CINI4.0

Cybersecurity for OT :
Zero Trust Private Acces

The best way to trust is Zero Trust

cornet

Unrestricted | © Siemens 2022 | Johan Van den Eede | Digital Industries DCP

SIEMENS

Remote Access to OT with Zero Trust concept
Close collaboration between OT and IT

> ***„…we would like to find a better and easier way for our department to perform machine maintenance…"*** *)

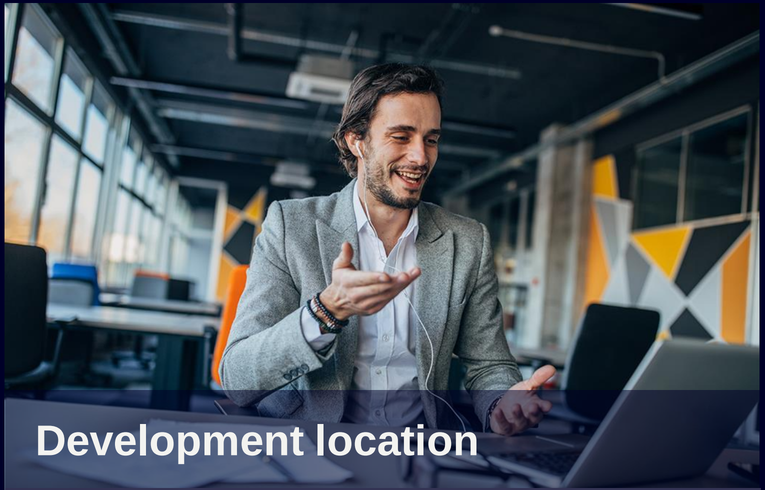
- Allow dedicated employees continuously remote access to restricted areas (e.g. manufacturing areas, restricted OT areas like labs)
- The connection is limited to the concerned machine network / restricted area and complies with cybersecurity rules
- Overcoming the hurdle's of classical VPN Remote Connections in combination with reduced operational efforts

> ***„…Zero Trust improves flexibility, agility and scalability, enabling digital ecosystems to work without exposing services directly to the internet, reducing risks of distributed denial of service attacks"***

- By 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed via Zero Trust
- By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of Zero Trust

*) Source: Gartner, Zero Trust Architecture and Solutions, published by Qi An Xin Group, 2020

Zero Trust for all industries - discrete and process industry
Mobile working - Areas of application

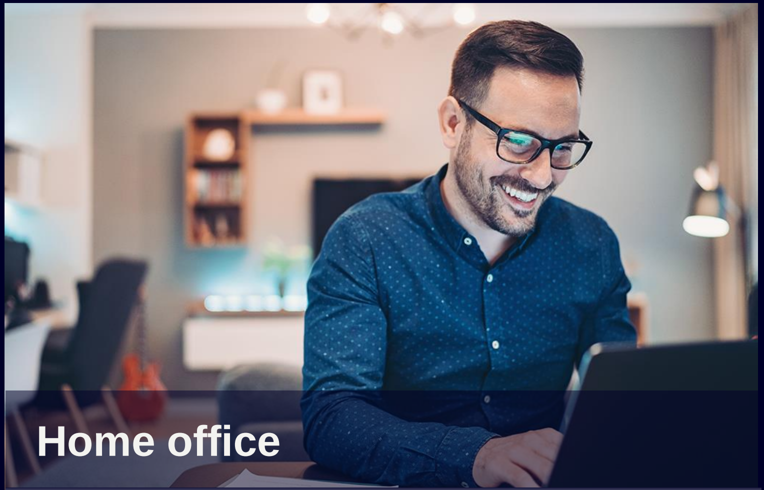


Development location

Development or test environments are crucial for production areas. Before adding new products to the actual manufacturing process intensive tests are carried out. The possibility to security access those areas from any location provides flexibility as well as comfort.

Production areas

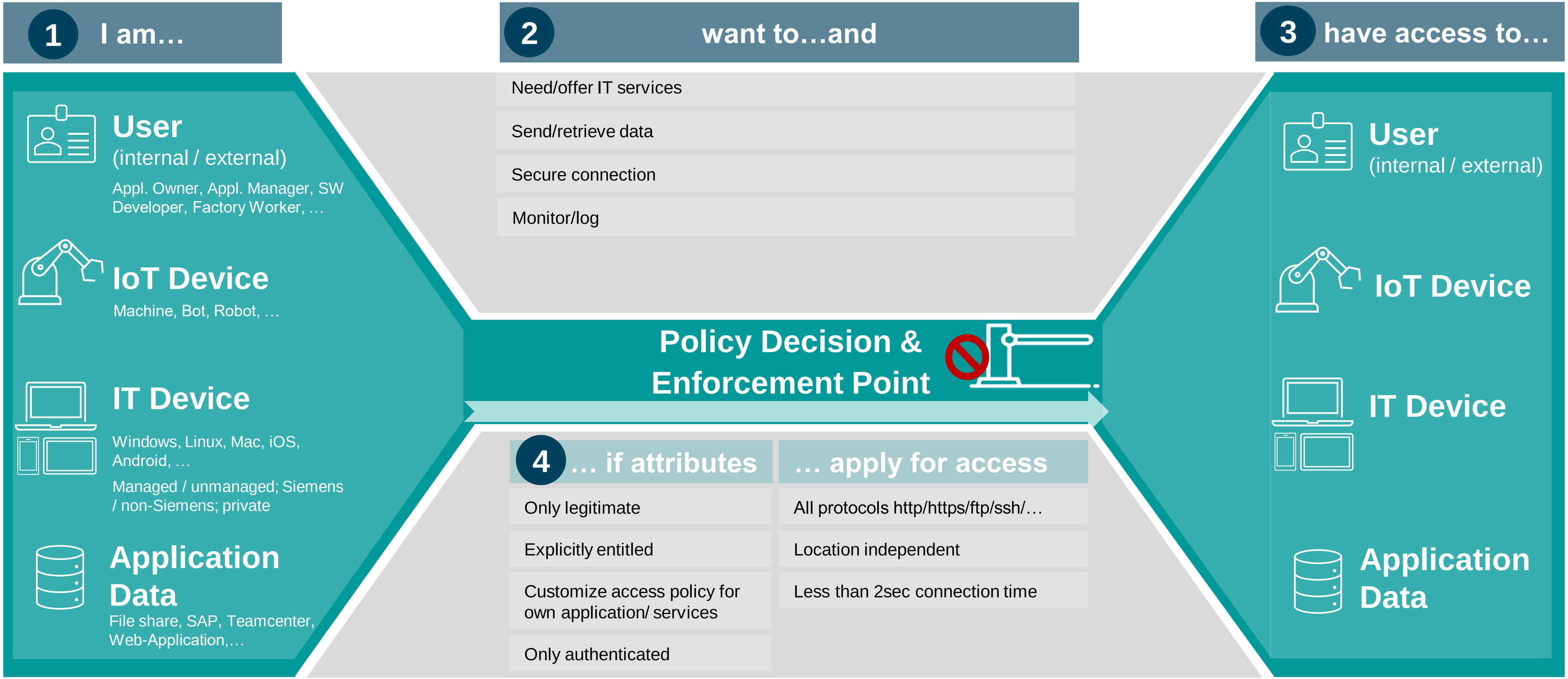
Constant availability is a top priority for production networks. Response times in the range of milliseconds, legacy devices with long product lifecycles as well as strict safety requirements make production areas the ideal location to place remote collaboration with corresponding zero trust principles.



Home office

Mobile working from home, from inland or abroad becomes reality for many employees – at least for those employed in office. Remote collaboration with zero trust enables workers employed in production environments to securely carry out quality management or other assistance tasks from anywhere.

Controlled communication between users, devices and applications
Generic architecture of a future Zero Trust approach adopted from IT



1 I am…

User (internal / external)
Appl. Owner, Appl. Manager, SW Developer, Factory Worker, …

IoT Device
Machine, Bot, Robot, …

IT Device
Windows, Linux, Mac, iOS, Android, …
Managed / unmanaged; Siemens / non-Siemens; private

Application Data
File share, SAP, Teamcenter, Web-Application,…

2 want to…and

- Need/offer IT services
- Send/retrieve data
- Secure connection
- Monitor/log

Policy Decision & Enforcement Point

3 have access to…

User (internal / external)

IoT Device

IT Device

Application Data

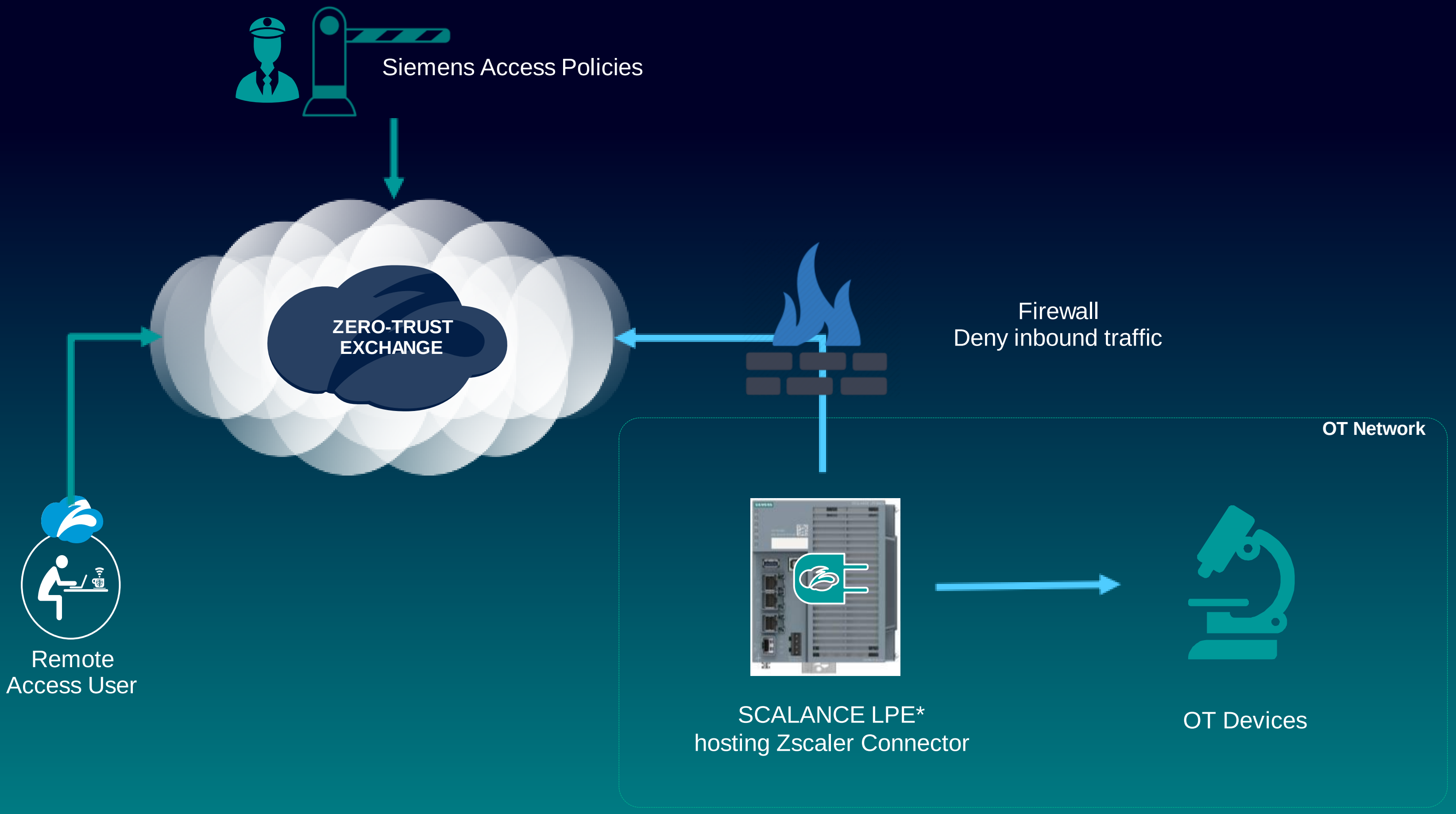
4 … if attributes	… apply for access
Only legitimate	All protocols http/https/ftp/ssh/…
Explicitly entitled	Location independent
Customize access policy for own application/ services	Less than 2sec connection time
Only authenticated	

Zero Trust Private Access of Zscaler

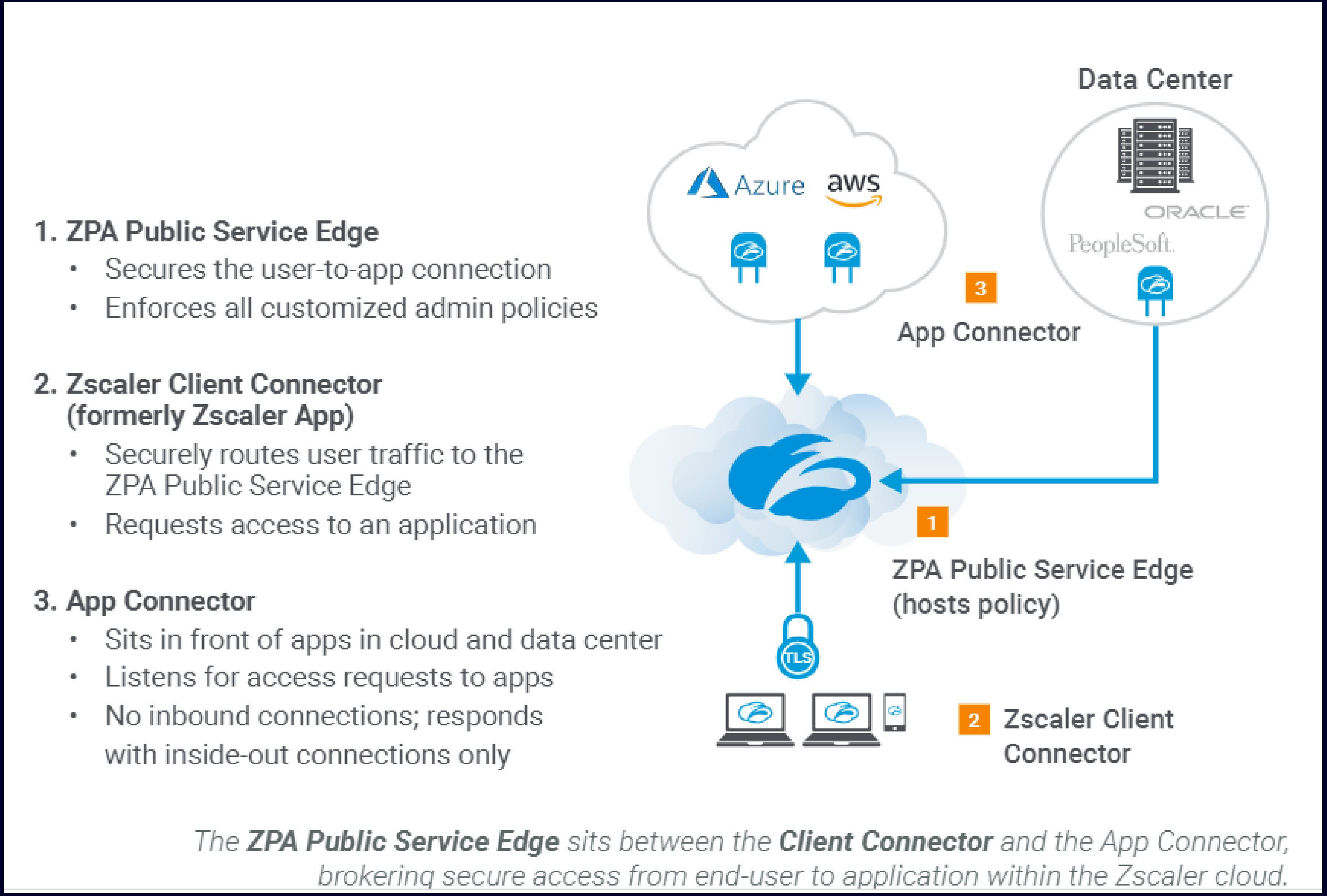
LPE – Zscaler at Siemens Factory

SIEMENS

LPE Zscaler Use Case –
Access for Siemens employee’s to ….



Zero Trust Private Acces Exchange



1. **ZPA Public Service Edge**
   - Secures the user-to-app connection
   - Enforces all customized admin policies

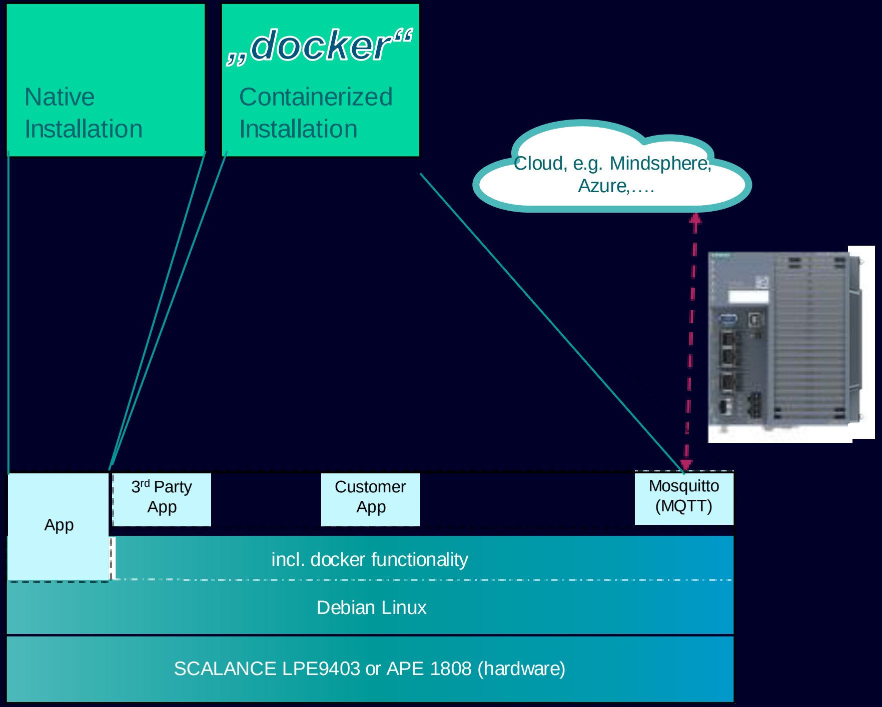
2. **Zscaler Client Connector (formerly Zscaler App)**
   - Securely routes user traffic to the ZPA Public Service Edge
   - Requests access to an application

3. **App Connector**
   - Sits in front of apps in cloud and data center
   - Listens for access requests to apps
   - No inbound connections; responds with inside-out connections only

*The **ZPA Public Service Edge** sits between the **Client Connector** and the App Connector, brokering secure access from end-user to application within the Zscaler cloud.*

SCALANCE LPE9403
For which Software packages is the LPE9403 suitable?

Software Installation	Native	Containerized
System requirement	• Debian Linux • ARM64 support + additional Linux packs	• Debian Linux • ARM64 support
Pros / Cons	- Dependency between Software & OS	+ Easy to install & maintain + No critical dependencies
Result	More effort	Recommended
Examples	- own app development (nodered) - IDS (eg Claroty) - Wireshark	- own app development (nodered) - IDS (eg Claroty) - Wireshark

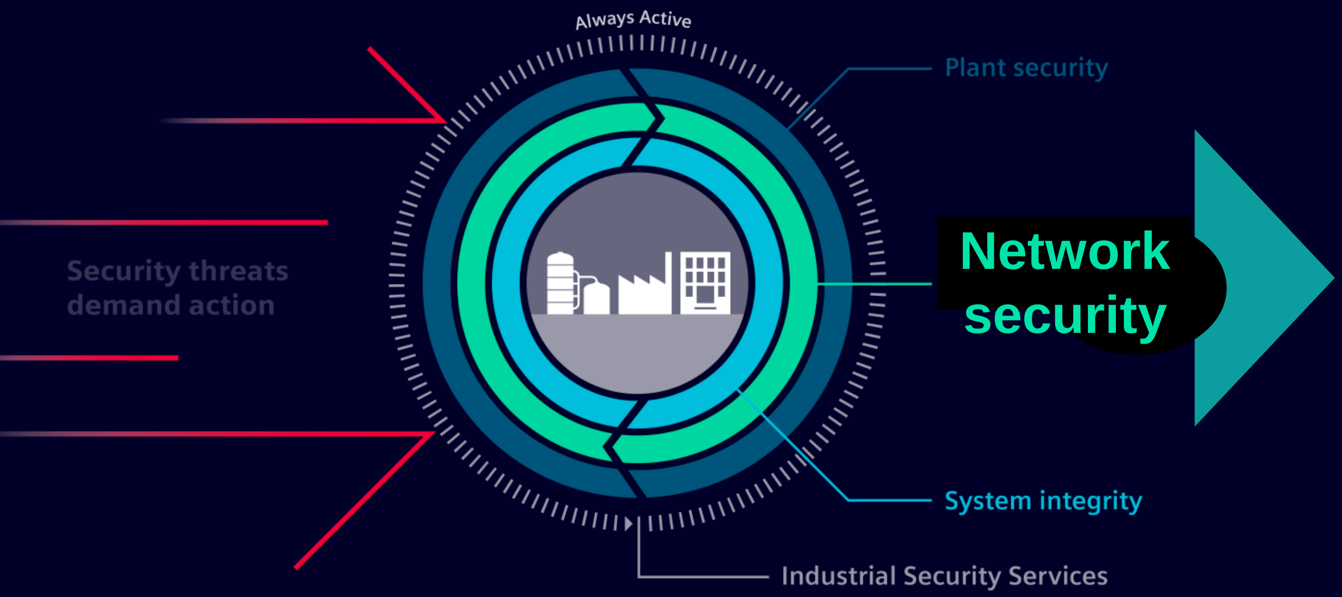

Native Installation
„docker“
Containerized Installation
Cloud, e.g. Mindsphere, Azure,….
App
3rd Party App
Customer App
Mosquitto (MQTT)
incl. docker functionality
Debian Linux
SCALANCE LPE9403 or APE 1808 (hardware)

SIEMENS

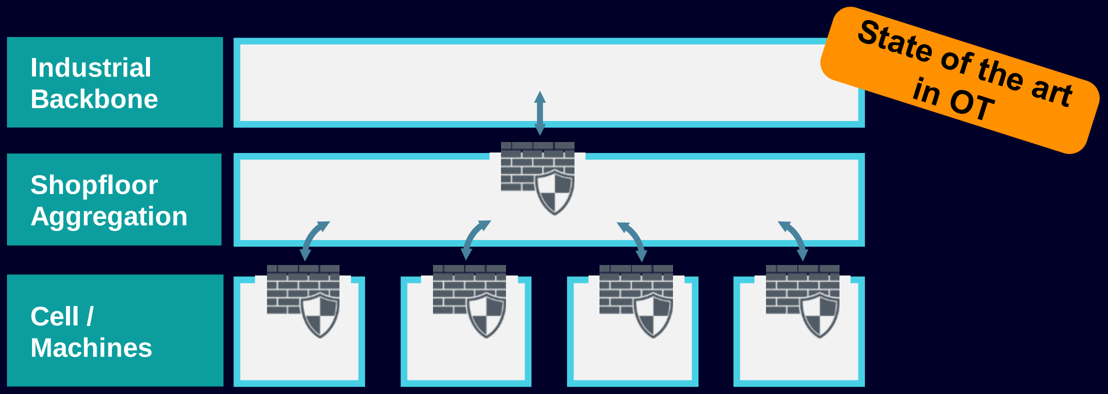
Supplementing Zero Trust
Combining Zero Trust and perimeter protection principles

Defense in depth …

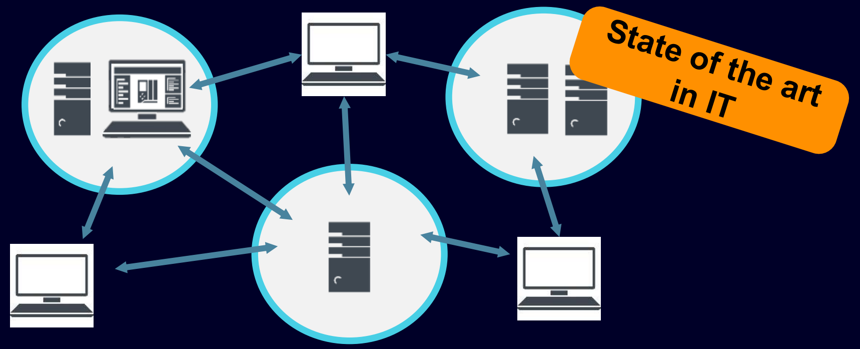
… remains state of the art,



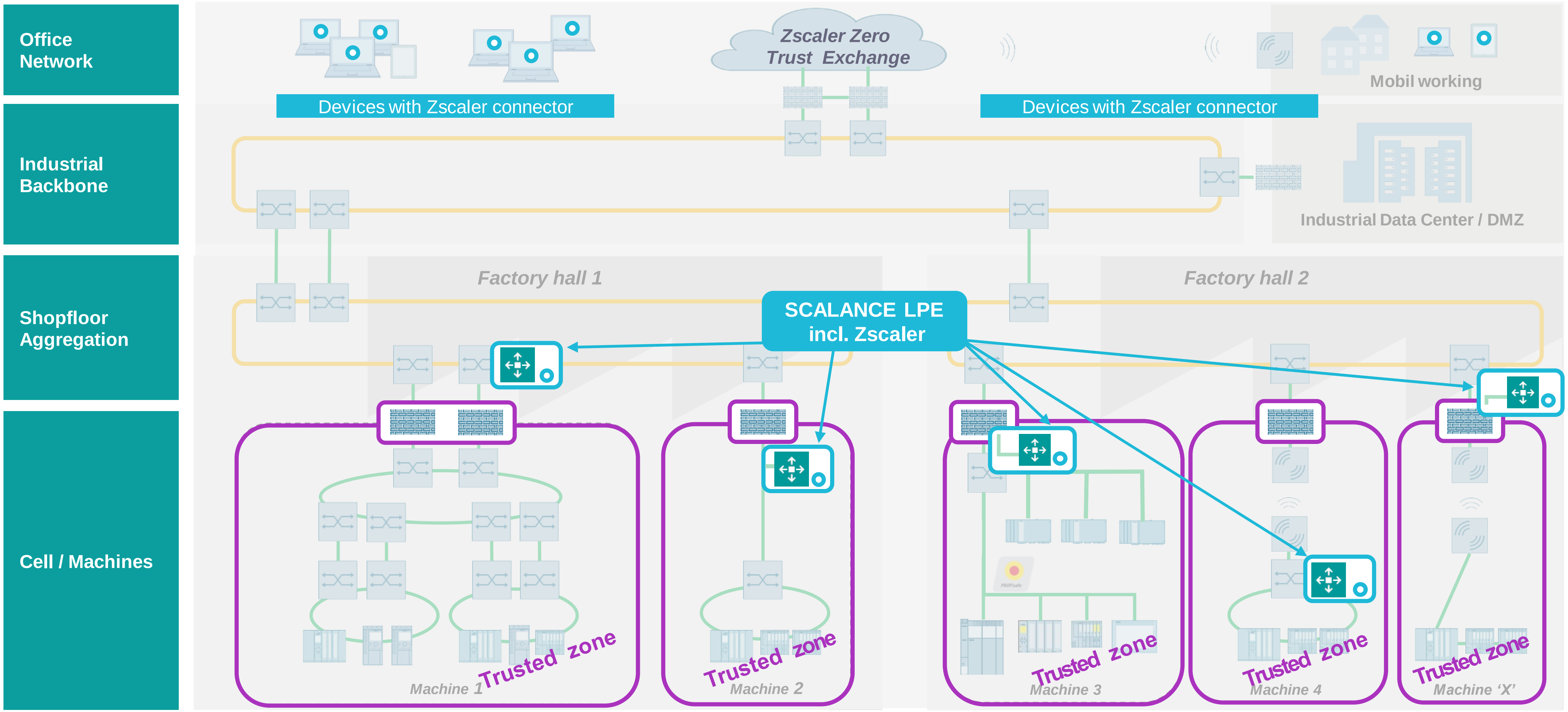
but classical cell protection



will be enriched by zero trust principles



Enabling Zero Trust principles in automation environments for remote access
Combining Zero Trust and perimeter-based defense



M2M communication not in focus at the moment

SIEMENS

Access and identification

Task

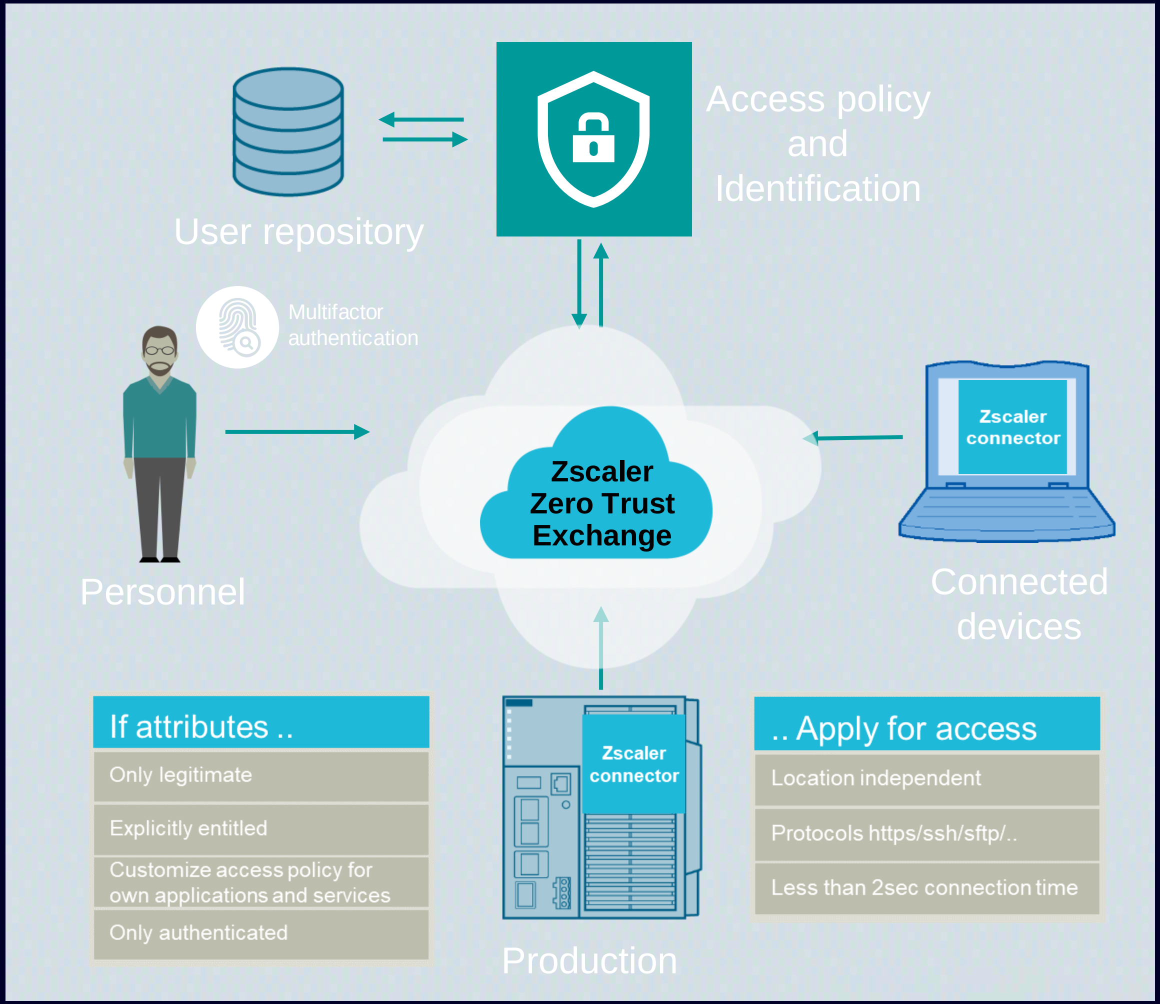
Identify and control access based on policies.

Solution

Zscaler Zero Trust Exchange checks connecting device information and credentials with company authority servers. Access is determined with up to date policies and authorizations.

Benefits

- Connecting entities are always checked against latest policies and authorizations
- Policy updates are rolled out instantly
- Connections and access are identified and logged
- Very granular access based on application layer.



User repository
Access policy and Identification
Multifactor authentication
Personnel
Zscaler Zero Trust Exchange
Zscaler connector
Connected devices
Zscaler connector
Production

If attributes ..
- Only legitimate
- Explicitly entitled
- Customize access policy for own applications and services
- Only authenticated

.. Apply for access
- Location independent
- Protocols https/ssh/sftp/..
- Less than 2sec connection time

M2M communication not in focus at the moment

Location independent access

Task

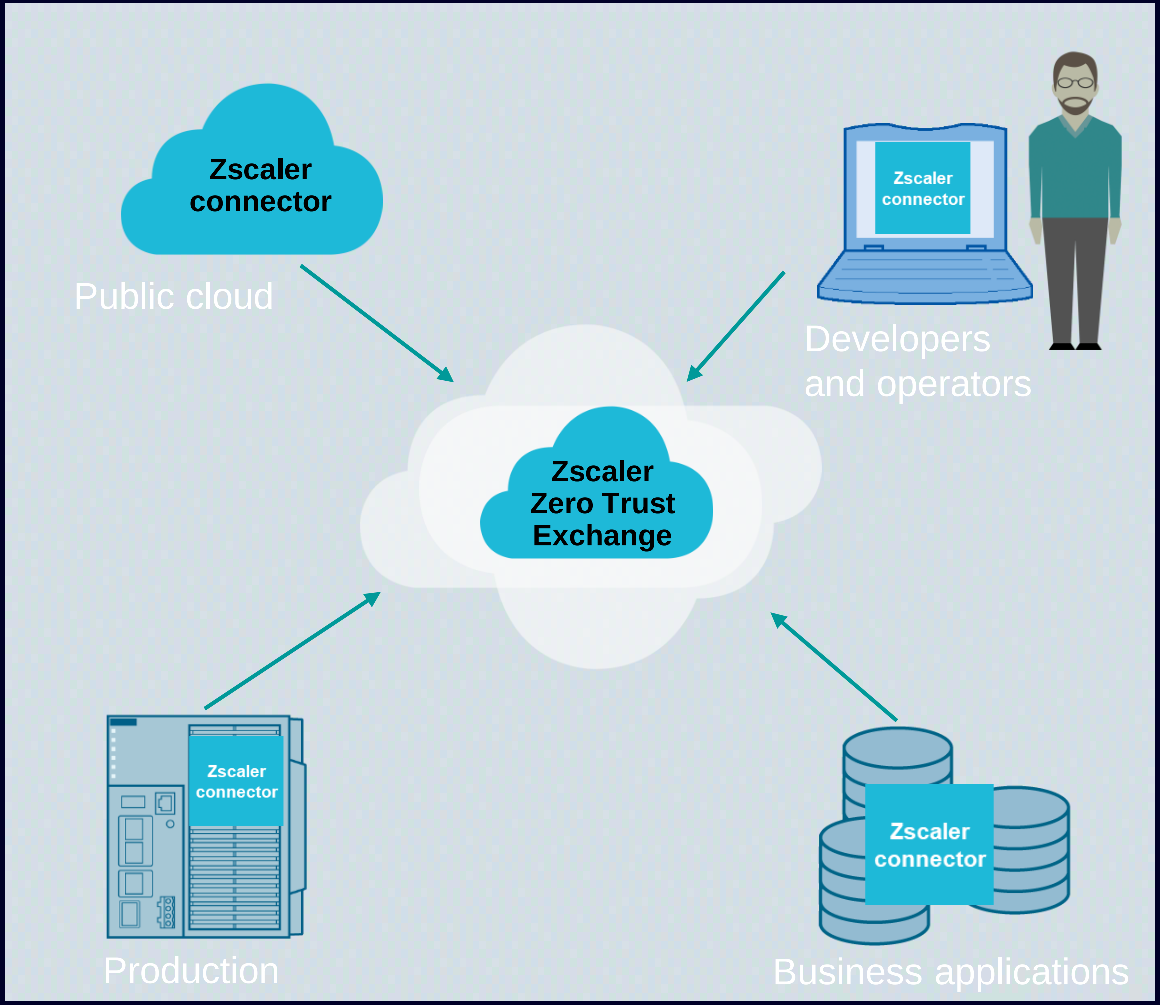
Provide access to IIoT ecosystems and specific resources for application development and operation personnel.

Solution

Zscaler provides authorized connectivity for developers and operators to access required tools and resources independent of location.
Every connection is treated as untrusted and continuously evaluated.

Benefits

- Connectivity between platforms and users
- One access concept to office and production locations
- Zscaler's cloud platform determines the best path between connections



M2M communication not in focus at the moment

SIEMENS

Thank You

CINI4.0

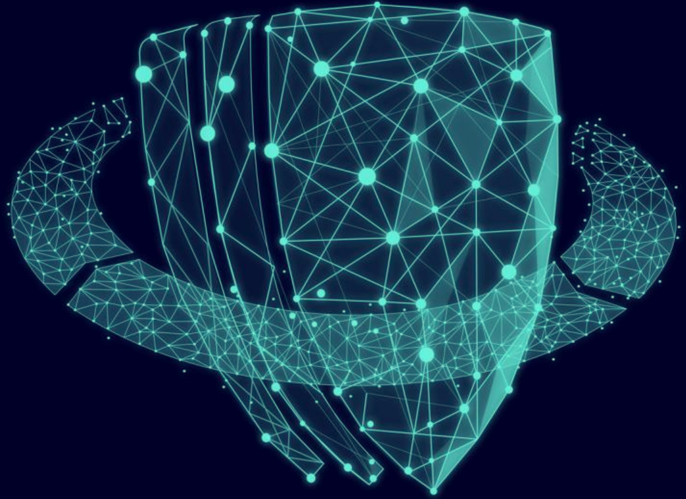
cornet

Contact

Published by Siemens NV/SA

Johan Van den Eede
Sales Specialist Industrial Communication & Security
Digital Industries - DCP
Guido Gezellestraat 123
1654 Huizingen
Belgium
Mobile +32470615281

E-mail johan.van_den_eede@siemens.com



SIEMENS