zentera™

Protect What Matters™

Secluded Semiconductors, Inc. Case Study

Software Engineering Institute Zero Trust Industry Day

Marty Fabry
May 14, 2024

Gartner Cool Vendor 2017

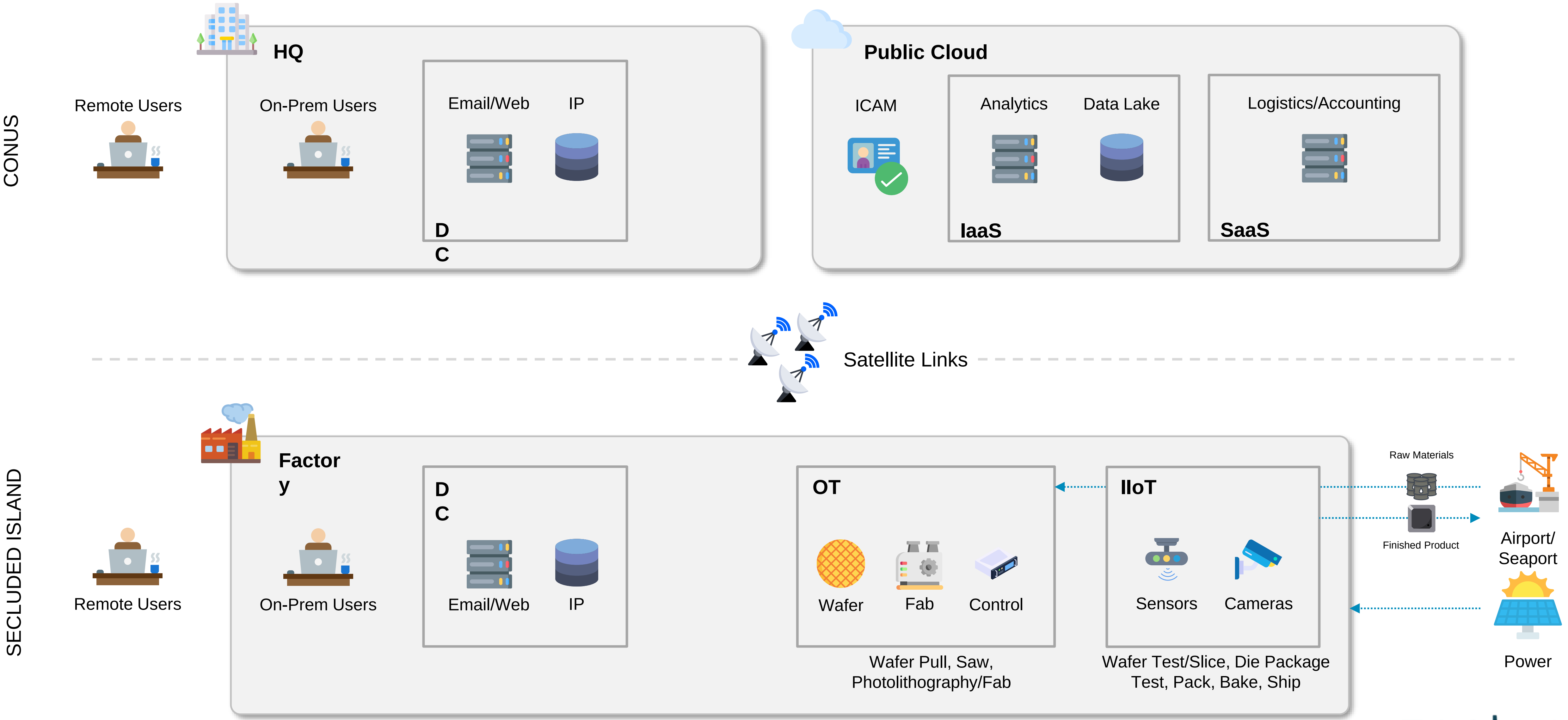
CISO CHOICE AWARDS 2020 FINALIST NETWORK SECURITY

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

Agenda

- Review of the Secluded Semiconductors environment
- Our approach to Zero Trust
- Proposed deployment architecture for Secluded Semiconductors
- Review of the challenge and specific questions
- Additional thoughts and considerations

Scenario - Secluded Semiconductors, Inc.



CONUS

Remote Users

HQ

On-Prem Users

Email/Web

IP

D
C

Public Cloud

ICAM

Analytics

Data Lake

IaaS

Logistics/Accounting

SaaS

Satellite Links

SECLUDED ISLAND

Remote Users

Factor
y

On-Prem Users

D
C

Email/Web

IP

OT

Wafer

Fab

Control

Wafer Pull, Saw, Photolithography/Fab

IIoT

Sensors

Cameras

Wafer Test/Slice, Die Package Test, Pack, Bake, Ship

Raw Materials

Finished Product

Airport/ Seaport

Power

Our Approach to Zero Trust

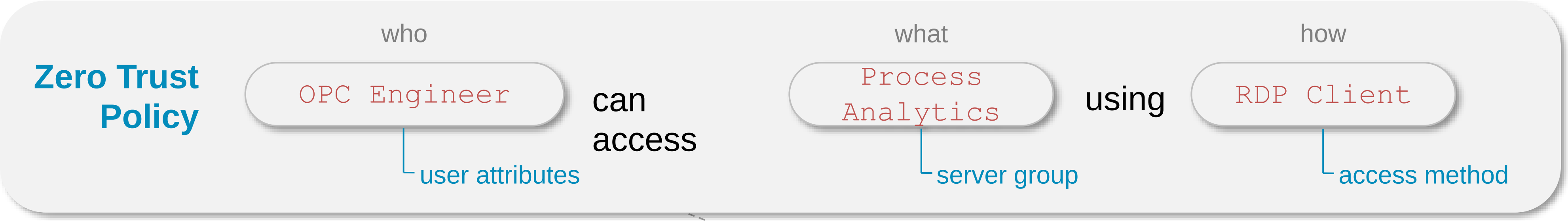
We combine

- Network zone-based segmentation (Virtual Chambers)
- Micro-segmentation inside and across chambers
- Access control (ZTNA, both remote and on-prem)
- Overlay application network

into an integrated, coherent solution

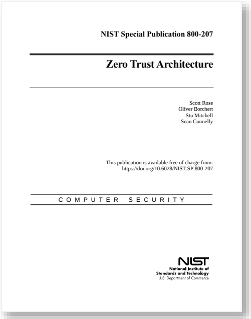
for IT, OT, and Cloud

Zentera CoIP® Platform: NIST SP800-207 ZTA With Simple, Identity-Based Policies



Zero Trust Policy

who: OPC Engineer (user attributes) can access what: Process Analytics (server group) using how: RDP Client (access method)



NIST Special Publication 800-207

Zero Trust Architecture

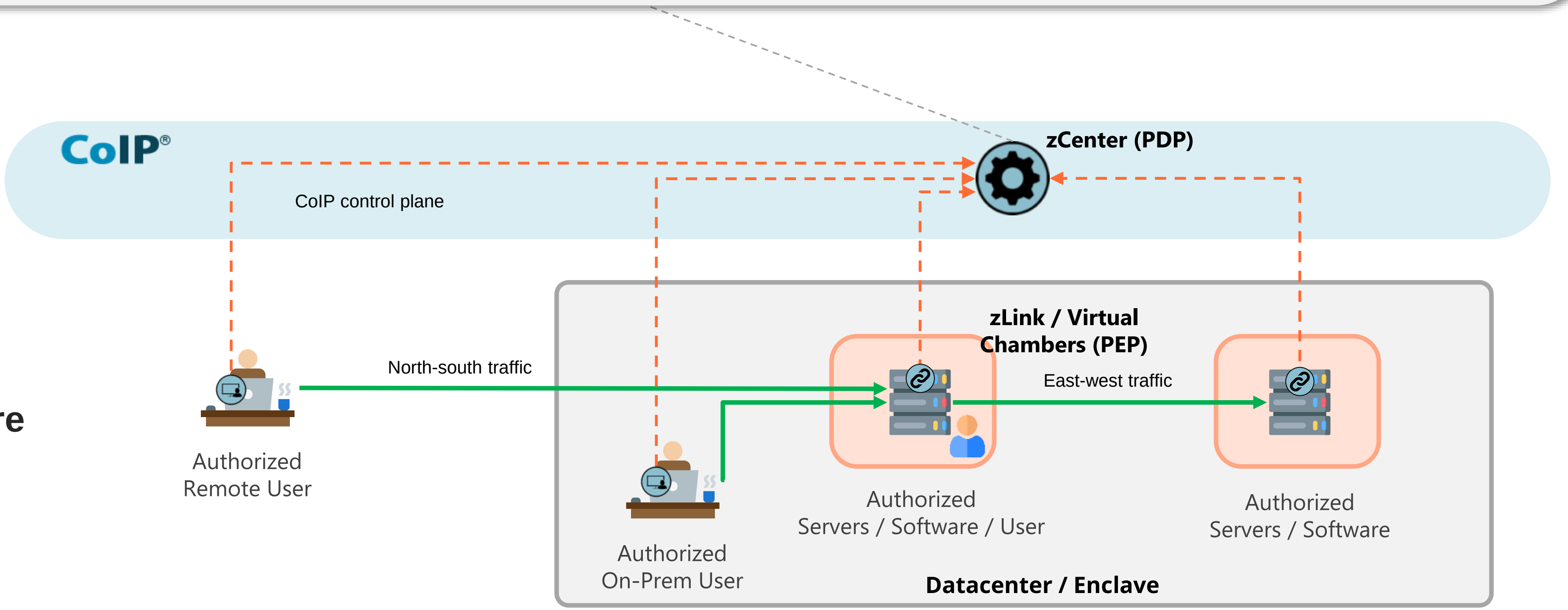
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

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

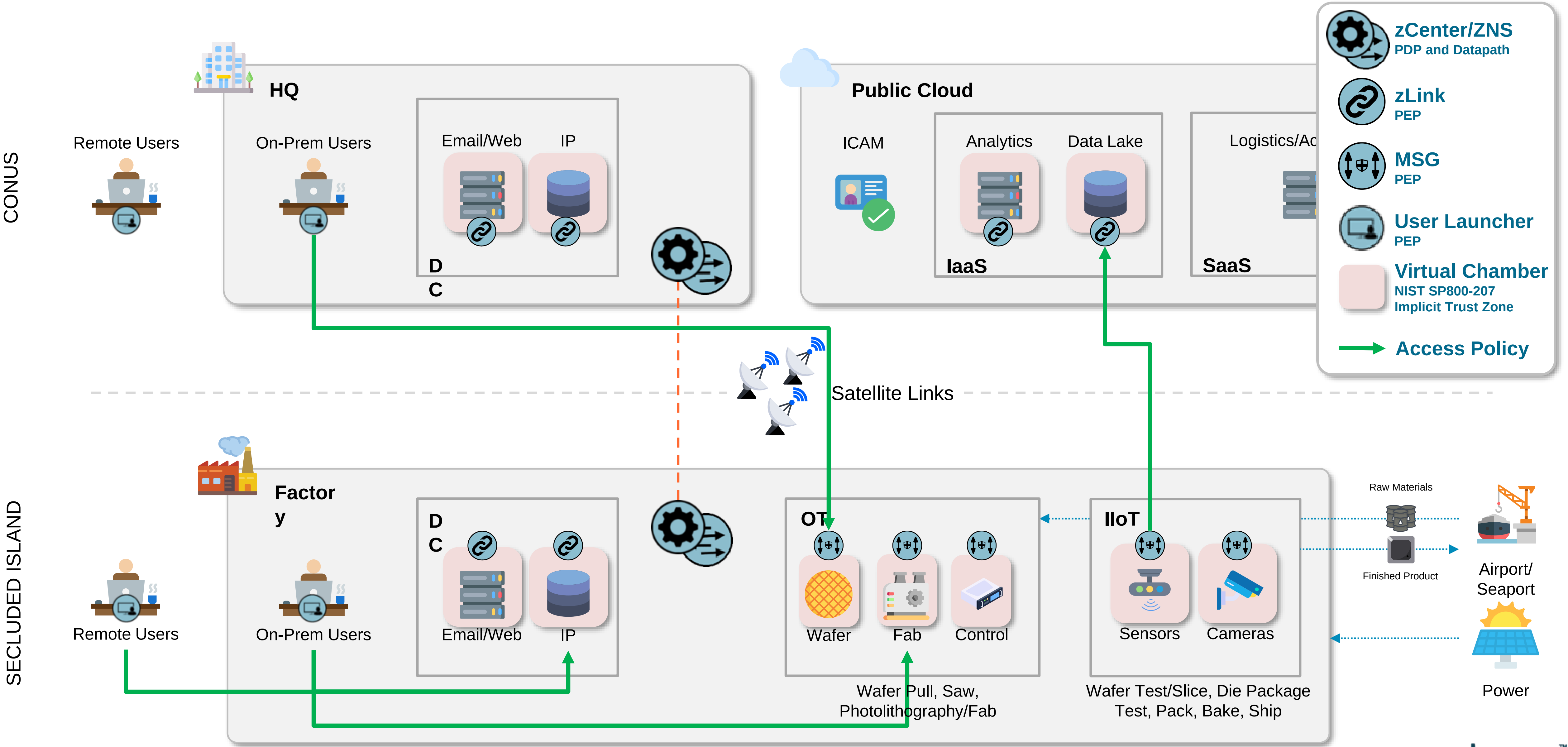
COMPUTER SECURITY

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

NIST SP 800-207
Zero Trust Architecture



Zentera Zero Trust Solution for Secluded Semiconductors



CONUS

Remote Users

HQ

On-Prem Users

Email/Web

IP

D
C

Public Cloud

ICAM

Analytics

Data Lake

IaaS

Logistics/Ac

SaaS

zCenter/ZNS
PDP and Datapath

zLink
PEP

MSG
PEP

User Launcher
PEP

Virtual Chamber
NIST SP800-207
Implicit Trust Zone

Access Policy

Satellite Links

SECLUDED ISLAND

Factor
y

D
C

Email/Web

IP

Remote Users

On-Prem Users

OT

Wafer

Fab

Control

IIoT

Sensors

Cameras

Wafer Pull, Saw, Photolithography/Fab

Wafer Test/Slice, Die Package Test, Pack, Bake, Ship

Raw Materials

Finished Product

Airport/ Seaport

Power

Challenge

A hurricane passes by the island that knocks out the satellite communications and could reduce the power grid capabilities for up to three days.

How would your zero trust approach support continued operations for the manufacturing facility?

Questions

1. What mitigations would reduce the resulting security/resilience risks and threats associated with the island infrastructure?

- For the ZT system, the PDP is deployed with HA – island and CONUS ZT systems continue to operate autonomously until connectivity is restored
  - Chambers continue to protect data and assets against unauthorized access, for example malicious insiders who may seek to take advantage of the event
- Virtual chambers can be configured to fail open, allowing administrators to prioritize availability/safety if the factory network infrastructure is unstable
- Dependencies on CONUS resources and applications should be identified and a suitable local backup should be configured to minimize the need to fail-open

Questions

2. What concerns do legacy systems create, and how would the legacy systems be addressed to support the zero trust strategy?

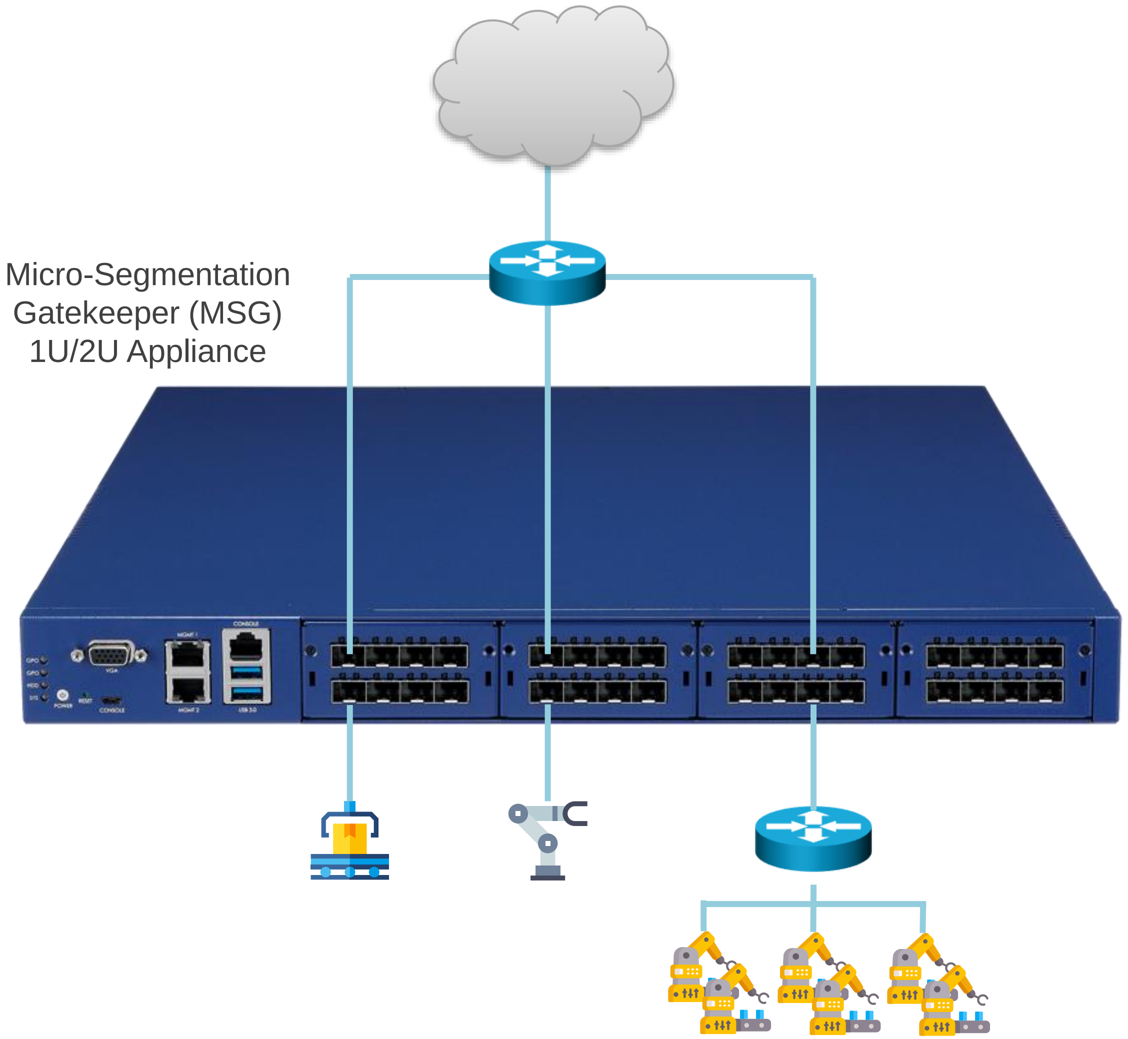
- Legacy systems:
  - May not be patchable, and may have many vulnerabilities as a result
  - May not support modern authentication methods, including multi-factor
  - May be deployed with network topologies that cannot be easily changed (e.g. to add segmentation)
- Zentera uses the following strategies to protect legacy systems
  - Micro-segmentation to isolate legacy systems, with ZT identity-based access control
  - Encrypted LAN/WAN overlay to hide vulnerable traffic
  - Agent-based PEP for Win XP+, RHEL 5+, etc
  - Agentless PEP (MSG) for all other types of legacy systems

Questions

3. What challenges arise with OT and IIoT systems when considering a zero trust implementation? How do you resolve those challenges?

- OT and IIoT systems often are closed, and do not support agent-based deployments
- The Zentera MSG enables a “Zero Trust DMZ” deployed in front of OT/IIoT workloads or subnets containing them

MSG: Micro-Segmentation, Access Control, with Zero Trust Enforcement

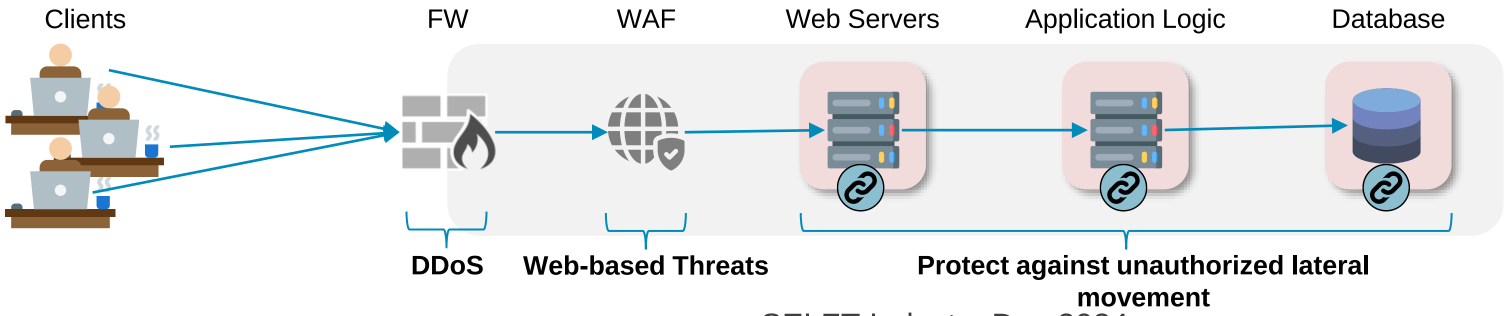


- Creates an inline segmentation boundary (“Zero Trust DMZ”) enforcing new implicit trust zones for groups of devices
- Layer 2 non-disruptive insertion (no change to existing IP switch and routing architecture), with hardware bypass for fail-open
- Inline Zero Trust access policy enforcement
- Terminates ZTNA user access sessions in ZT DMZ
- Various form factors and LAN modules for different applications

Questions

4. In a highly connected system like a smart city, how do you handle threats and vulnerabilities with a zero trust implementation without impacting overall functionality?

- Wherever possible, migrate users to ZT authentication, especially for sensitive or privileged services, and make web / data services private
- In a highly connected system, it may not be feasible to identify every single client (e.g. public-facing web service)
  - In such cases, we recommend deploying standard application protections (e.g. FW, WAF) and protect each tier with its own NIST SP800-207 trust zone



Zero Trust enforces proper flow of tiered communications, and enables quarantining of servers that violate policy

Questions

5. How does zero trust help address the accessibility and availability required of a manufacturing environment?

- Zero Trust can:
  - help to reduce the urgency of patching, or provide a compensating control for unpatchable (EOL) systems
  - provide simple, least-privilege access to remote users, improving user experience while reducing the attack surface of the manufacturing environment
  - be configured to fail-open, enabling administrators to make conscious choices about how and when to degrade security effectiveness
  - reduce the urgency of cyber incident response due to compartmentalization provided by segmentation

Questions

6. What factors must be considered when managing disasters with a zero trust implementation?

- Failover behavior triggered by denied, degraded, intermittent, or limited (DDIL) communications on ZT orchestration and dependencies
- Implicit trust zone behavior for an asset: fail-closed (prioritize Confidentiality) or fail-closed (prioritize Availability)?
- Enhanced logging and history during a disaster are crucial for forensics and post-mortem analysis

Questions

7. In the event of a loss of connectivity with cloud services, how do you manage identity and access management (IAM)?

- Our Zero Trust solutions can support configuration of multiple IAM/identity providers to help avoid single points of failure
- Access rights are documented by Zero Trust policies and maintained in a replicated database

Final Considerations for Secluded Semiconductors

- The importance of integration
  - For the Zero Trust program to succeed, it cannot just be about maturity in each pillar; action must be orchestrated across *all* pillars; even “best of breed” tools may be exceedingly difficult to orchestrate if not designed for this!

- Focus on adopting Zero Trust from the inside out
  - Zero Trust is about protecting assets and data – not about creating “secure infrastructure”
  - Make the problem and journey tractable by protecting a few applications, learning how to operate, and then scale

- Overlay networks can be very useful!
  - Eliminating dependence on physical IPs can help with resiliency by allowing you to quickly use alternate connectivity
  - Service insertion of other tools as necessary – eg DLP scanning, threat analysis, etc.

Q&A

Thank You!

Marty Fabry

VP of Field Services

mfabry@zentera.net

www.zentera.net | info@zentera.net | 408-436-4811

zentera™

Connect · Protect · Shield