Device Visibility** is key to proper segmentation



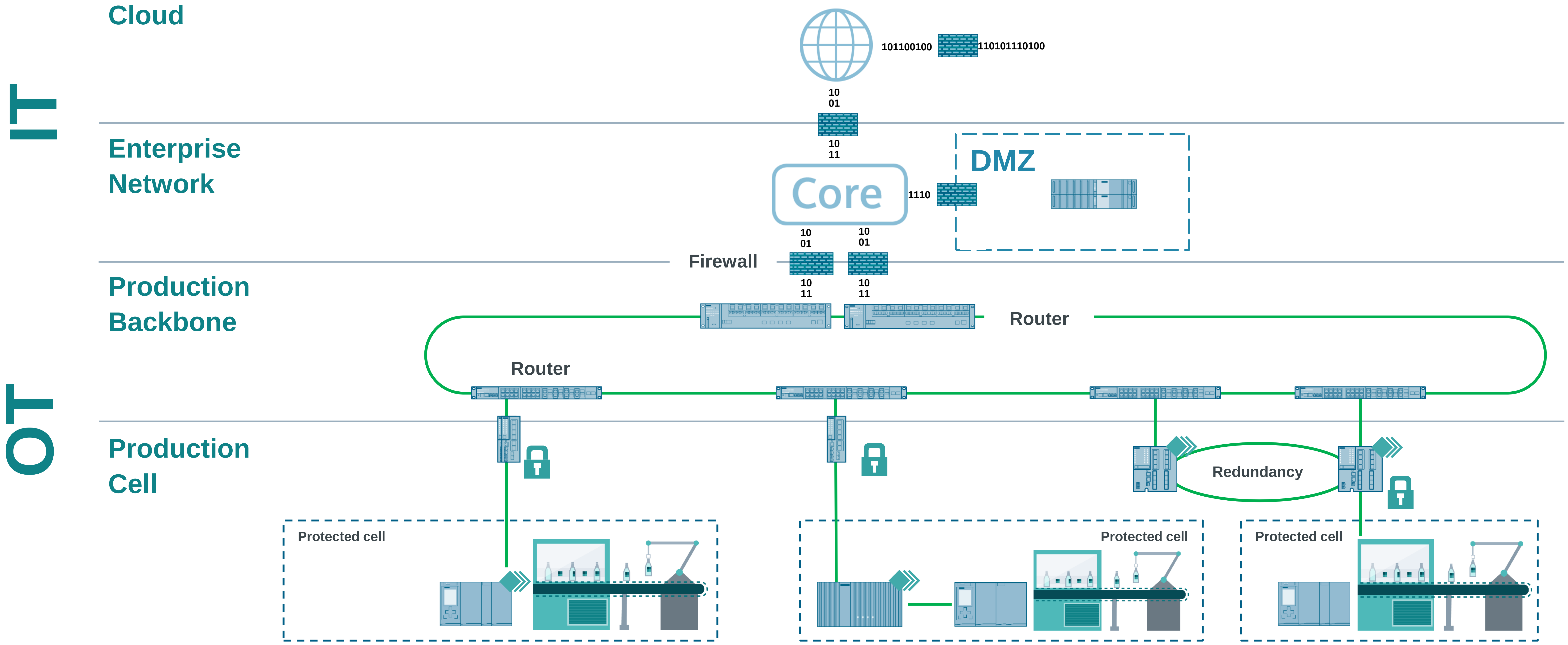
DEEP PACKET INSPECTION (DPI)

- Device Attributes
- IP/MAC Address
- Application Access
- Communication Protocols
- Communication Frequency

MACHINE LEARNING

Crowdsourcing

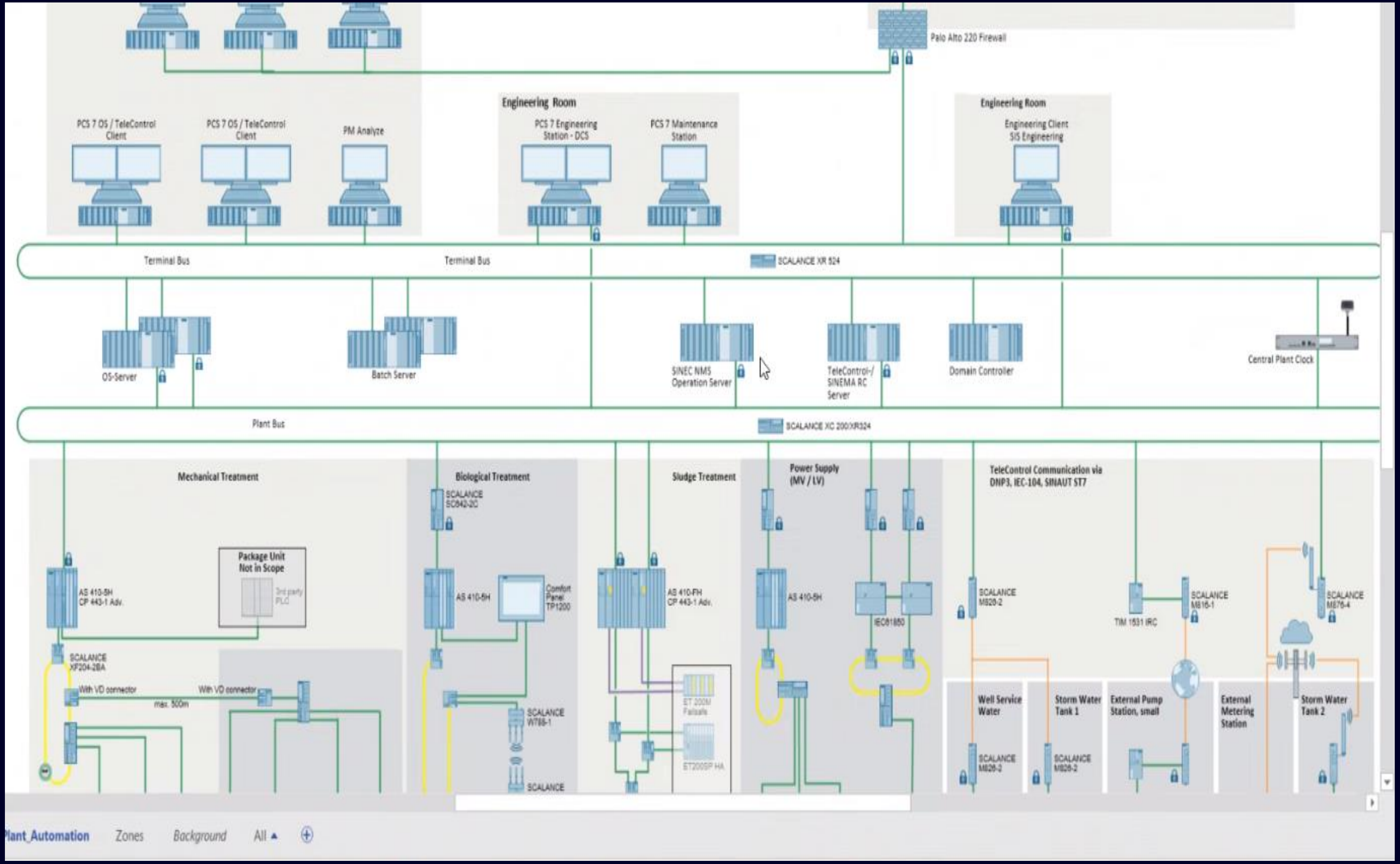
# Network Segmentation on different levels



# NETWORKSEGMENTATION and CELL PROTECTION
# PLANTBUS vs TERMINALBUS

SCADA design
vs purdue model

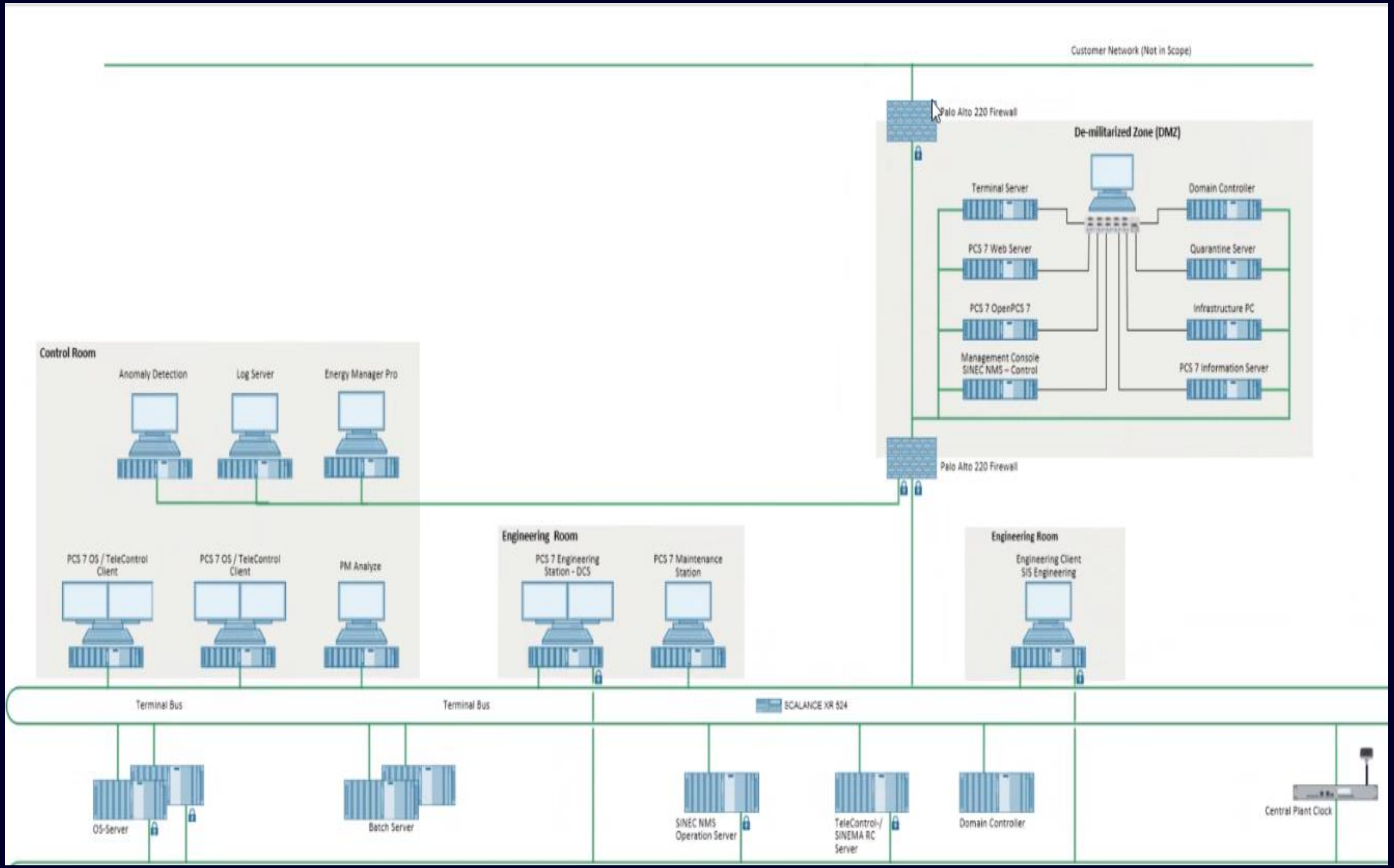
## Conflict



# INDUSTRIAL DMZ CONCEPT

A DMZ dedicated for OT

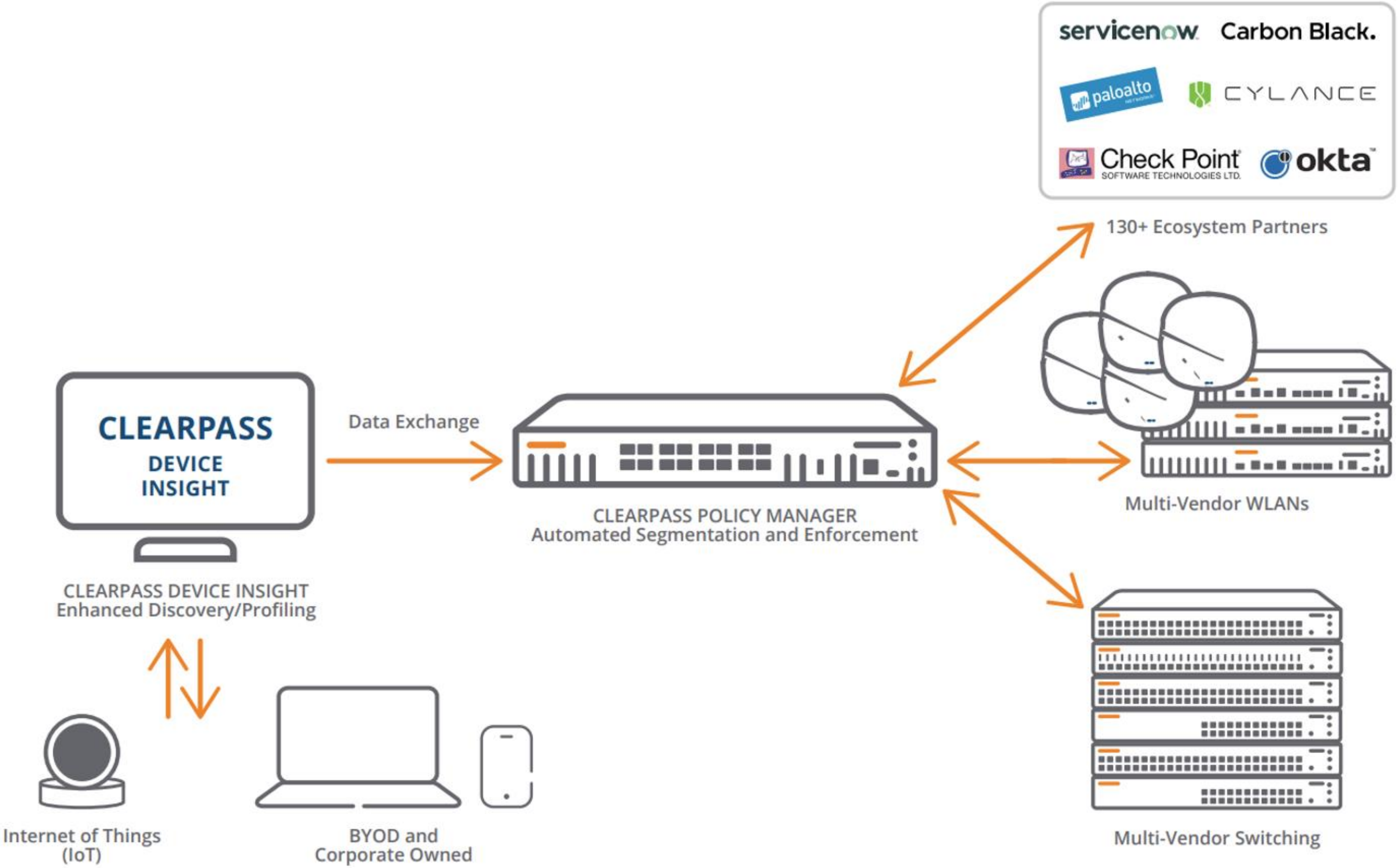
IDMZ



SIEMENS

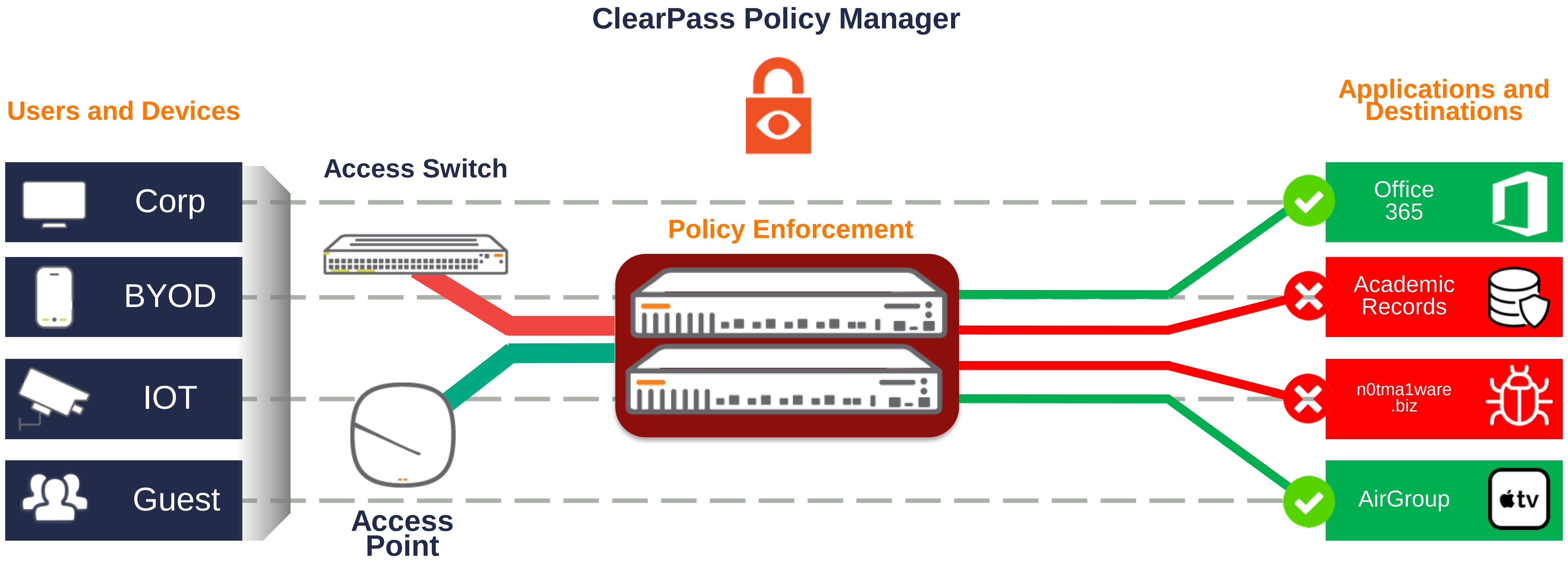
# Network Access Control

Gain control on which devices can do what on your network



# Network Access Control

Gain control on which devices can do what on your network



# Security strategies & best practices

## Monitoring

Get notified when anomalies are detected or if systems are unavailable

## Patch Management

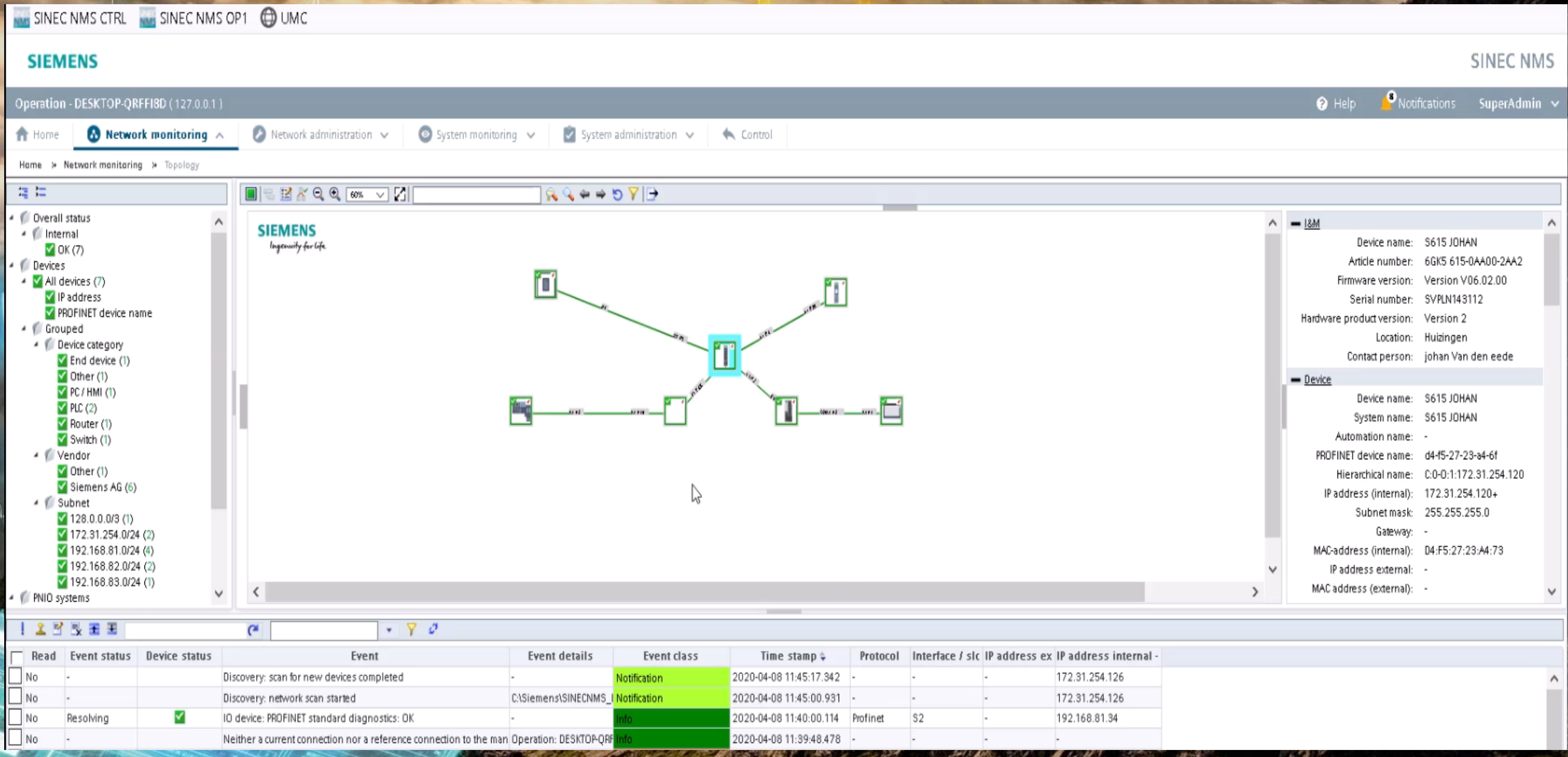
Make sure that all devices have the latest security patches installed

## Vulnerability Management

Calculate the risks of new vulnerabilities that might affect your assets

## Identity Access Management

Gain control on who can do what on your network



Operation - DESKTOP-QRFFI8D ( 127.0.0.1 )

Home » Network monitoring » Topology

- Overall status
  - Internal
    - ☑ OK (7)
- Devices
  - ☑ All devices (7)
    - ☑ IP address
    - ☑ PROFINET device name
  - Grouped
    - Device category
      - ☑ End device (1)
      - ☑ Other (1)
      - ☑ PC / HMI (1)
      - ☑ PLC (2)
      - ☑ Router (1)
      - ☑ Switch (1)
    - Vendor
      - ☑ Other (1)
      - ☑ Siemens AG (6)
    - Subnet
      - ☑ 128.0.0.0/3 (1)
      - ☑ 172.31.254.0/24 (2)
      - ☑ 192.168.81.0/24 (4)
      - ☑ 192.168.82.0/24 (2)
      - ☑ 192.168.83.0/24 (1)
- PNIO systems

I&M

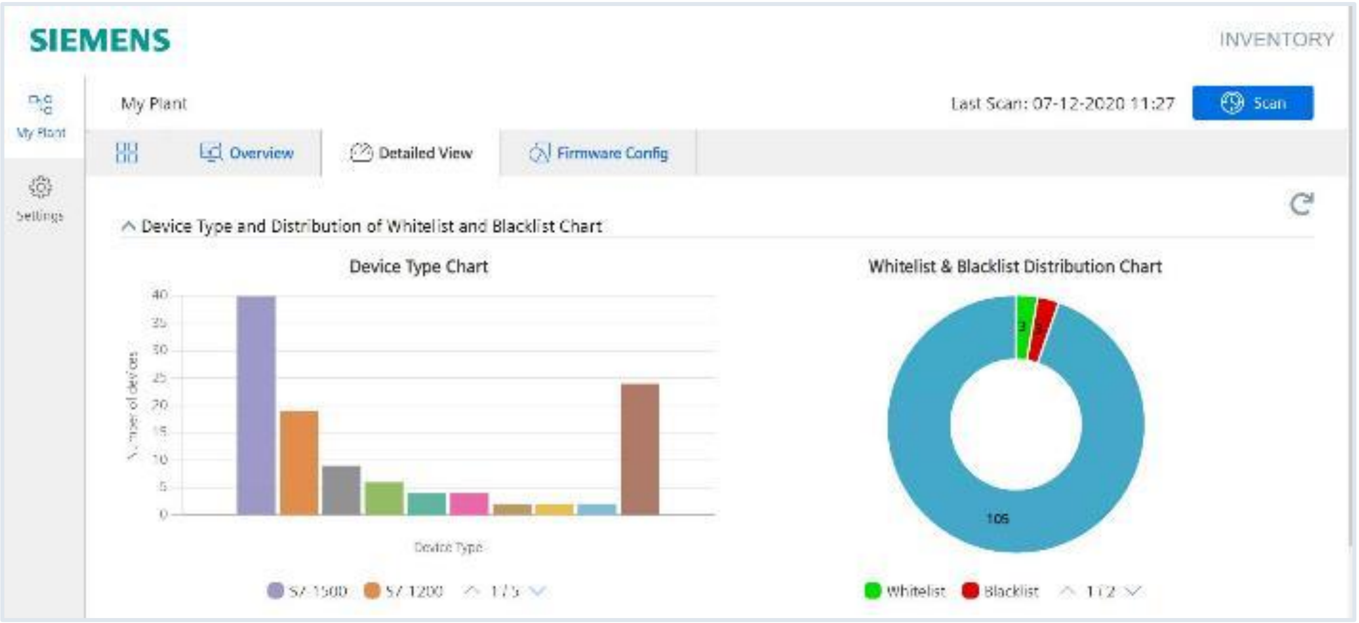
Device name: S615 JOHAN
Article number: 6GK5 615-0AA00-2AA2
Firmware version: Version V06.02.00
Serial number: SVPLN143112
Hardware product version: Version 2
Location: Huizingen
Contact person: johan Van den eede

Device

Device name: S615 JOHAN
System name: S615 JOHAN
Automation name: -
PROFINET device name: d4-f5-27-23-a4-6f
Hierarchical name: C:0-0:1:172.31.254.120
IP address (internal): 172.31.254.120+
Subnet mask: 255.255.255.0
Gateway: -
MAC-address (internal): D4:F5:27:23:A4:73
IP address external: -
MAC address (external): -

| □ | Read | Event status | Device status | Event | Event details | Event class | Time stamp | Protocol | Interface / slc | IP address ex | IP address internal - |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | No | - | | Discovery: scan for new devices completed | - | Notification | 2020-04-08 11:45:17.342 | - | - | - | 172.31.254.126 |
| □ | No | - | | Discovery: network scan started | C:\Siemens\SINECNMS_I | Notification | 2020-04-08 11:45:00.931 | - | - | - | 172.31.254.126 |
| □ | No | Resolving | ☑ | IO device: PROFINET standard diagnostics: OK | - | Info | 2020-04-08 11:40:00.114 | Profinet | S2 | - | 192.168.81.34 |
| □ | No | - | | Neither a current connection nor a reference connection to the man | Operation: DESKTOP-QRF | Info | 2020-04-08 11:39:48.478 | - | - | - | - |

# OT aware network monitoring & management



**Available features**

- Works for Siemens and 3rd party devices
- Available information for all devices (also with Device Scanner Service)
  - MAC Address, IP Address, Subnet mask
  - Order number (for PROFINET devices)
  - FW-Version (for PROFINET devices)
  - Hardware version (for PROFINET devices)
  - Software version (for PROFINET devices)
  - Serial number (for PROFINET devices)
  - CPU status (for PROFINET devices)
  - Station name (for PROFINET devices)
- Firmware check (Blacklist/Whitelist) to detect outdated firmware
- MQTT interface to share inventory information with e.g. SAP ERP system
- Based on PROFINET mechanism and standard protocols (TCP, RPC and SNMP)
- Plug and play configuration

# Early detection of threats with Industrial Anomaly Detection

## Industrial Anomaly Detection

- Transparency on the shopfloor
- Detecting non-standard behavior

## Main value drivers

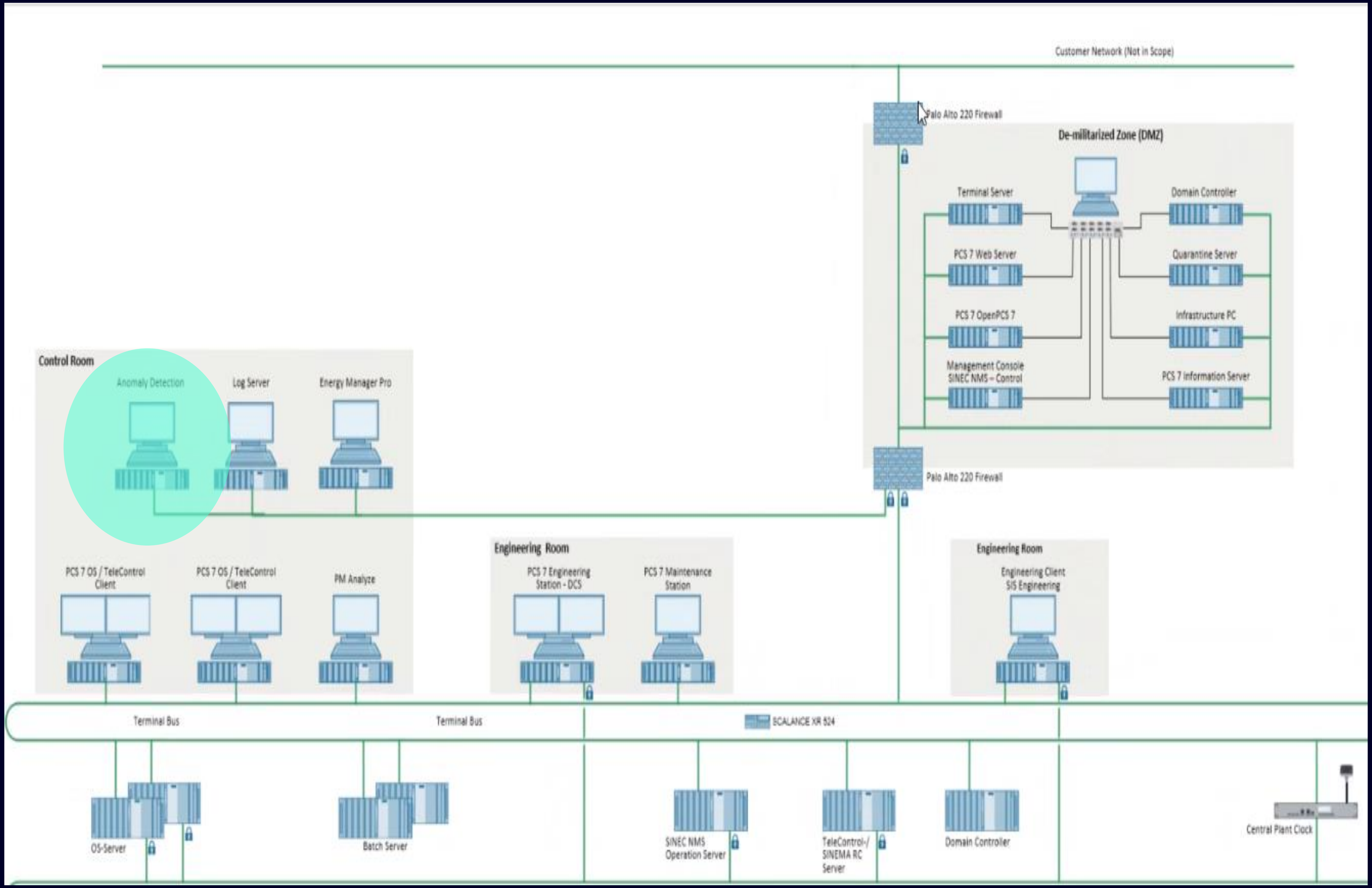
Transparency over data exchange within industrial networks

Early detection of anomalies and threats

Transparency over assets and vulnerabilities

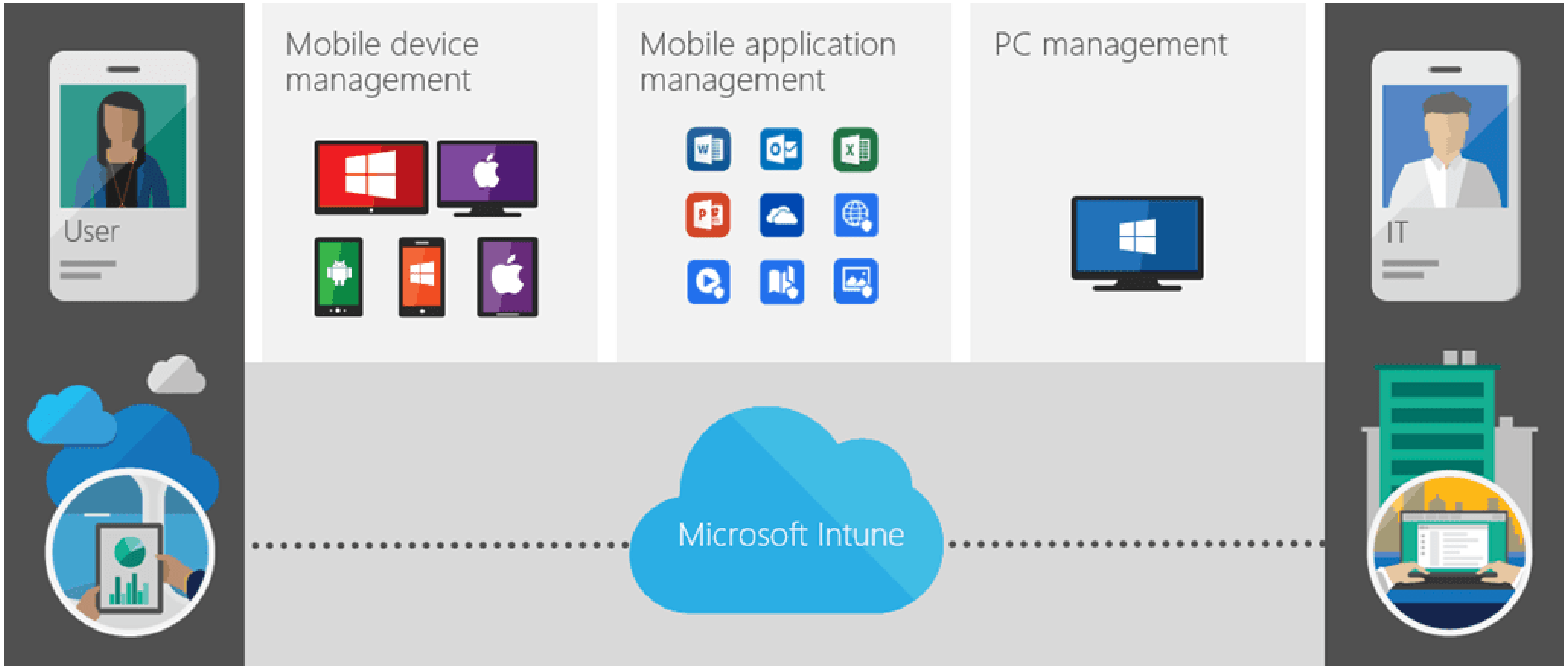
# INDUSTRIAL DMZ CONCEPT

## Industrial
## ANOMALY Detection

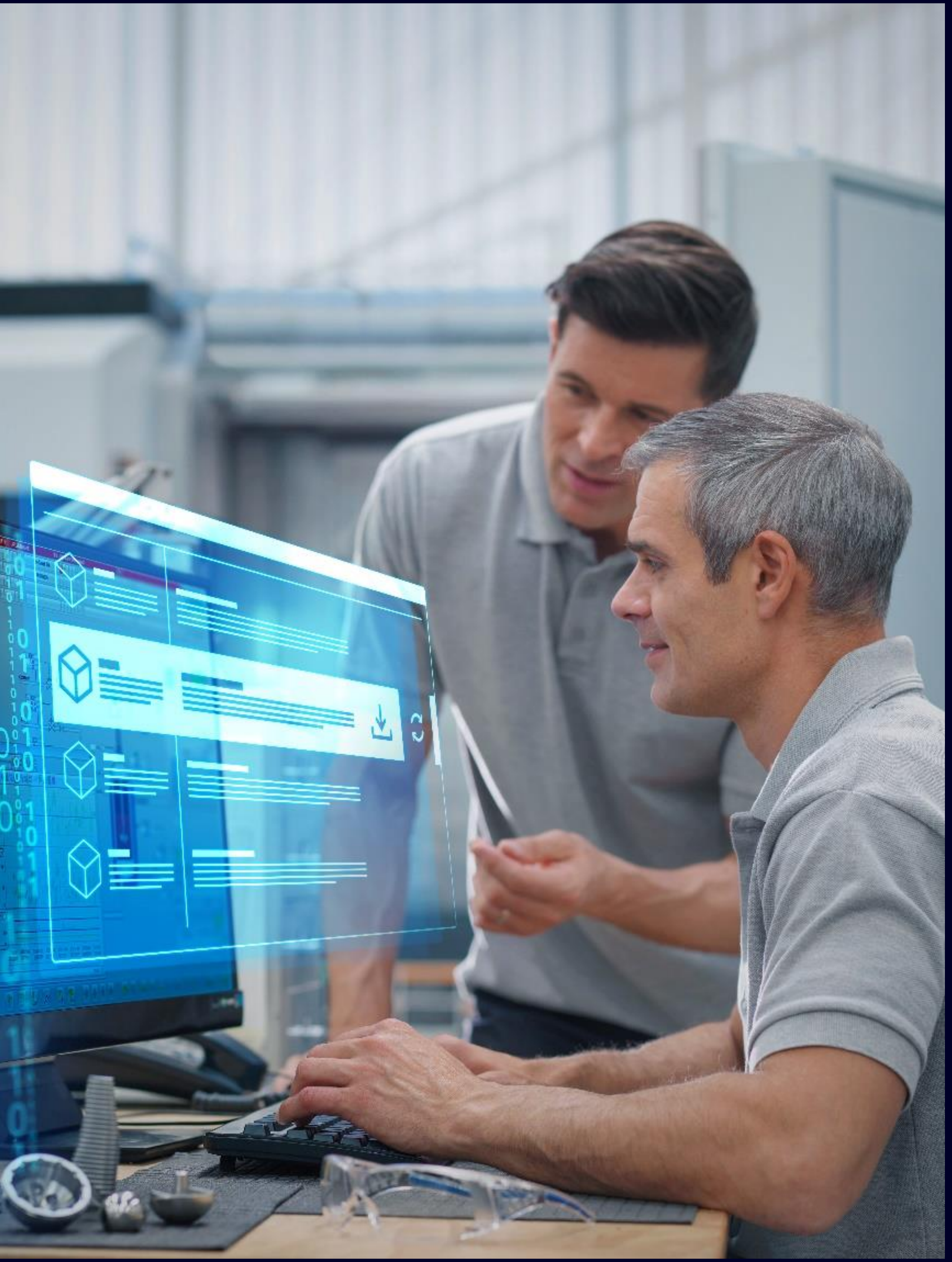


# Patch management

Make sure that all devices have the latest security patches installed



# Managing Vulnerabilities & Critical Updates
# Patch Management !



## Patch Management

- Security patches and critical updates in Microsoft products for **SIMATIC PCS 7/WIN CC** to simplify the patch process on the plant.

### How does it work?

- **Step 1:** tested and verified for compatibility
- **Step 2:** The **central WSUS** – sends the information automatically to the **local WSUS** server.
- **Step 3:** The customer receives a notification and can download the approved patches directly from Microsoft.

More info: FAQ here

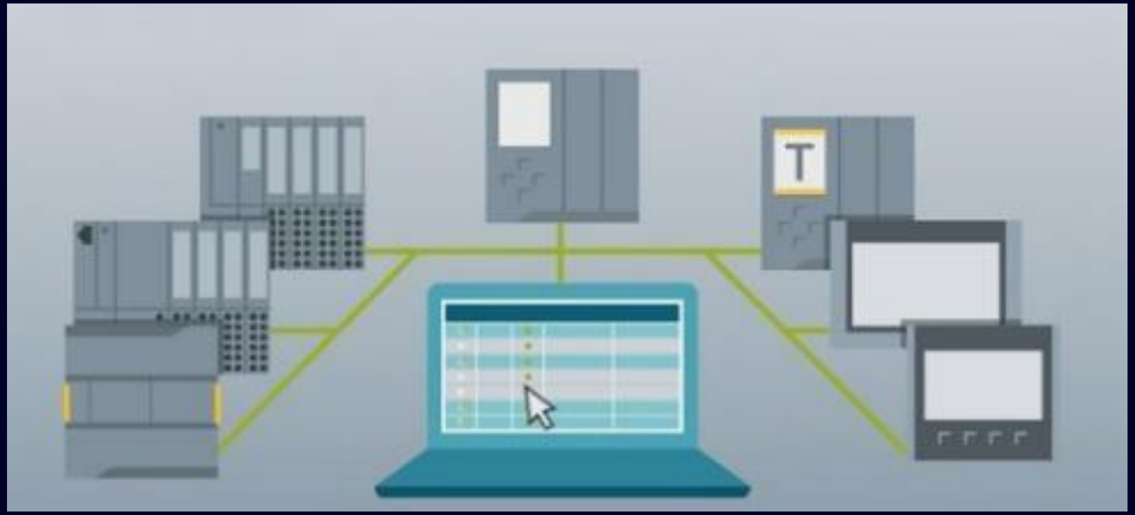
## Main value drivers

Save time and cost due to reduction of manual work on-site

Minimize risk of human error

Enhanced plant availability

# Update your systems with SIMATIC Automation Tool

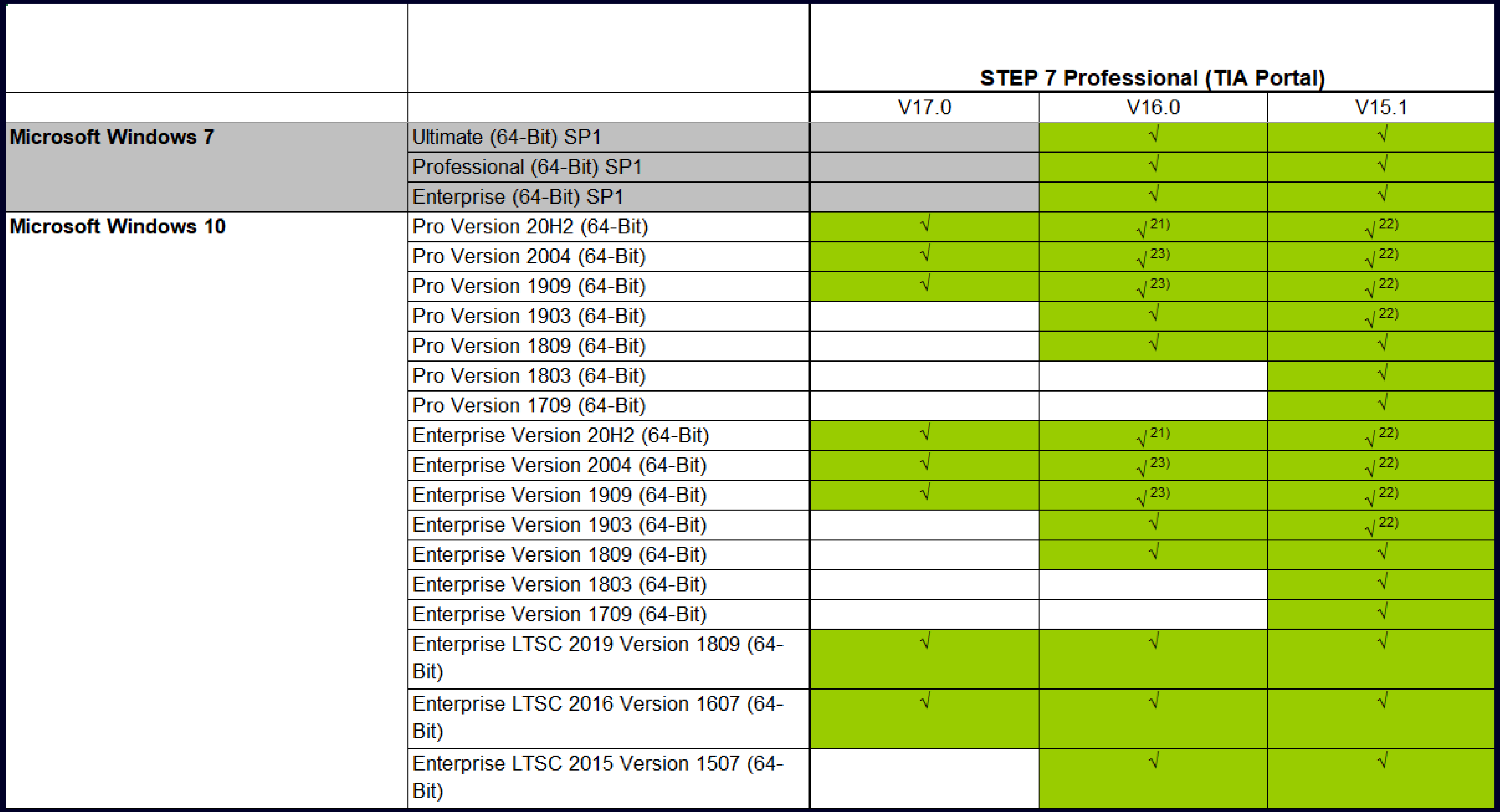


Available Features

- Works separately from TIA portal
- Firmware, application and PLC code update for S7-1200 and S7-1500
- Show network information (IP, MAC, Subnet mask, Gateway, Network Interface, Device Type, Device status, firmware, current application ID
- User management from Edge platform is applied to update restriction/approval
- Remote Updates via SIMATIC Automation Tool with 2 separated network interfaces for secure update mechanism

# Tested/Guaranteed SW Compatibility

Software combinations need vendor support



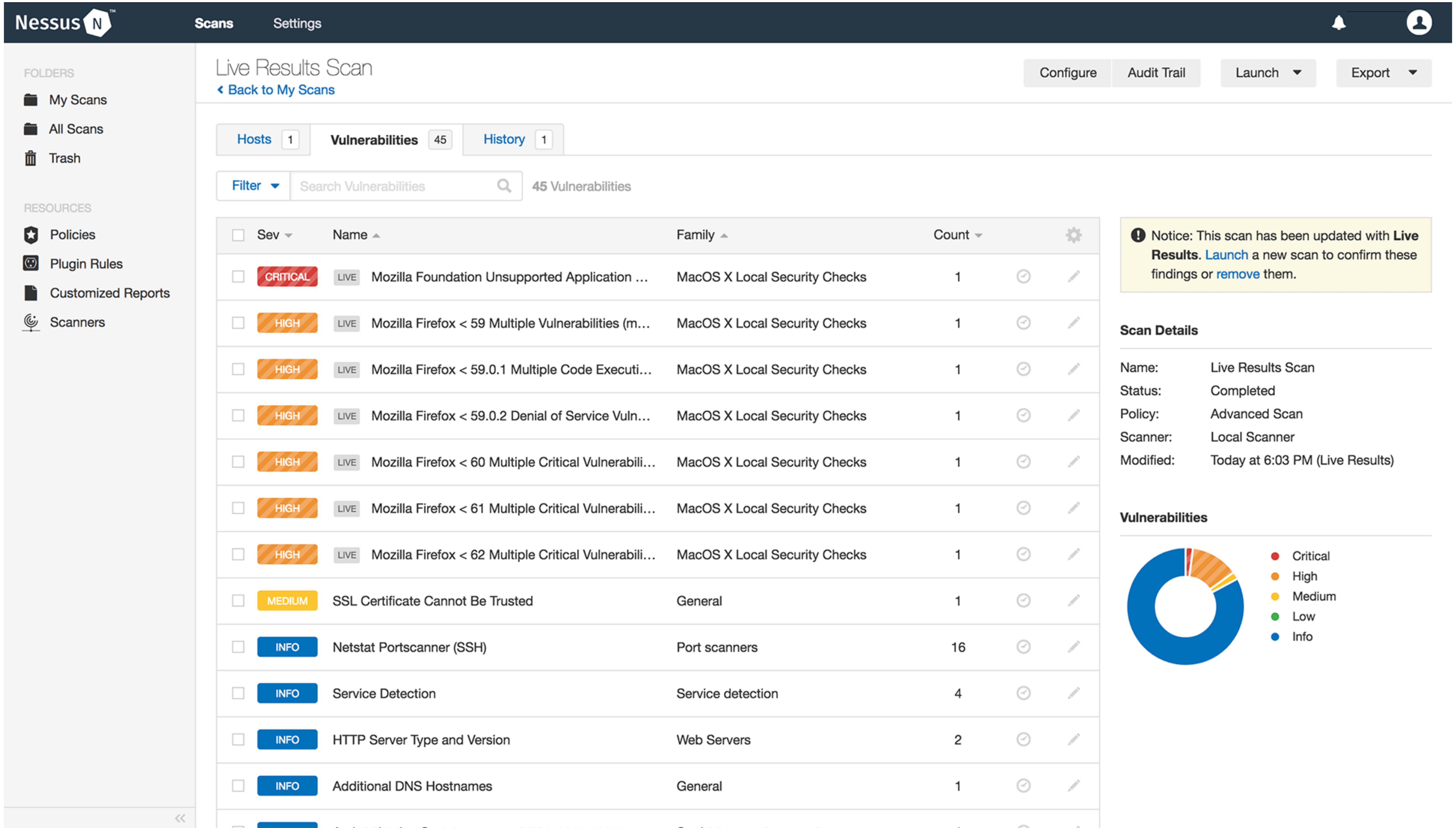
| | | STEP 7 Professional (TIA Portal) | | |
|---|---|---|---|---|
| | | V17.0 | V16.0 | V15.1 |
| **Microsoft Windows 7** | Ultimate (64-Bit) SP1 | | √ | √ |
| | Professional (64-Bit) SP1 | | √ | √ |
| | Enterprise (64-Bit) SP1 | | √ | √ |
| **Microsoft Windows 10** | Pro Version 20H2 (64-Bit) | √ | √[21] | √[22] |
| | Pro Version 2004 (64-Bit) | √ | √[23] | √[22] |
| | Pro Version 1909 (64-Bit) | √ | √[23] | √[22] |
| | Pro Version 1903 (64-Bit) | | √ | √[22] |
| | Pro Version 1809 (64-Bit) | | √ | √ |
| | Pro Version 1803 (64-Bit) | | | √ |
| | Pro Version 1709 (64-Bit) | | | √ |
| | Enterprise Version 20H2 (64-Bit) | √ | √[21] | √[22] |
| | Enterprise Version 2004 (64-Bit) | √ | √[23] | √[22] |
| | Enterprise Version 1909 (64-Bit) | √ | √[23] | √[22] |
| | Enterprise Version 1903 (64-Bit) | | √ | √[22] |
| | Enterprise Version 1809 (64-Bit) | | √ | √ |
| | Enterprise Version 1803 (64-Bit) | | | √ |
| | Enterprise Version 1709 (64-Bit) | | | √ |
| | Enterprise LTSC 2019 Version 1809 (64-Bit) | √ | √ | √ |
| | Enterprise LTSC 2016 Version 1607 (64-Bit) | √ | √ | √ |
| | Enterprise LTSC 2015 Version 1507 (64-Bit) | | √ | √ |

More info: FAQ here

SIEMENS

# Vulnerability Management

Calculate the risks of new vulnerabilities that might affect your assets



| □ | Sev | Name | Family | Count |
|---|---|---|---|---|
| □ | CRITICAL | LIVE Mozilla Foundation Unsupported Application ... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 59 Multiple Vulnerabilities (m... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 59.0.1 Multiple Code Executi... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 59.0.2 Denial of Service Vuln... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabili... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabili... | MacOS X Local Security Checks | 1 |
| □ | HIGH | LIVE Mozilla Firefox < 62 Multiple Critical Vulnerabili... | MacOS X Local Security Checks | 1 |
| □ | MEDIUM | SSL Certificate Cannot Be Trusted | General | 1 |
| □ | INFO | Netstat Portscanner (SSH) | Port scanners | 16 |
| □ | INFO | Service Detection | Service detection | 4 |
| □ | INFO | HTTP Server Type and Version | Web Servers | 2 |
| □ | INFO | Additional DNS Hostnames | General | 1 |

Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

**Scan Details**

| | |
|---|---|
| Name: | Live Results Scan |
| Status: | Completed |
| Policy: | Advanced Scan |
| Scanner: | Local Scanner |
| Modified: | Today at 6:03 PM (Live Results) |

**Vulnerabilities**

# INDUSTRIAL VULNERABILITY MNGT

## Industrial Vulnerability Manager

- Tailored for OT
- Industrial Communication Aware

### How does it work?

- Step 1: Definition of components to be monitored
- Step 2: Monitoring regarding published vulnerabilities
- Step 3: Automatic generation of digital “Security Bulletins”

## Main value drivers

Instant transparency on vulnerabilities and patches

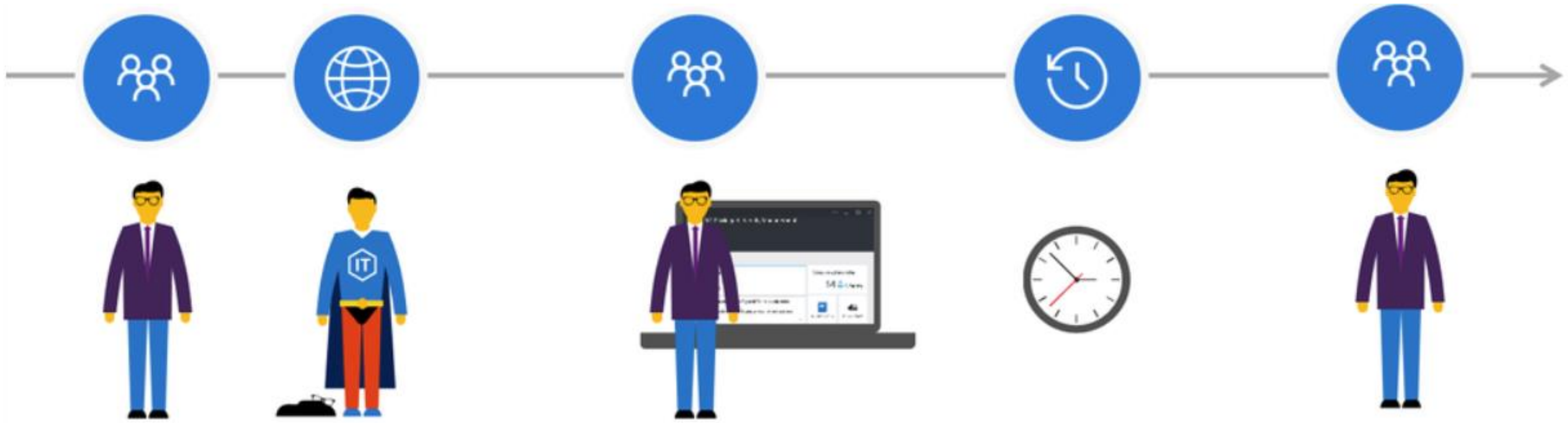
Proactive management of cyber risks

Avoid downtime and save costs

# Identity Access Control (remote)

How to secure remote access

Self-Service Privileged Identity Management (SSPIM)



### Management dashboard

A management dashboard to determine which users can have which privileges for a certain duration

### Web application

A web application, hosted in the cloud, that enables users to request escalation of their privileges

### On-premises agent

On-prem agents that follow up on escalation requests

# SINEMA Remote Connect use case
# UMC/ AD use case with server in the factory

## Task

- Secure remote maintenance for series machines and larger systems using central user and permission management

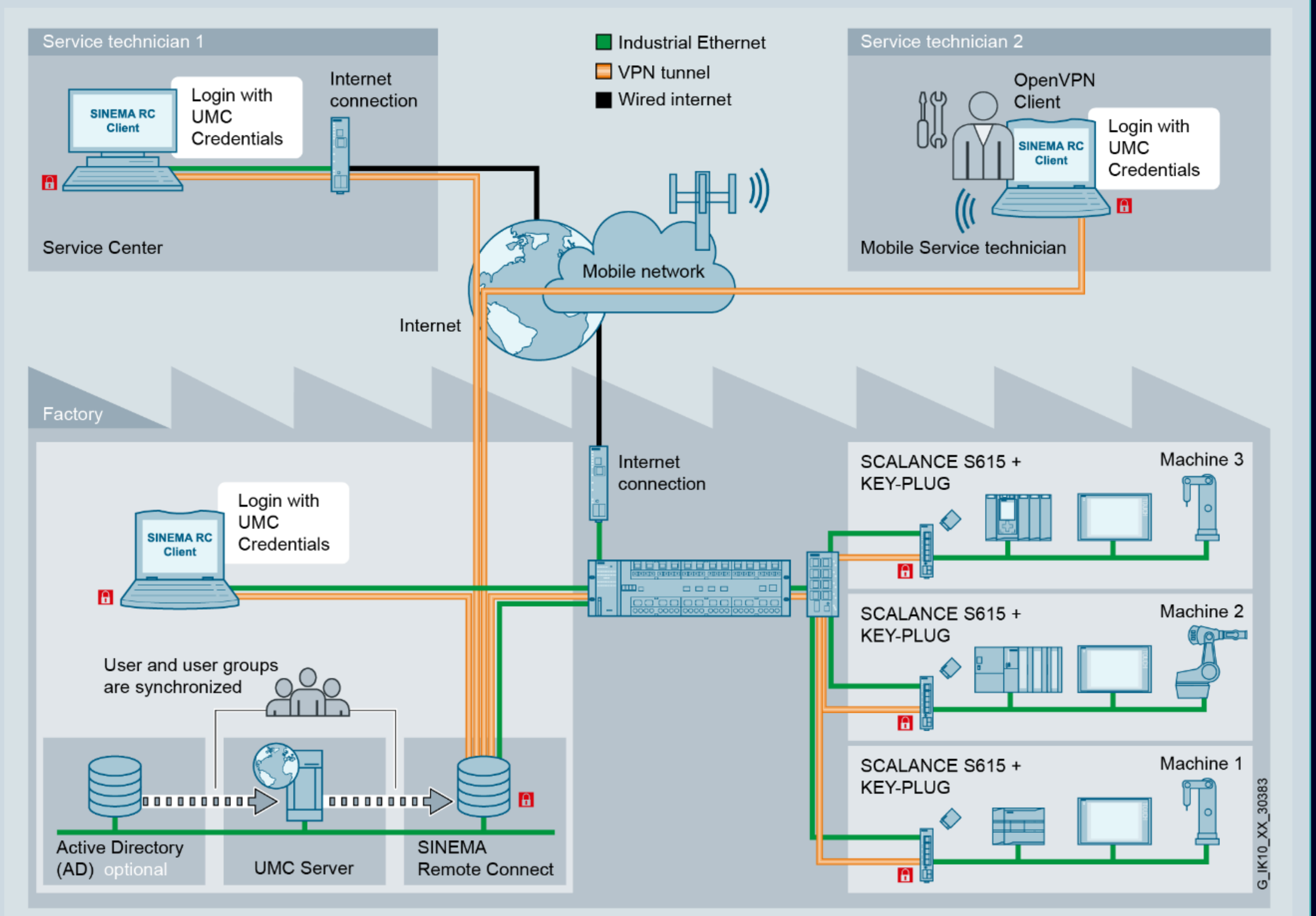
## Solution

- Uniform login with Active Directory user data on SINEMA RC server and SINEMA RC client
- Optional connection to Active Directory

## Benefits

- Central user and rights management
- Cooperation via UMC server with other systems

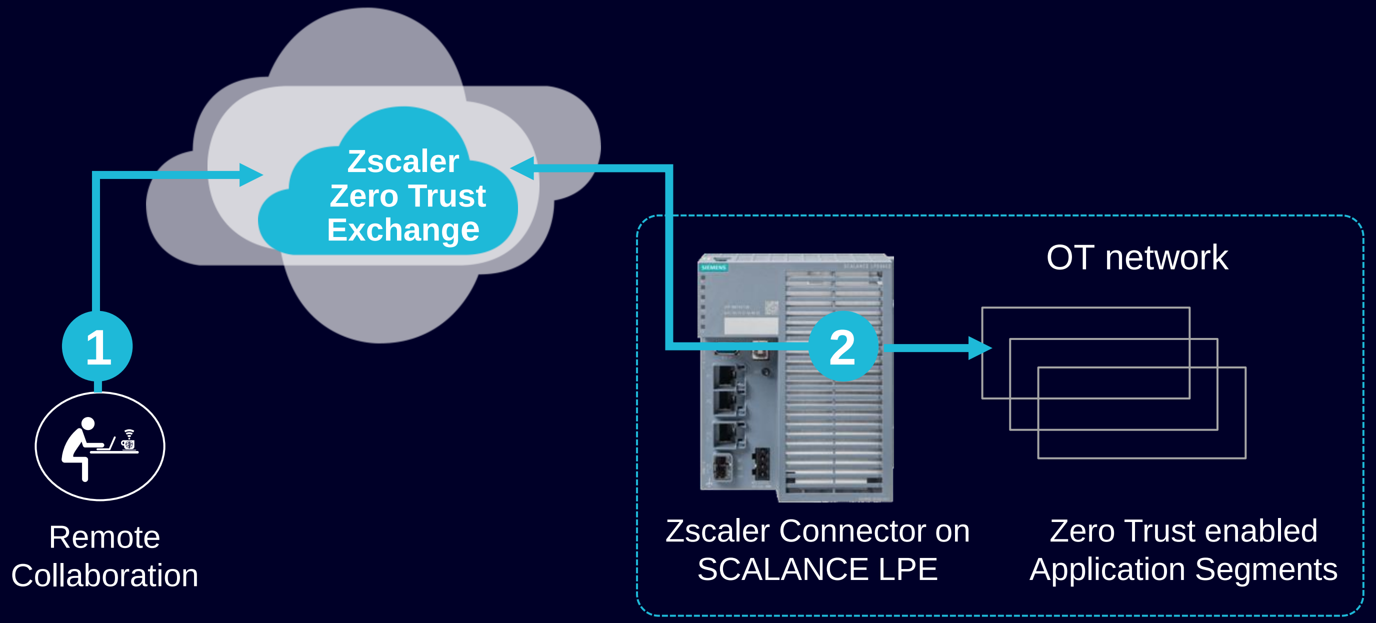
### Configuration example SINEMA Remote Connect: Remote service for special machine construction with central authentication



# Zscaler Connector running on Siemens SCALANCE LPE
# Driving the technological OT/IT convergence

**Scale up Zscaler as proven Zero Trust IT-Technology to:**

- Enable SCALANCE products to support Zscaler technology out of the box
- Leverage the approach of Siemens and Zscaler to empower existing automation networks


Zscaler
Zero Trust
Exchange
1
Remote Collaboration
2
OT network
Zscaler Connector on SCALANCE LPE
Zero Trust enabled Application Segments

**1**) Zscaler client connector

**2**) Zscaler app connector

# Security strategies & best practices

## Systems hardening

Deploy best-practice security configurations to your assets

## Backup Management

Ensure proper backups are being taken of all data containing systems

## Response Plans

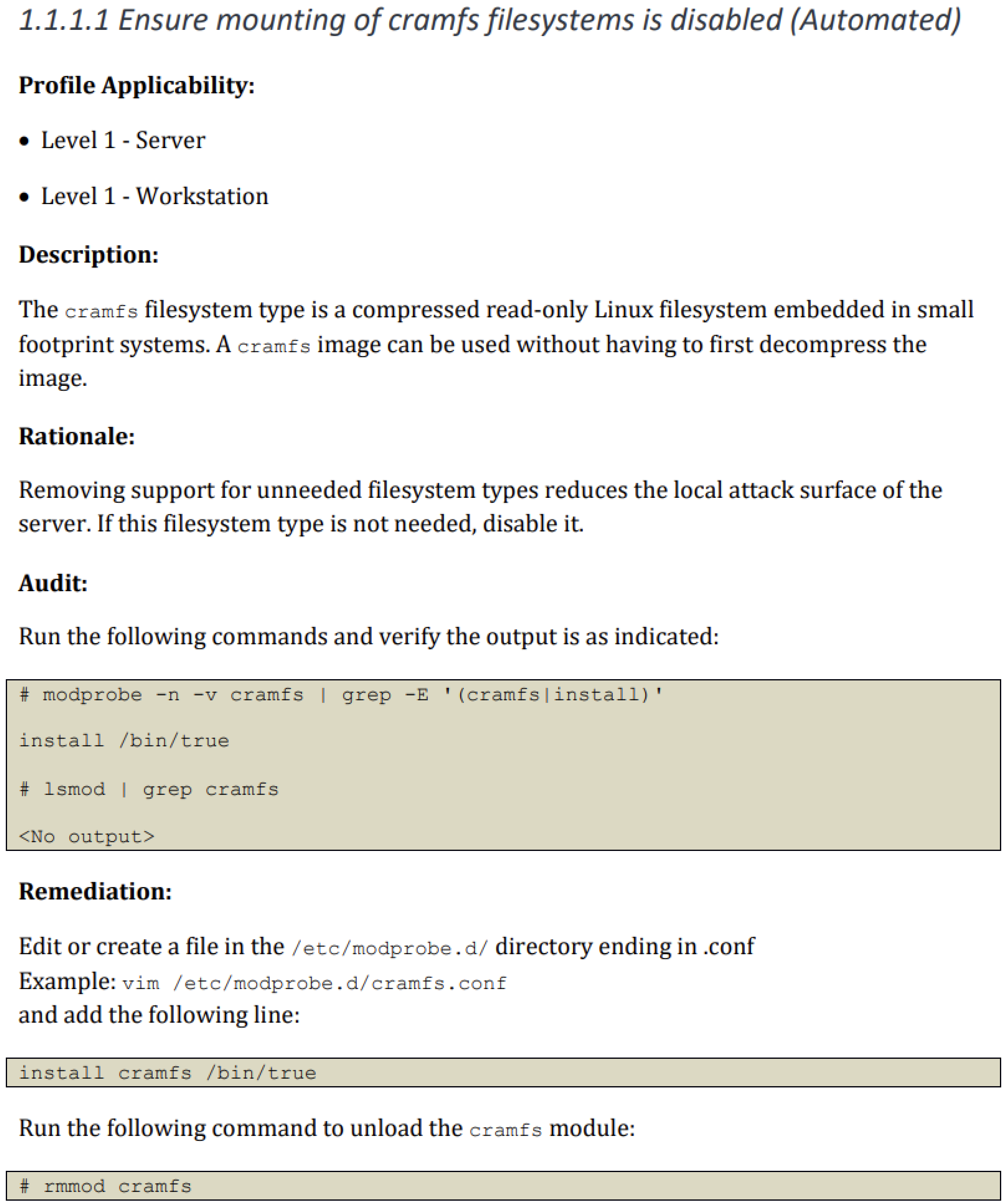
Make sure response plans are in place to quickly react in case of an incident

## Standardization

Simplify Vertical Digitalization by bottom-up standardization

# Systems hardening

Deploy best-practice security configurations to your assets



*1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

**Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

**Audit:**

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs | grep -E '(cramfs|install)'

install /bin/true

# lsmod | grep cramfs

<No output>
```

**Remediation:**

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /etc/modprobe.d/cramfs.conf`
and add the following line:

```
install cramfs /bin/true
```

Run the following command to unload the `cramfs` module:

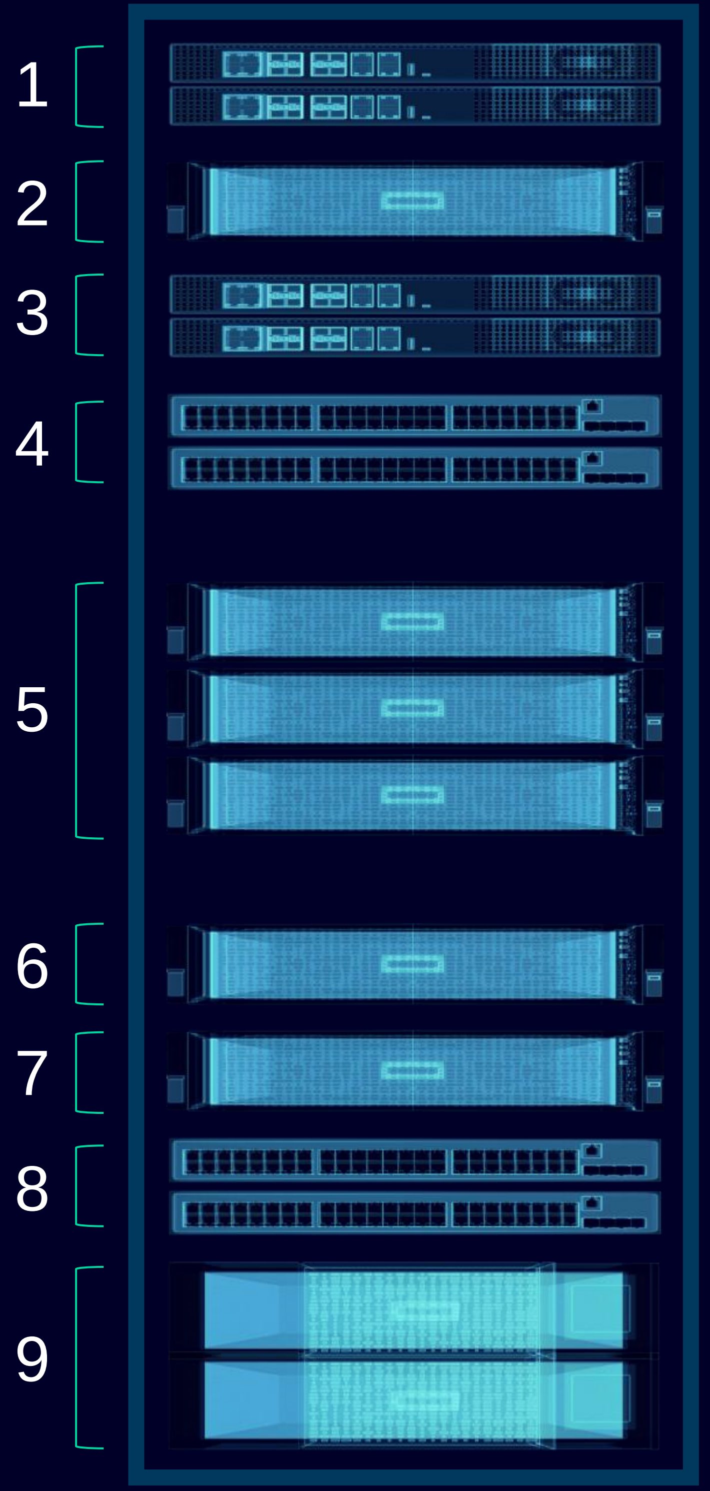
```
# rmmod cramfs
```

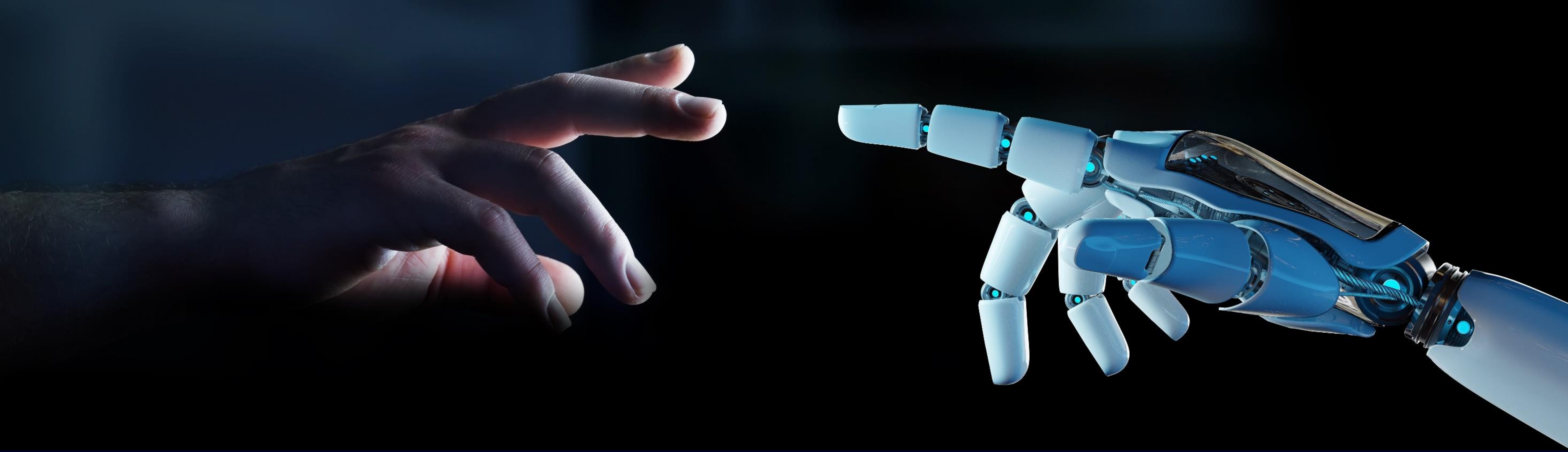
# Implementation on the hyper-convergent IT platform Industrial Automation DataCenter

## Pre-configured and pre-tested HW/SW components

1. Front Firewall
2. Industrial DMZ
3. Back Firewall
4. IT Networking
5. Computing
6. Backup & Disaster Recovery
7. Process Historian
8. OT Networking
9. Uninterruptable Power Supply

inetum. realdolmen Positive digital flow + SIEMENS

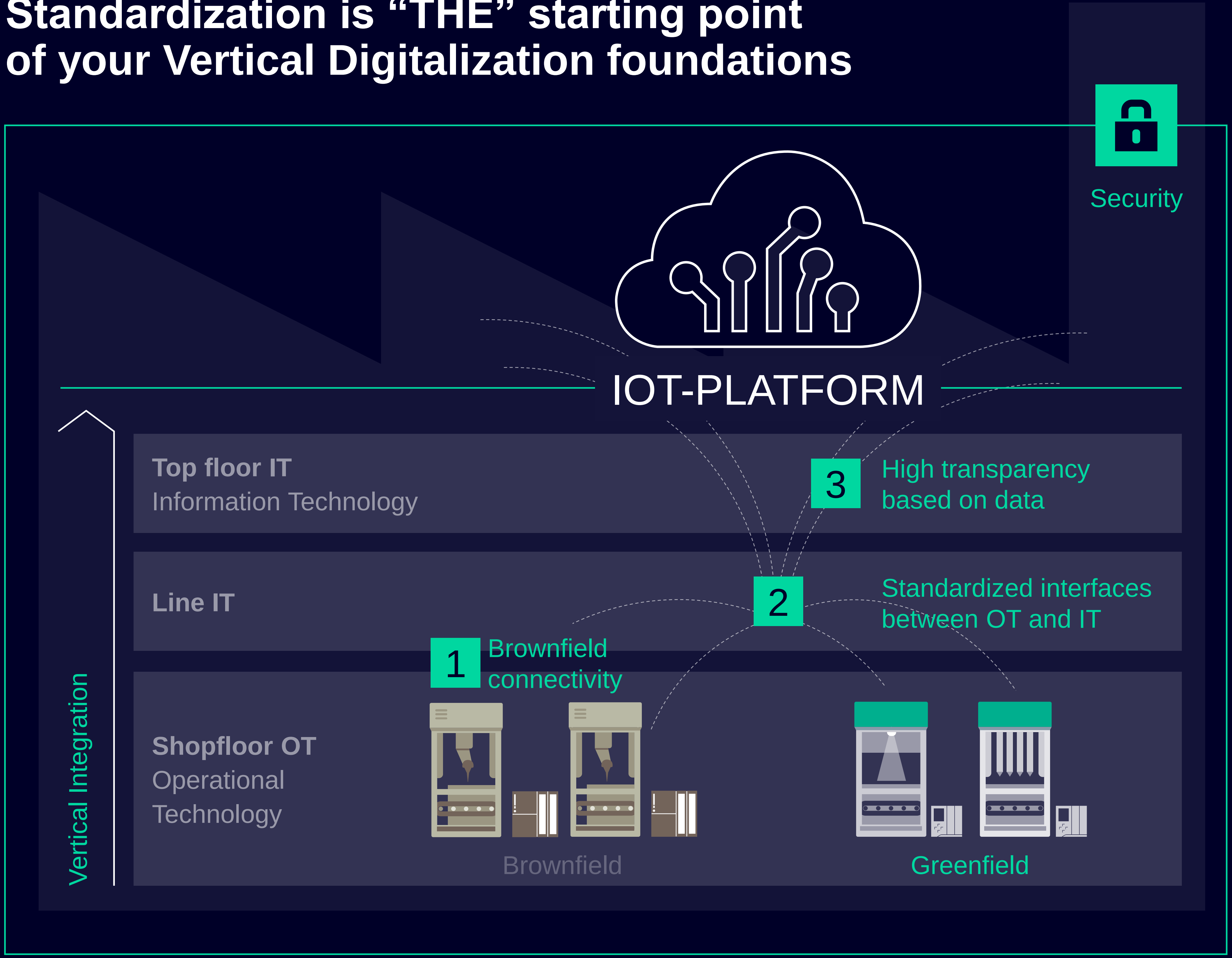




# Simplify your Digitalization use-case by starting with the right foundations

SIEMENS

# Standardization is “THE” starting point of your Vertical Digitalization foundations



Security

IOT-PLATFORM

Top floor IT
Information Technology

3 High transparency based on data

Line IT

2 Standardized interfaces between OT and IT

1 Brownfield connectivity

Shopfloor OT
Operational Technology

Brownfield

Greenfield

Vertical Integration

Increase efficiency and gain new business models based on data from all areas.

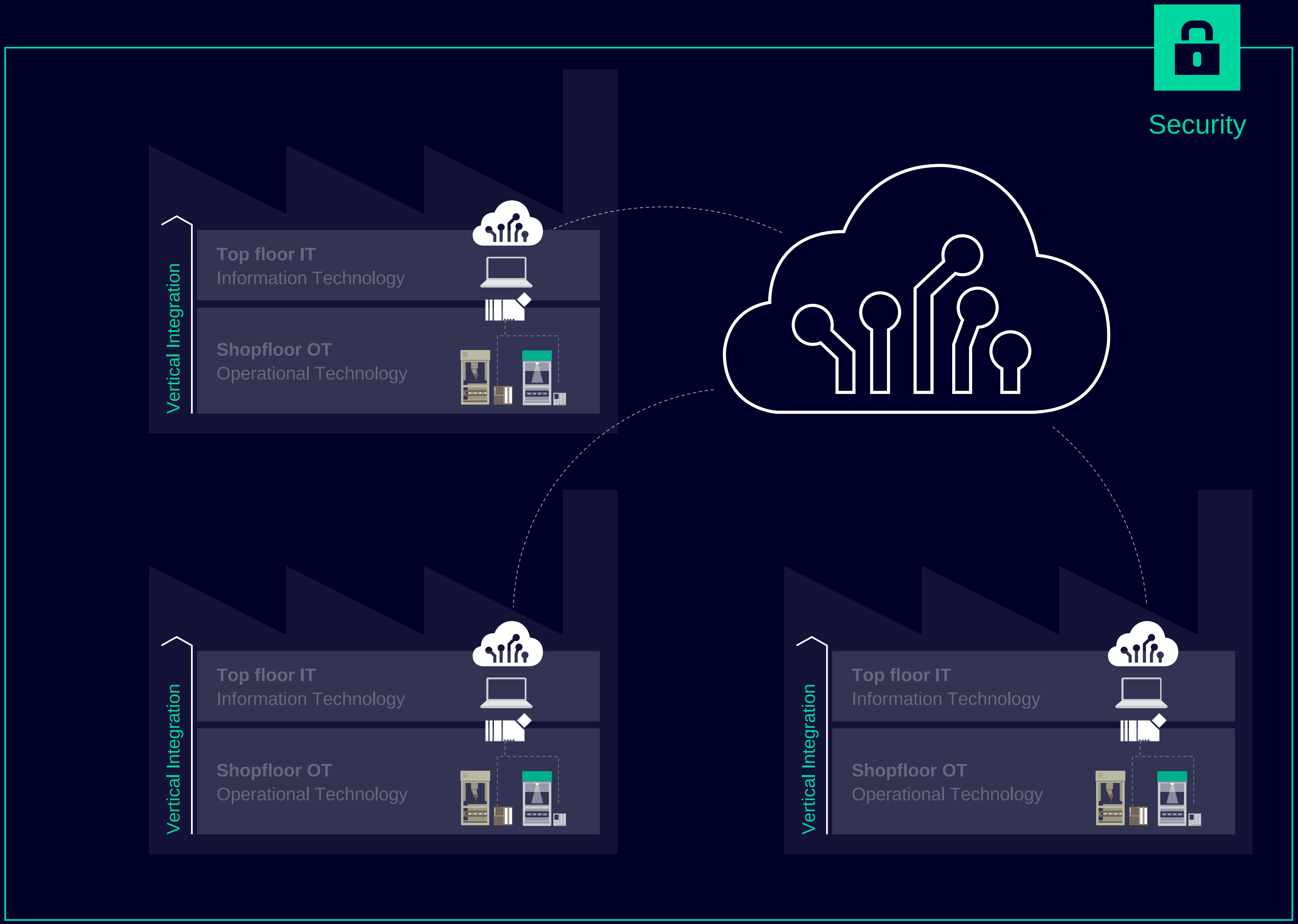
Data …

… analysis — Transparency

… communication — Connectivity

… generation — Data model

# Set the base for further open ecosystems



Build a digital enterprise for more flexibility and optimization.

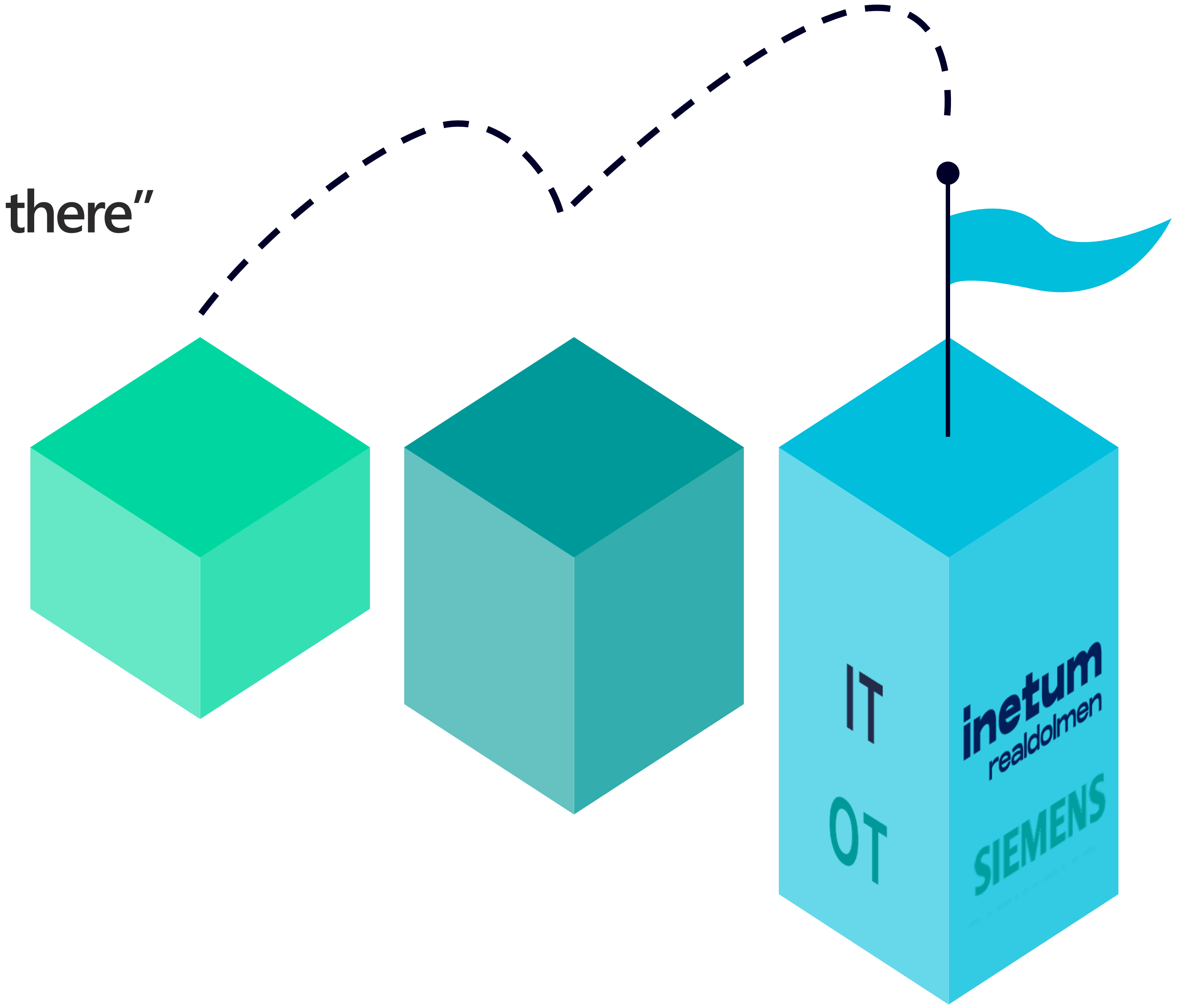
More transparency about global production facilities increases efficiency.

The standardized OT-IT concept must be integrated into every factory.

# How to get started?

Security Maturity Roadmap

"From here to there"



Roadmap outcome

# Call to action

## *Who ?*

***SPOC: Single Point Of Contact: Frederik De Naeyer***
***GSM: 0496/23.53.05***
***Email: frederik.denaeyer@inetum-realdolmen.world***

## *What ?*

***Peilen >***

- ***Behoefte ? SID, Availability, Security,…***

***Ondersteunen >***

- ***Expertise OT_IT***

## *How ?*

***Afsluiten >***

- ***Step1: Intake-meeting onsite***
- ***Step2: Quick scan, passive / Active scanning,…?***

***Doel >***

- ***Begeleidingstraject opstarten met oog op performante, stabiele, en cyber-secure omgeving***

# Combining the Best of OT and IT

SIEMENS

inetum.
realdolmen
Positive digital flow

and **get the most out of your factory** inetum

realdolmen

Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE