
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Zero Trust Security and the Industrial IoT

Jason Greengrass
Business Solutions Architect – Industry Solutions Group
PSOIND-2000

Agenda

- Industrial Security overview
- Zero Trust overview
- NIST Zero Trust Architecture
- Cisco Zero Trust
- Zero Trust for Industrial IoT

Industrial Security overview

cisco Live!

Ransomware attacks are now targeting industrial control systems

Ekans ransomware is designed to target industrial systems in what researchers describe as a "deeply concerning evolution" in malware.

Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk

Major German manufacturer still down a week after getting hit by ransomware

Pilz, a German company making automation tool, was infected with the BitPaymer ransomware on October 13.

By Catalin Cimpanu for Zero Day | October 21, 2019 -- 19:15 GMT (12:15 PDT) | Topic: Security

The Malware Used Against The Ukrainian Power Grid Is More Dangerous Than Anyone Thought

Researchers have discovered a new powerful – and dangerous – malware that targets industrial control systems.

ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

Mysterious New Ransomware Targets Industrial Control Systems

EKANS appears to be the work of cybercriminals, rather than nation-state hackers—a worrying development, if so.

26 Sep 2019

Ad-hoc: Rheinmetall AG: Regional disruption of production due to malware at Rheinmetall Automotive

5/20/2019 09:30 AM

Kelly Jackson Higgins

How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

The infamous Ryuk ransomware slammed a small company that makes heavy-duty vehicle alternators for government and emergency fleet. Here's what happened.

19 MAR 2020 NEWS

Norsk Hydro Outage May Have Been Destructive State Attack

Nextgov CYBERSECURITY EMERGING TEC

TRENDING // CLOUD // QUANTUM COMPUTING // ELECTION SEC

Shipping giant Pitney Bowes hit by ransomware

Zack Whittaker @zackwhittaker / 9:29 am PDT • October 14, 2019

Cybersecurity Firm Flags Novel Ransomware Aimed at Industrial Control Systems

Manufacturing giant Aebi Schmidt hit by ransomware

Zack Whittaker @zackwhittaker / 2:04 pm PDT • April 23, 2019 Comment

Bloomberg

Ransomware Linked to Iran, Targets Industrial Controls

See article on: www.bloomberg.com Gwen Ackerman 1/29/2020

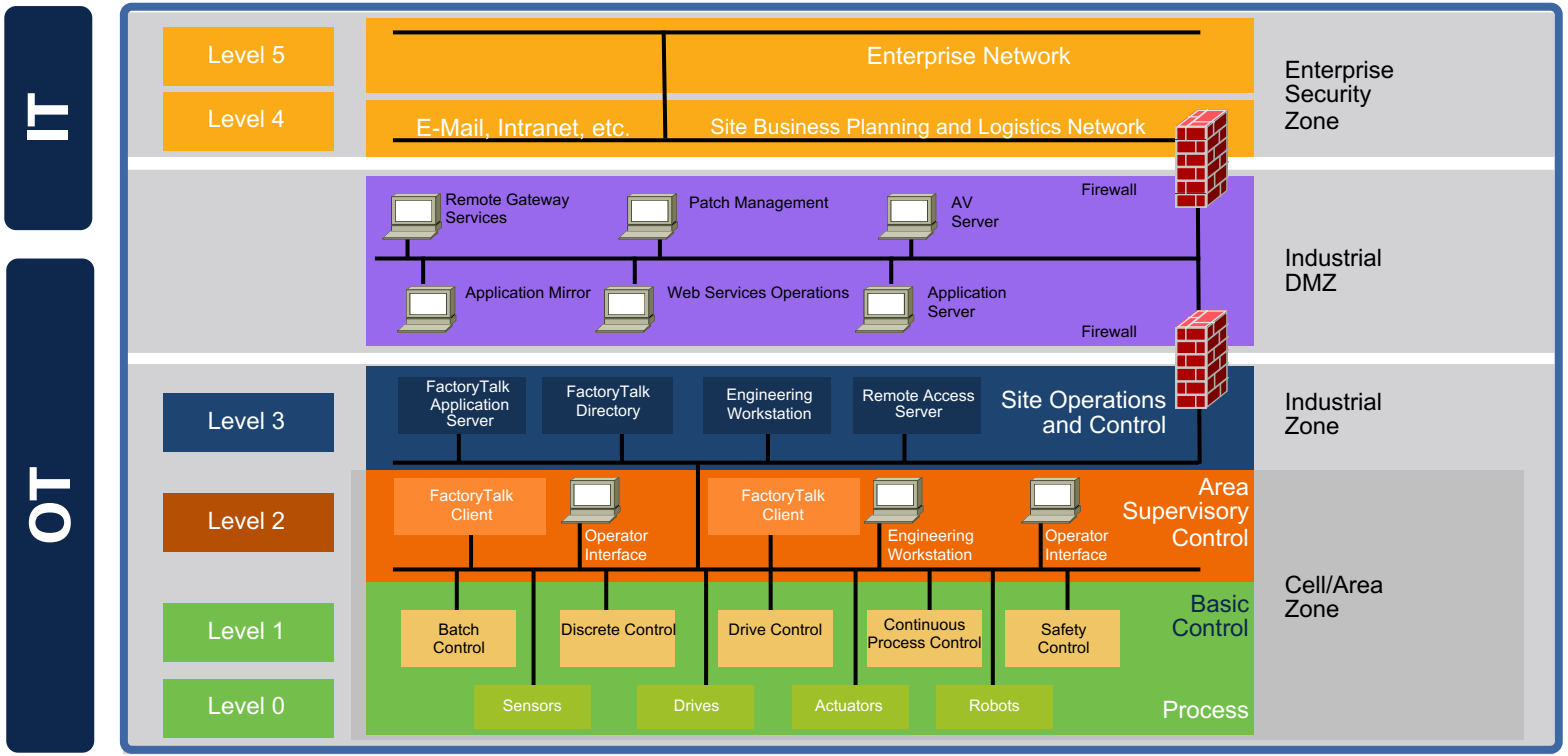
Ransomware halts production for days at major airplane parts manufacturer

Nearly 1,000 employees sent home for the entire week, on paid leave.

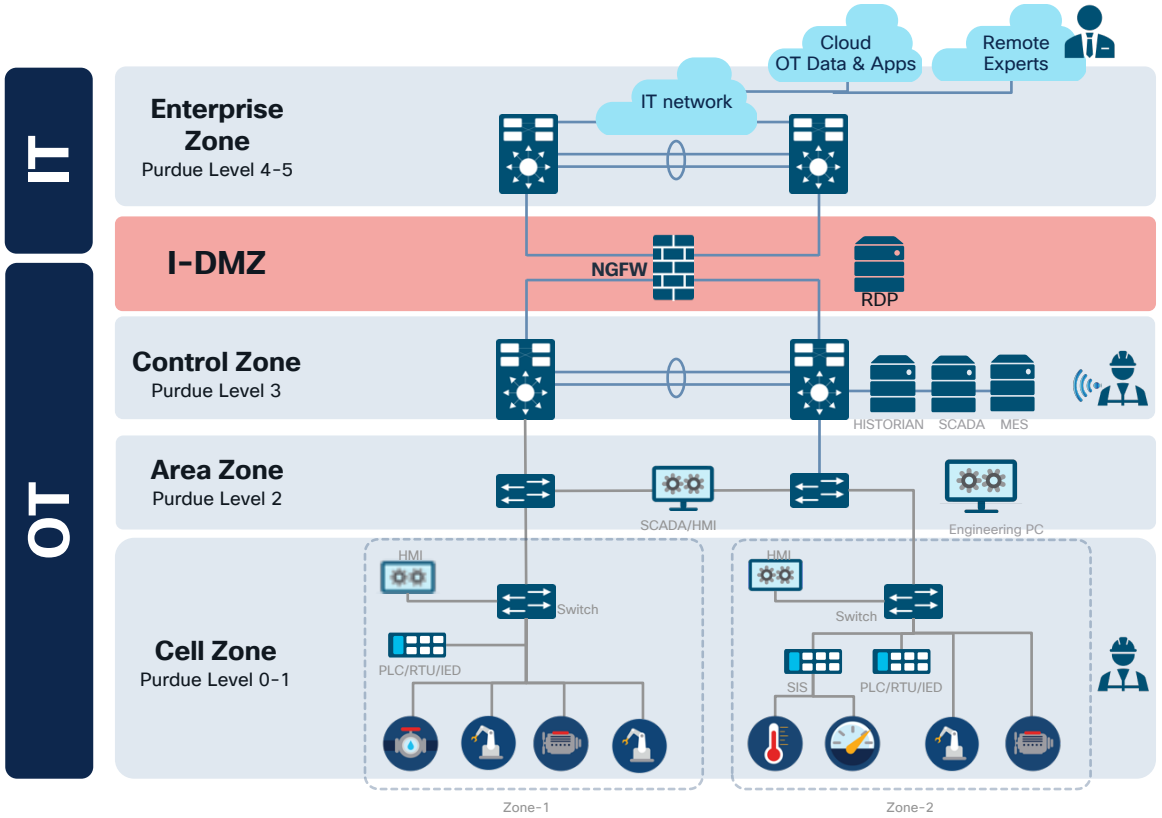
By Catalin Cimpanu for Zero Day | June 12, 2019 -- 19:27 GMT (12:27 PDT) | Topic: Security

Built on Industry Standards

Purdue/IE62443 Reference Model



Classic Industrial Model



Segment OT and IT with an Industrial DMZ

Controlled access to OT and flow of data between OT/IT

Further Segmentation of networks and production Cells

Assumed Trust not enough

Industrial Threats and Vulnerabilities

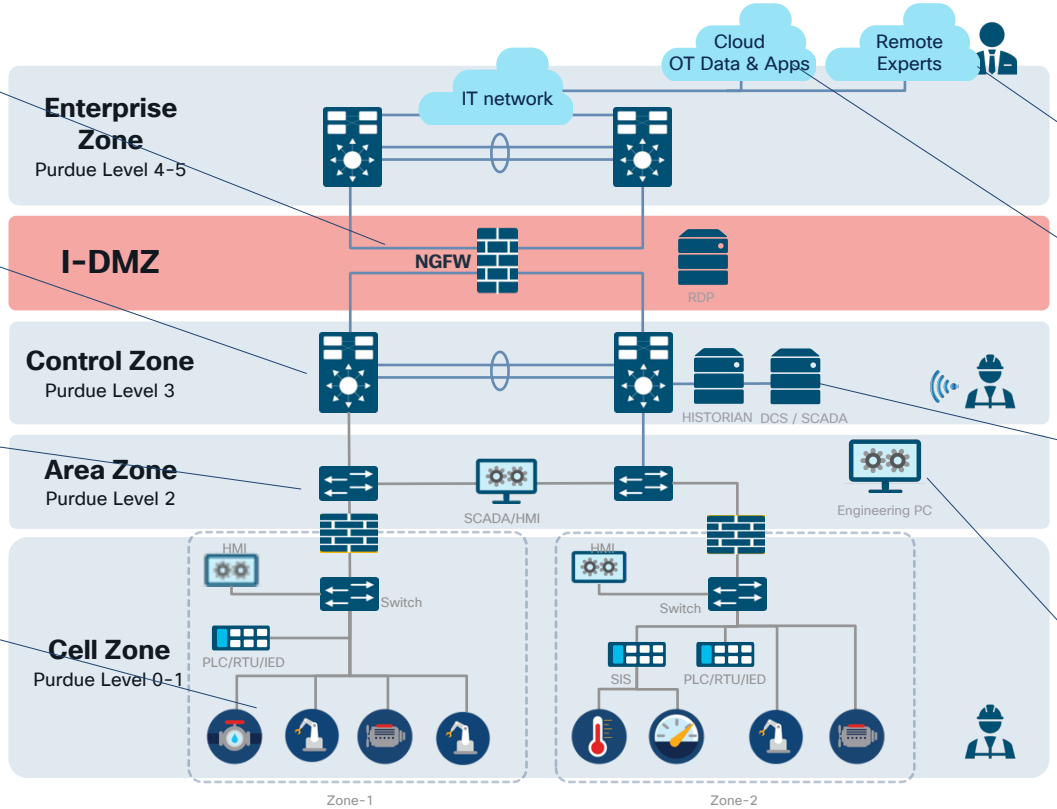
Insufficient segmentation between Enterprise and Operations, with increased exchange of data.

Limited visibility into baselines for normal operations slows time to detect cyber incidents.

OT network architecture unable to contain or control lateral movement of threats.

Limited visibility into OT assets and vulnerabilities.

ICS-specific targeted attacks increasing.



Increased requirements for remote access for system monitoring, troubleshooting and control.

OT data and applications moving to cloud and SaaS environments.

Growing set of plant-wide applications using commodity hardware and operating systems.

Exposure to malware and ransomware for Windows platforms in OT

Zero Trust overview

A Little Bit of Zero Trust History

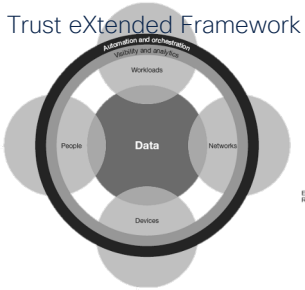
2004
Jericho Forum
"De-Perimeterization"

2009
FORRESTER®
Coins the term
"Zero Trust"

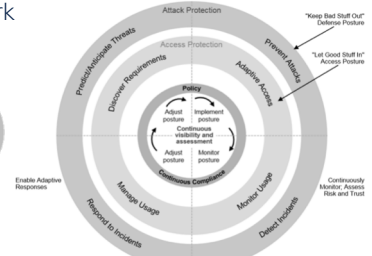
2014
Google publishes
"BeyondCorp"

2015
Technology vendors
begin to multiply

2017
FORRESTER®
Zero Trust eXtended Framework



Gartner

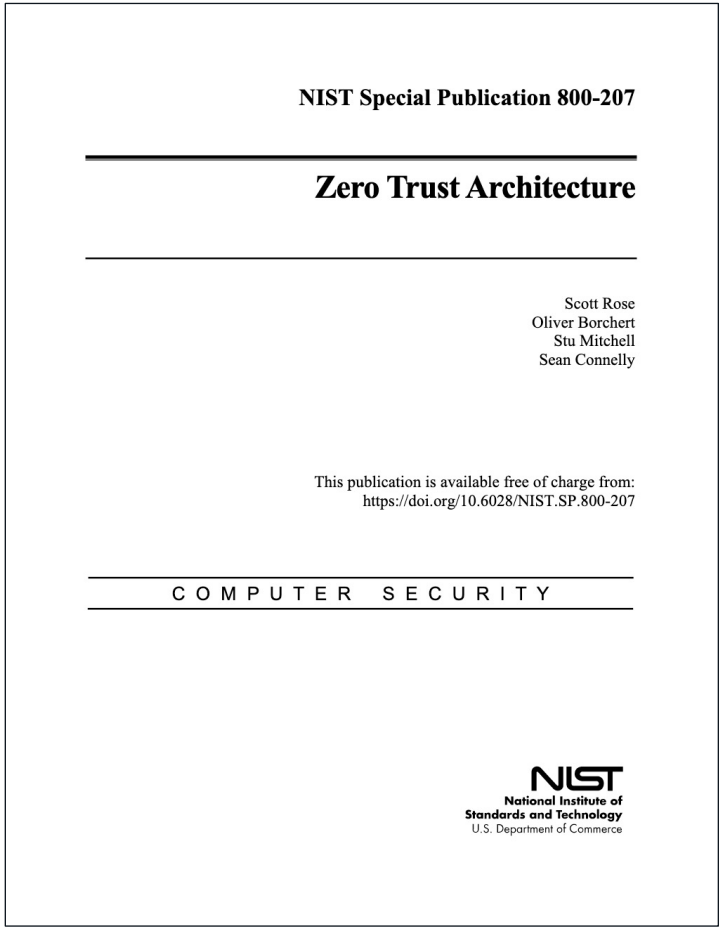


Continuous Adaptive Risk and
Threat Assessment (CARTA)

2019
NIST 800-207

NIST SP 800-207

Zero Trust Architecture



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST's "Tenets of Zero Trust Architecture"

1. **All data sources and computing services** are considered resources.
2. All communication is secure regardless of network location. **Network location does not imply trust.**
3. Access to individual enterprise resources is **granted on a per-connection basis**.
4. **Access to resources is determined by dynamic policy**, including the observable state of user identity and the requesting system, and may include other behavioral attributes.
5. The enterprise ensures **all owned and associated systems** are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible.
6. User **authentication is dynamic and strictly enforced** before access is allowed.
7. The enterprise collects as much information as possible about the **current state** of assets, network infrastructure and communications and uses it to improve its security posture.

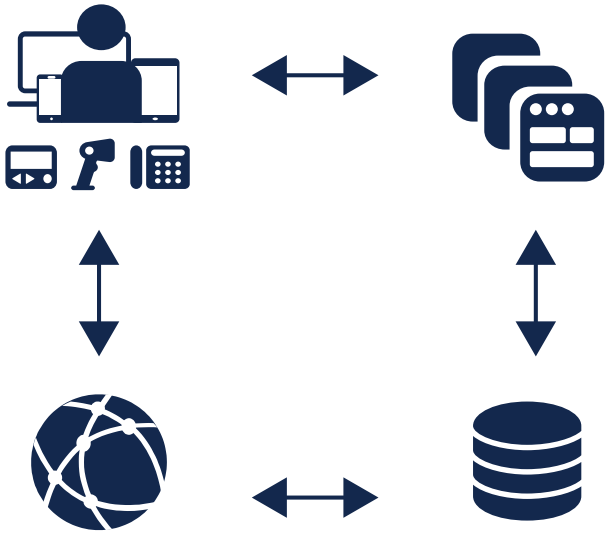
Cisco Zero Trust

Cisco Zero Trust

A zero-trust approach to securing access across your applications and environment, from any user, device and location.

Workforce

Ensure only the right users and secure devices can access applications.



Workplace

Secure all user and device connections across your network, including IoT.

Workload

Secure all connections within your apps, across multi-cloud.

Enforce Policy-Based Controls

Cisco's Implementation of Zero Trust

We establish trust by verifying:

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise

We enforce least privilege access to:

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins

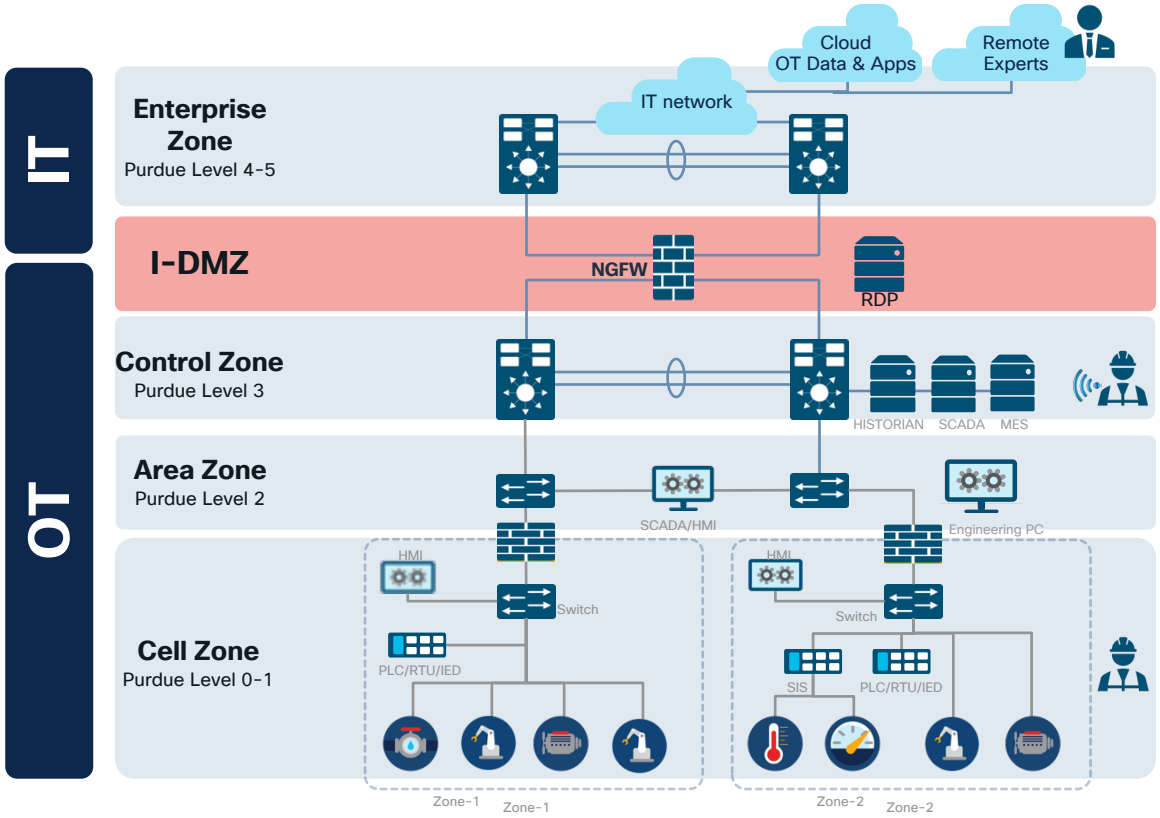
We continuously verify:

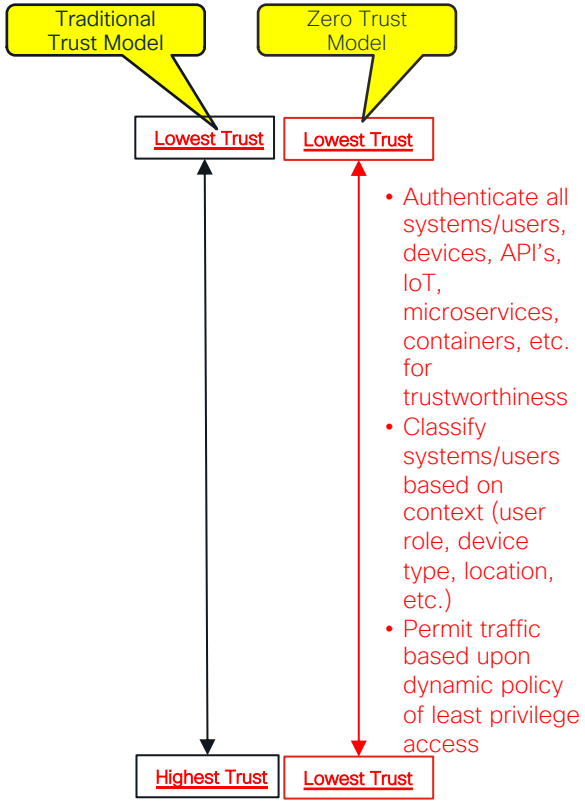
- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

Zero Trust for Industrial IoT

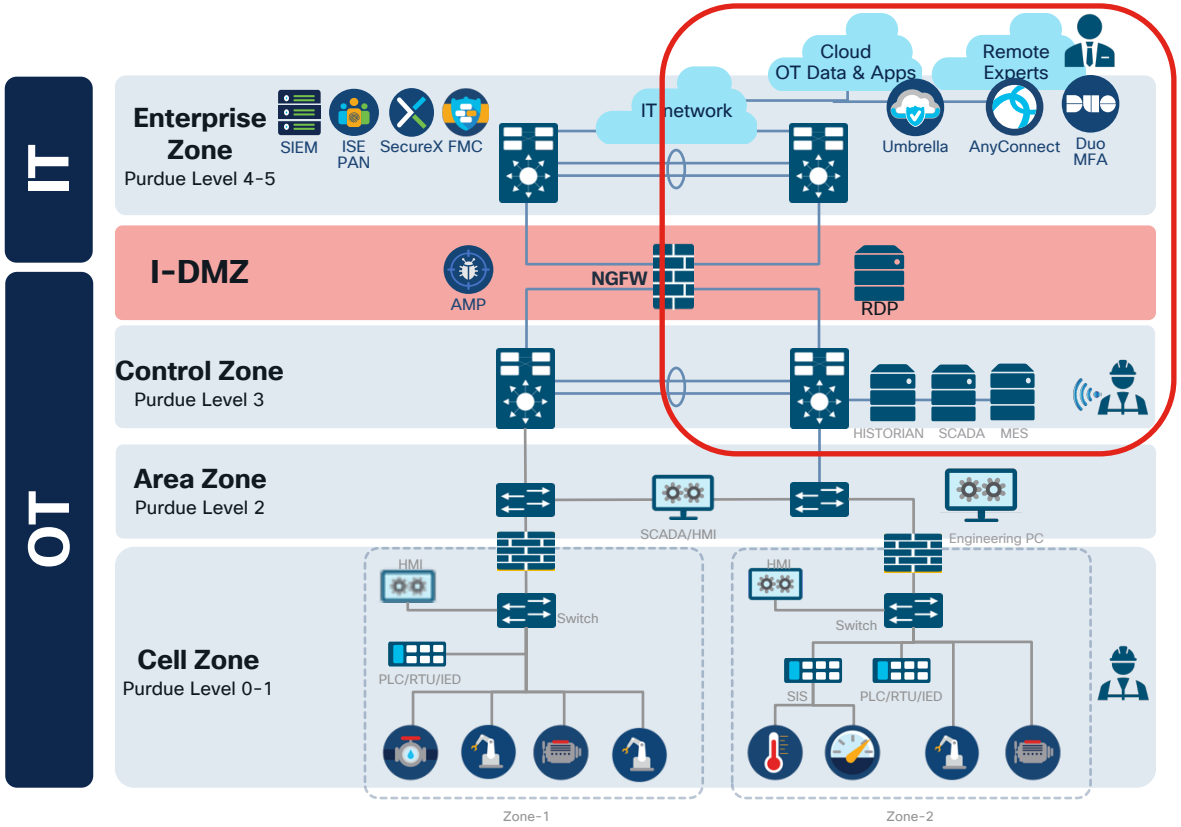
cisco Live!

Traditional v Zero Trust





Zero Trust for OT – Workforce

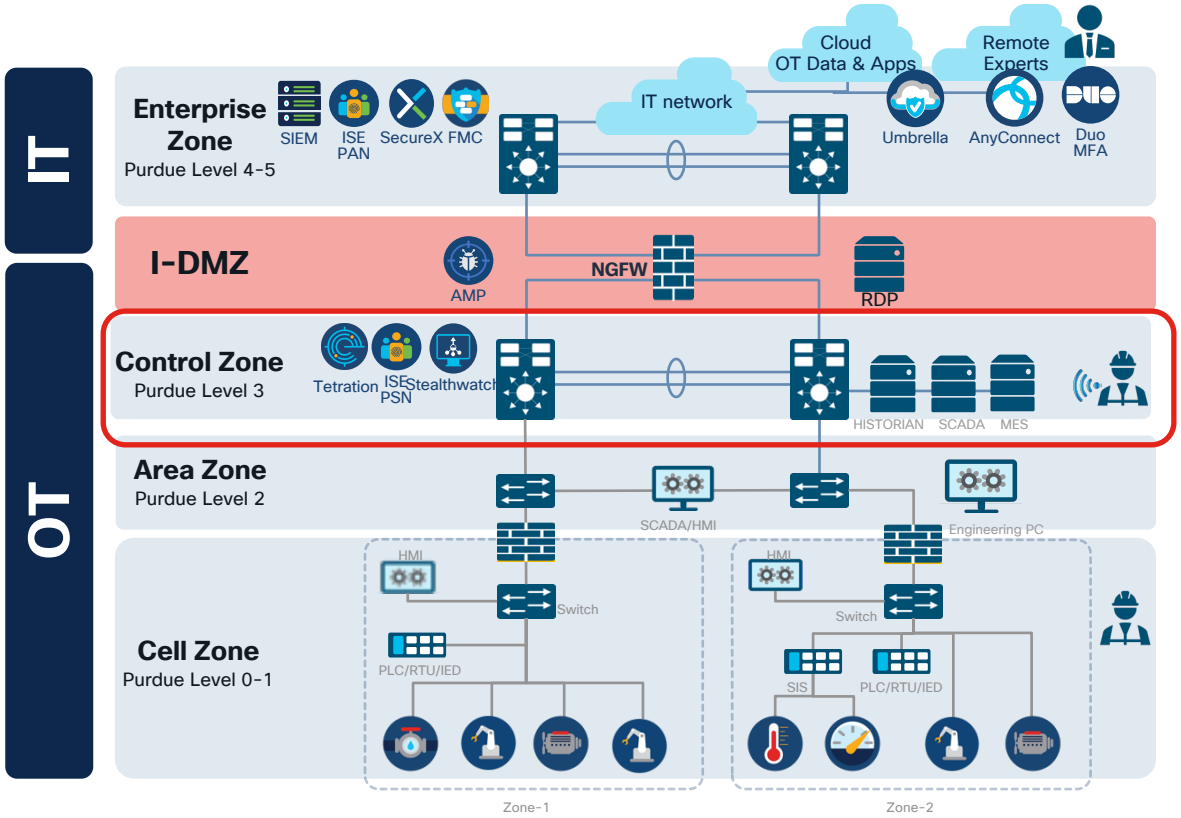


Apply strong authentication to all remote connections into the OT environment:

- VPN access
- RDP access
- Cloud Access

DUO, Umbrella, Anyconnect, Cisco Identity Services Engine (ISE)

Zero Trust for OT – Workloads

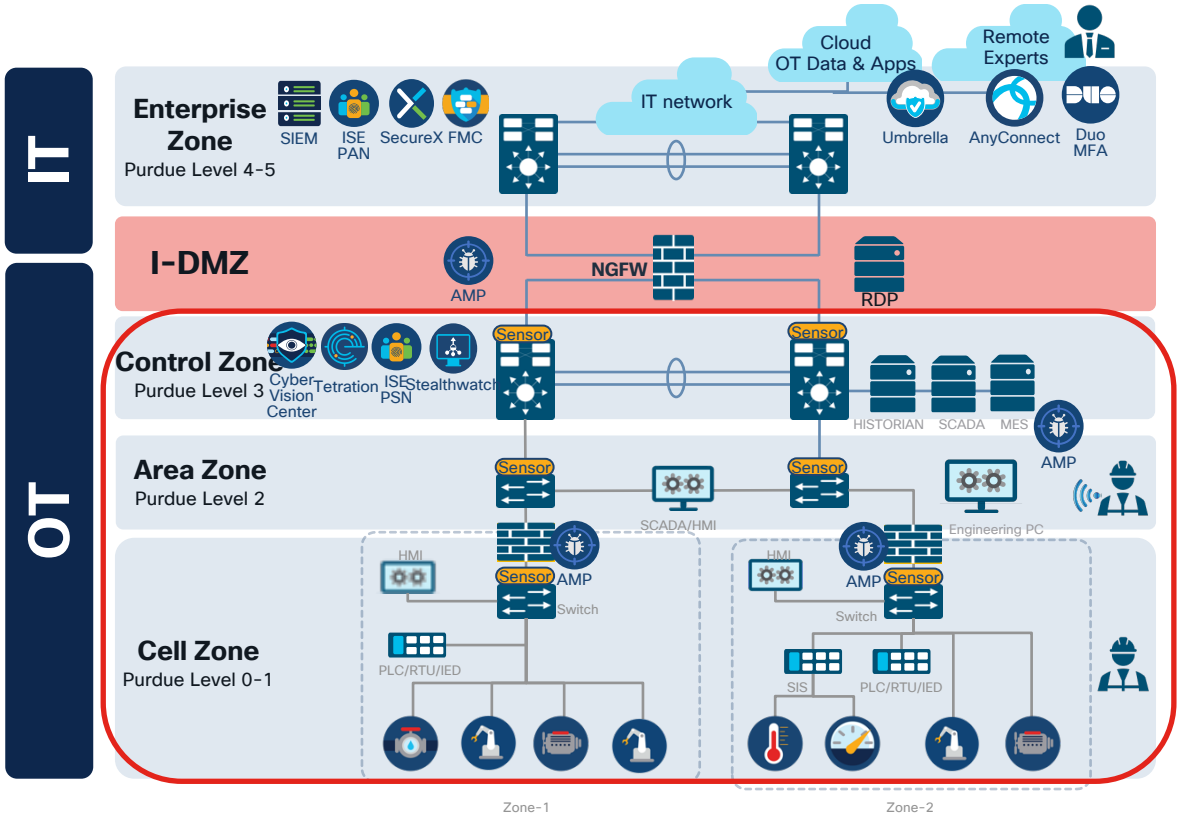


Enable application segmentation and whitelisting, along with host-based visibility, on critical apps that sit within the plant

An increasing number of applications moving to cloud environments for new Industry 4.0 use cases

Tetration, AppDynamics, Stealthwatch, ISE

Zero Trust for OT – Workplace

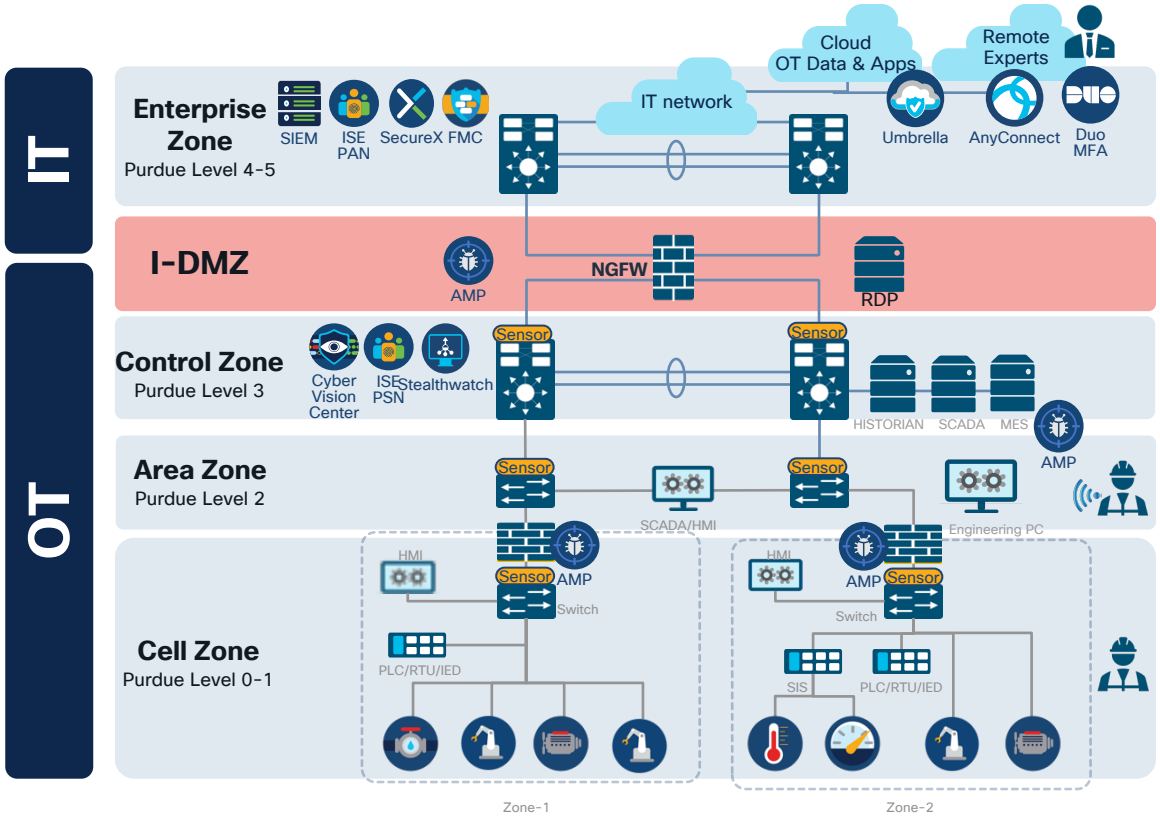


Automate device discovery and inventory using tools that are OT protocol-aware to provide context for segmentation policies.

Leverage software-defined segmentation between plant zones and ultimately within zones.

ISE, AMP, Cyber Vision, Stealthwatch, Industrial Firewall/IDS

Summary – Zero Trust for Industrial OT



Secure Workforce enabling the Secure Remote workforce, Remote Industrials Experts and Industrial collaboration irrespective of location

Secure Workloads and applications within the Industrial Datacenters and Secure the workloads in the cloud as new Industry 4.0 Initiatives drive cloud adoption

Secure Workplace for Industrial applications, processes and users within the industrial facilities

Continue your education

Demos in the Cisco campus

Meet the engineer 1:1 meetings

Walk-in labs

Relevant Sessions : PSOIOT-1002 Extending Zero Trust for the workplace to Industrial IoT

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive