

Enable Zero Trust Network Access for Industrial Networks with Cisco Secure Equipment Access

CISCO Live !

Jie Wei
Industrial IoT Solutions Engineer

Cisco Webex App

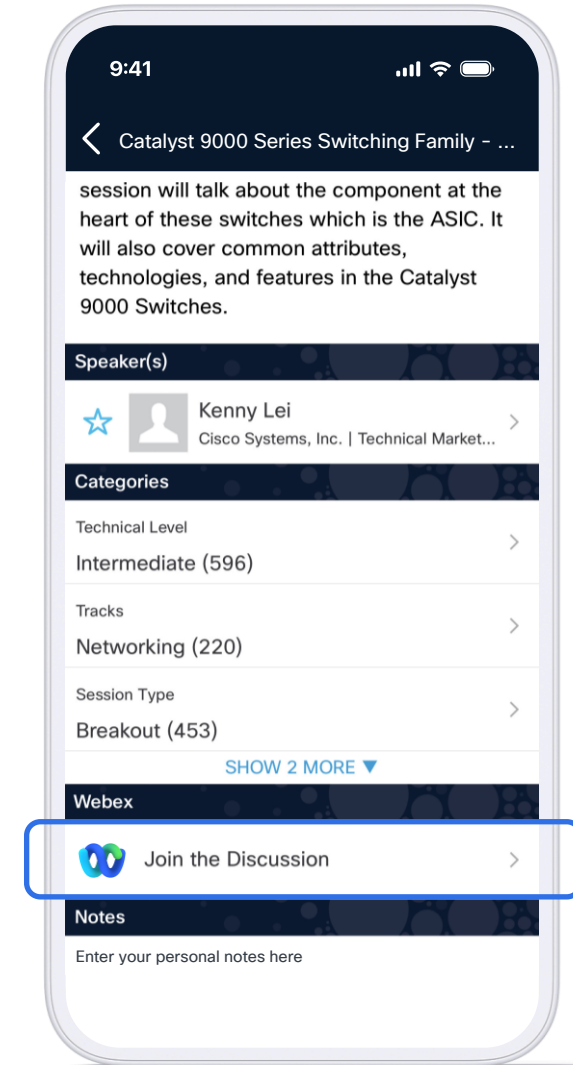
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-1005>

Let's start with Slido

slido.com #153 2463



Passcode: a4tls8

- 1 Cyber security mandates for remote access
- 2 Identity Security: The importance of MFA
- 3 Is cloud based remote access risky?
- 4 Remote Access Technologies and Cyber Security
- 5 Cisco Secure Equipment Access



**What technology do you currently use
for remote access to OT network?
Select all that apply.**



Is your remote access solution dedicated to the OT? Or do you leverage the existing IT implementation?



The Slido app must be installed on every computer you're presenting from

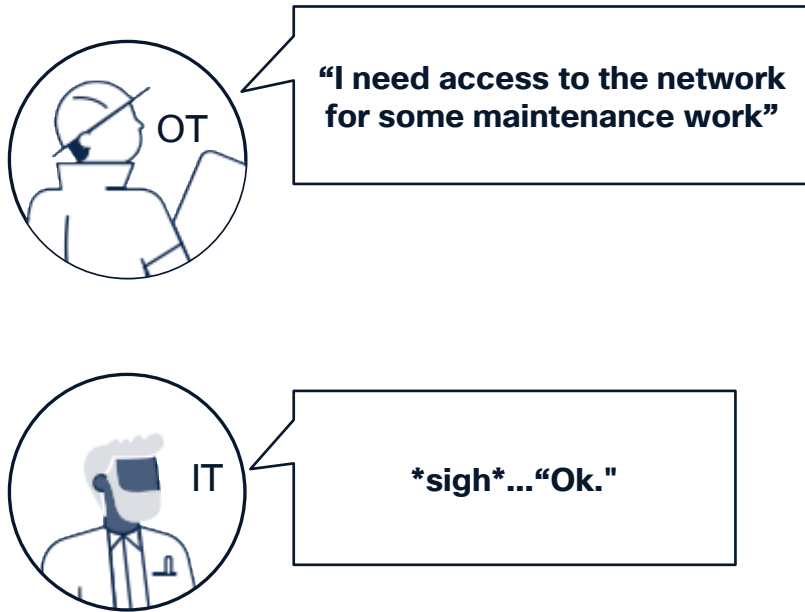
BRKIOT-1005

slido



What are your biggest challenges when providing remote access to 3rd parties?

“Secure” remote access typically means user frustration with cumbersome experiences



- ⚠ Add user account to the VPN
- ⚠ MFA is an optional add-on!
- ⚠ Create policies for VPN user so they cannot access network
- ⚠ Give user credentials to the jump server
- ⚠ Add network policies to jump server to stop lateral movement
- ⚠ Setup WebEx call so I can watch remotely
- ⚠ Remember to close all policies when session is over

How long does it take for remote access to be granted to the OT network?

2024 by the numbers

User identity is still the top target for attackers:

- **Credential abuse** is the most common way to breach a network
- **Phishing** is the most common delivery method

Exploiting the remote access hardware is a new trend:

- **34% rise** in successful exploits due to vulnerabilities
- **22%** of all vulnerability exploitation breaches targeted **edge infrastructure** such as **firewalls, VPN & remote access gateways** which was only 3% in 2023



2025 Verizon Data Breach Investigations Report

Mandates must be implemented to drive change

NIS2

BRIEFING

EU Legislation in Progress



European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Proposal for a directive on measures for a high common level of cybersecurity across the Union		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2020) 823
Rapporteur:	Bart Groothuis (Renew, the Netherlands)	16.12.2021
Shadow rapporteurs:	Eva Maydell (EPP, Bulgaria)	2020/0359(COD)
	Eva Kallii (S&D, Greece)	
	Rasmus Andresen (Greens/EFA, Germany)	Ordinary legislative procedure (COD)
	Thierry Mariani (UD, France)	(Parliament and Council on equal footing – formerly 'co-decision')
	Evžen Tolemovský (ECR, Czechia)	
	Marisa Matias (The Left, Portugal)	
Procedure completed:	Directive (EU) 2022/2555	
	OJ L 333, 27.12.2022, pp 80-152	

NIST

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-82 Rev. 3

Guide to Operational Technology (OT) Security

f

t

in

e

Date Published: September 2023

Supersedes: [SP 800-82 Rev. 2 \(06/03/2015\)](#)

Author(s)

Keith Stouffer (NIST), Michael Pease (NIST), CheeFee Tang (NIST), Timothy Zimmerman (NIST), Victoria Pillitteri Lightman (NIST), Adam Hahn (MITRE), Stephanie Saravia (MITRE), Aslam Sherula (MITRE), Michael Thompson (P

Abstract

This document provides guidance on how to secure operational technology (OT) while addressing their un performance, reliability, and safety requirements. OT encompasses a broad range of programmable system that interact with the physical environment (or manage devices that interact with the physical environmer systems and devices detect or cause a direct change through the monitoring and/or control of devices, pr events. Examples include industrial control systems, building automation systems, transportation systems control systems, physical environment monitoring systems, and physical environment measurement syste document provides an overview of OT and typical system topologies, identifies common threats and vulne these systems, and provides recommended security countermeasures to mitigate the associated risks.

Keywords

computer security; distributed control systems (DCS); industrial control systems (ICS); information security security; operational technology (OT); programmable logic controllers (PLC); risk management; security cc supervisory control and data acquisition (SCADA) systems

ISA/IEC-62443

ISA

International Society of Automation

Standards

ISA Standards and Publications / ISA Standards / ISA/IEC 62443 Series of Standards

ISA/IEC 62443 Series of Standards

The World's Only Consensus-Based Automation Systems Cybersecurity Standards



The ISA/IEC 62443 series of standards define requirements and processes for implementing a electronically secure industrial automation and control systems (IACS). These standards set b security and provide a way to assess the level of security performance. Their approach to the challenge is a holistic one, bridging the gap between operations and information technology a process safety and cybersecurity.

NERC CIP

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standards for the Bulk Electric Systems of North America

Updated April 1, 2024

RELIABILITY | ACCOUNTABILITY



TSA



U.S. Department of Homeland Security
Transportation Security Administration
6545 Springfield Center Drive
Springfield, Virginia 20598

NUMBER

Security Directive 1580/82-2022-01

SUBJECT

Rail Cybersecurity Mitigation Actions and Testing

EFFECTIVE DATE

October 24, 2022

EXPIRATION DATE

October 24, 2023

SUPERSEDES

Not Applicable

APPLICABILITY

Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads

AUTHORITY

49 U.S.C. 114(d), (f), (i) and (m)

LOCATION

All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to mitigate the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure."¹

This Security Directive requires actions necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads.² Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply

¹ See *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).

² This Security Directive is issued under the authority of 49 U.S.C. 114(j)(2)(A), which states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without needless action or

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKIOT-1005

Mandates must be implemented to drive change

NIS2

*the use of **multi-factor authentication** or continuous authentication solutions*

NIST

***MFA** is an accepted best practice for remote access to OT applications*

ISA/IEC-62443

*SR 1.1 RE 2 – **MFA** for untrusted networks*

*SR 1.1 RE 3 – **MFA** for all networks*

NERC CIP

*005-7 – Remote Access Management: **Require MFA***

TSA

MFA** or other logical and physical security controls that **supplement password authentication

Identity Security: The Importance of MFA

Why hack when you can log in?



of breaches leveraged identity
as a key component

Source: Cisco Talos Incident Response Data 2023-2024

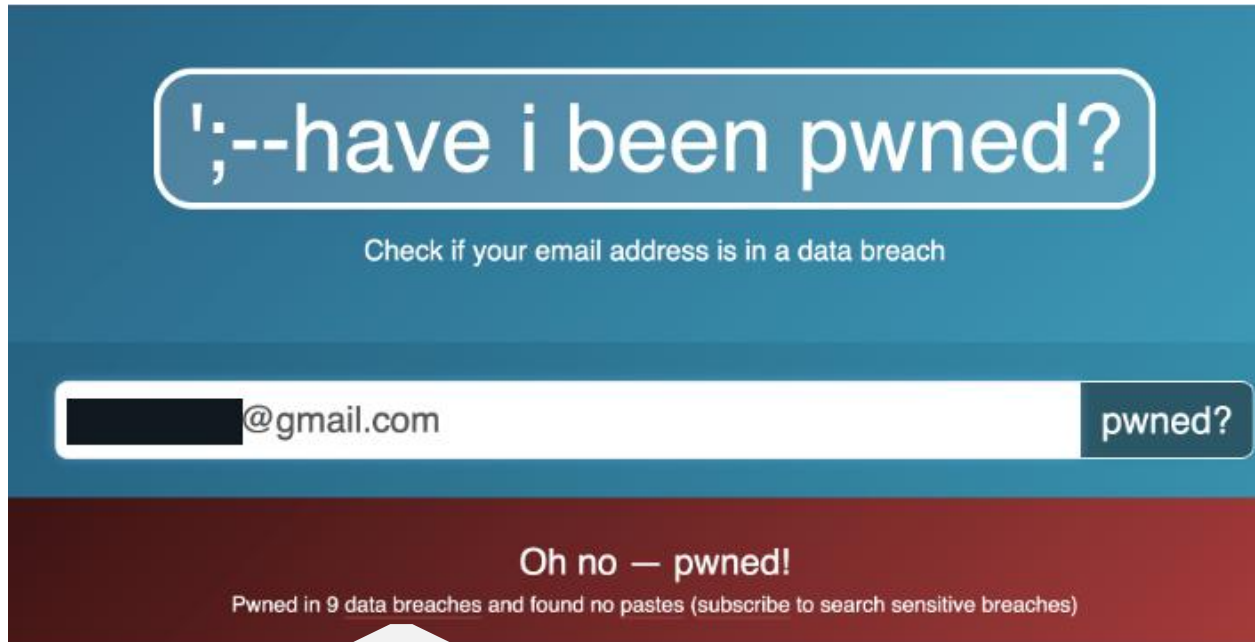
It is sometimes as easy as this



How many of you scanned this at the start of the session?

How many of these have you scanned at this trade show?

Have I been Pwned?



';--have i been pwned?

Check if your email address is in a data breach

pwned?

Oh no — pwned!

Pwned in 9 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

9 data breaches

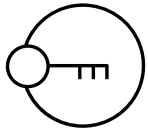
361M unique email addresses

Combolist Posted to Telegram: In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

Compromised data: Email addresses, Passwords, Usernames

Passwords,

Multi-Factor Authentication (MFA)



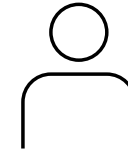
Something you **know**

- Password
- PIN
- Email Verification



Something you **have**

- Mobile
- Yubikey

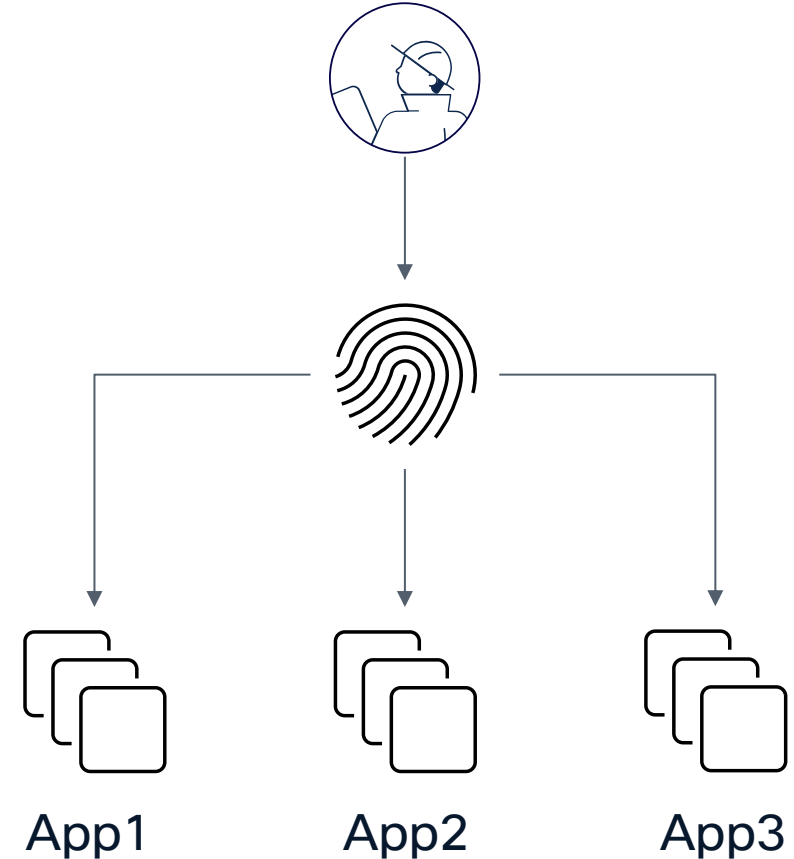


Something you **are**

- Fingerprint
- Facial Recognition

Single Sign-On (SSO)

- One authentication for many applications
- Reduces password sprawl
- Single set of policies across all your applications



Identity Threat Detection & Response (ITDR)

focuses on identifying anomalies in human behavior, detecting potential unauthorized access, and responding to security incidents promptly.

Proactive



Monitoring identity infrastructure for misconfiguration and weaknesses

Examples:

- No or weak MFA
- Dormant accounts
- Over-privileged users
- Administrative account overuse
- SSO bypass
- User inconsistencies

Reactive



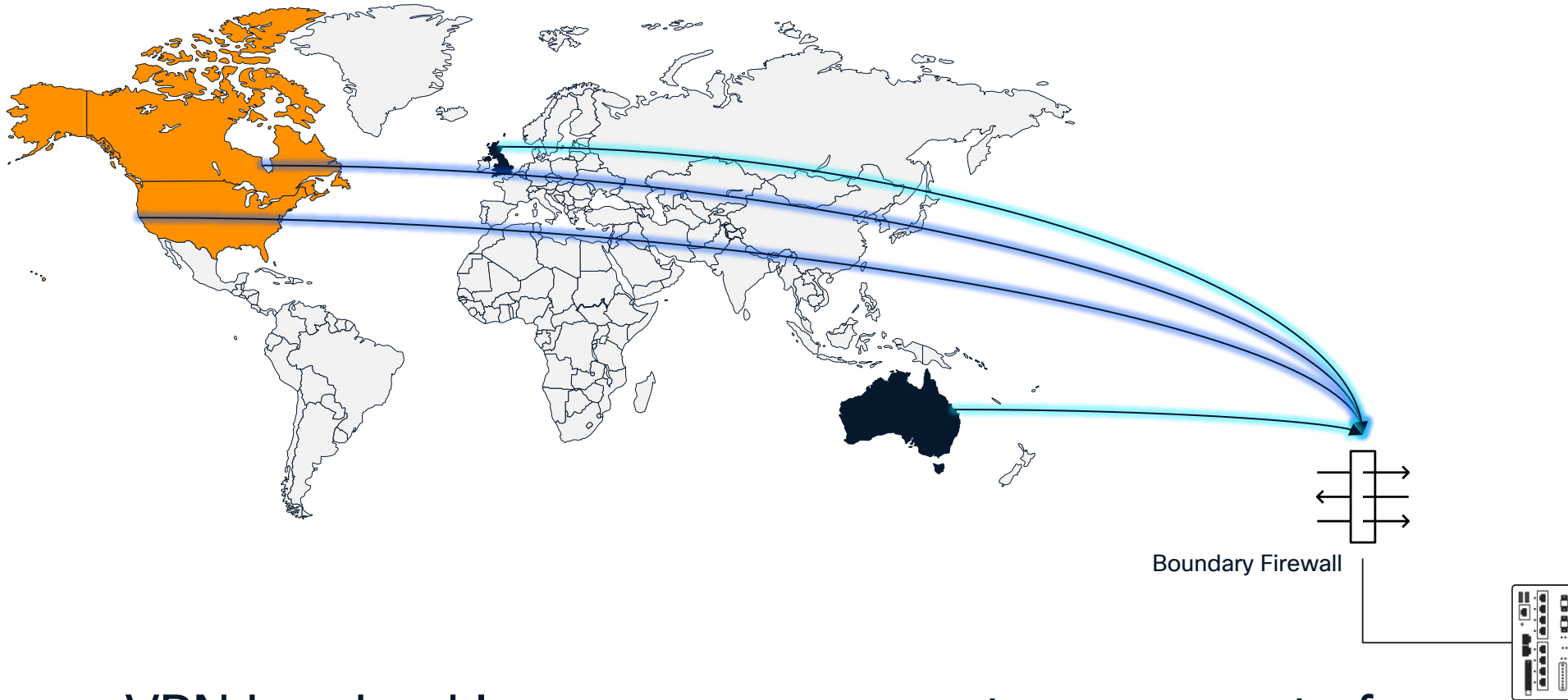
Detection logic that prioritizes identity Tactics, Techniques and Procedures (TTPs)



Automation to eradicate, recover from, and remediate identity threats

Is cloud-based remote access risky?

Remote users come from outside of your network



If your VPN headend is on-prem, you must expose part of your network to the public **which invites exploitation**

Revisiting the numbers

User identity is still the top target for attackers:

- Credential abuse is the most common way to breach a network
- Phishing is the most common delivery method

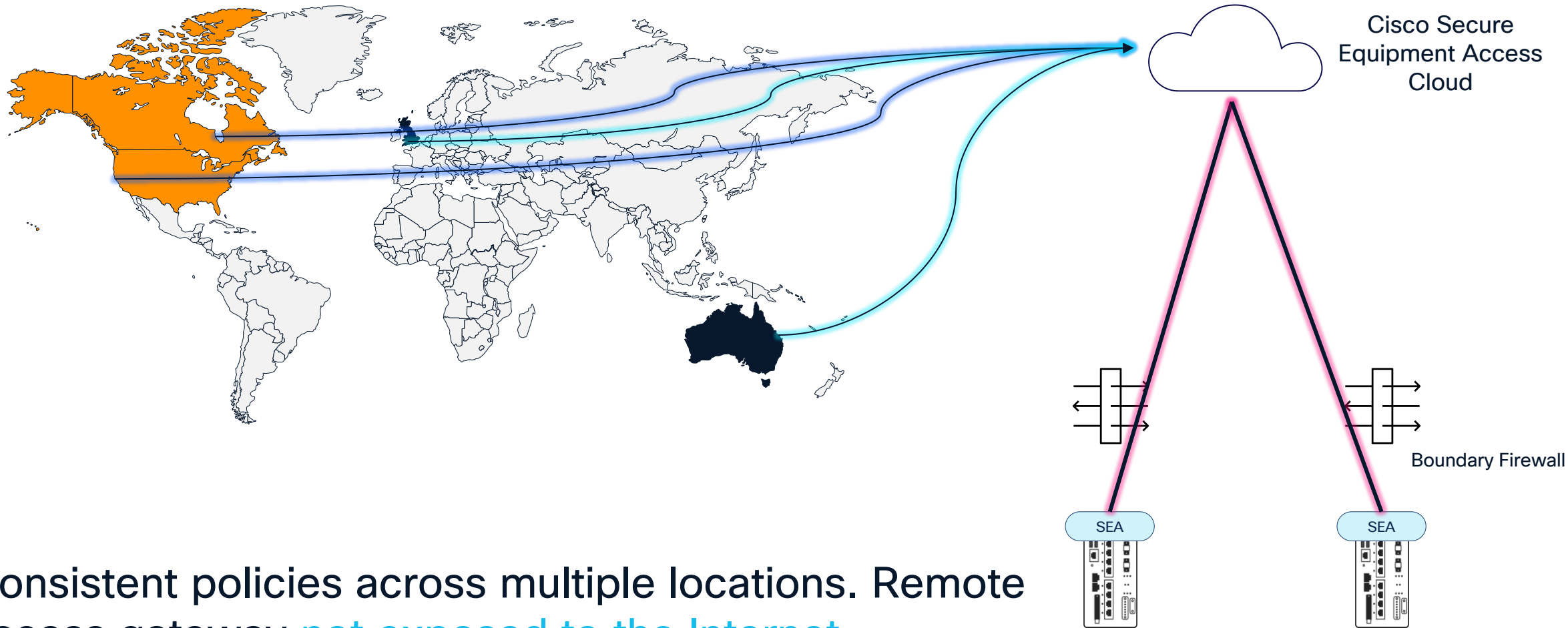
Exploiting the remote access hardware is a new trend:

- 34% rise in successful exploits due to vulnerabilities
- 22% of all vulnerability exploitation breaches targeted edge infrastructure such as firewalls, VPN & remote access gateways which was only 3% in 2023



2025 Verizon Data Breach Investigations Report

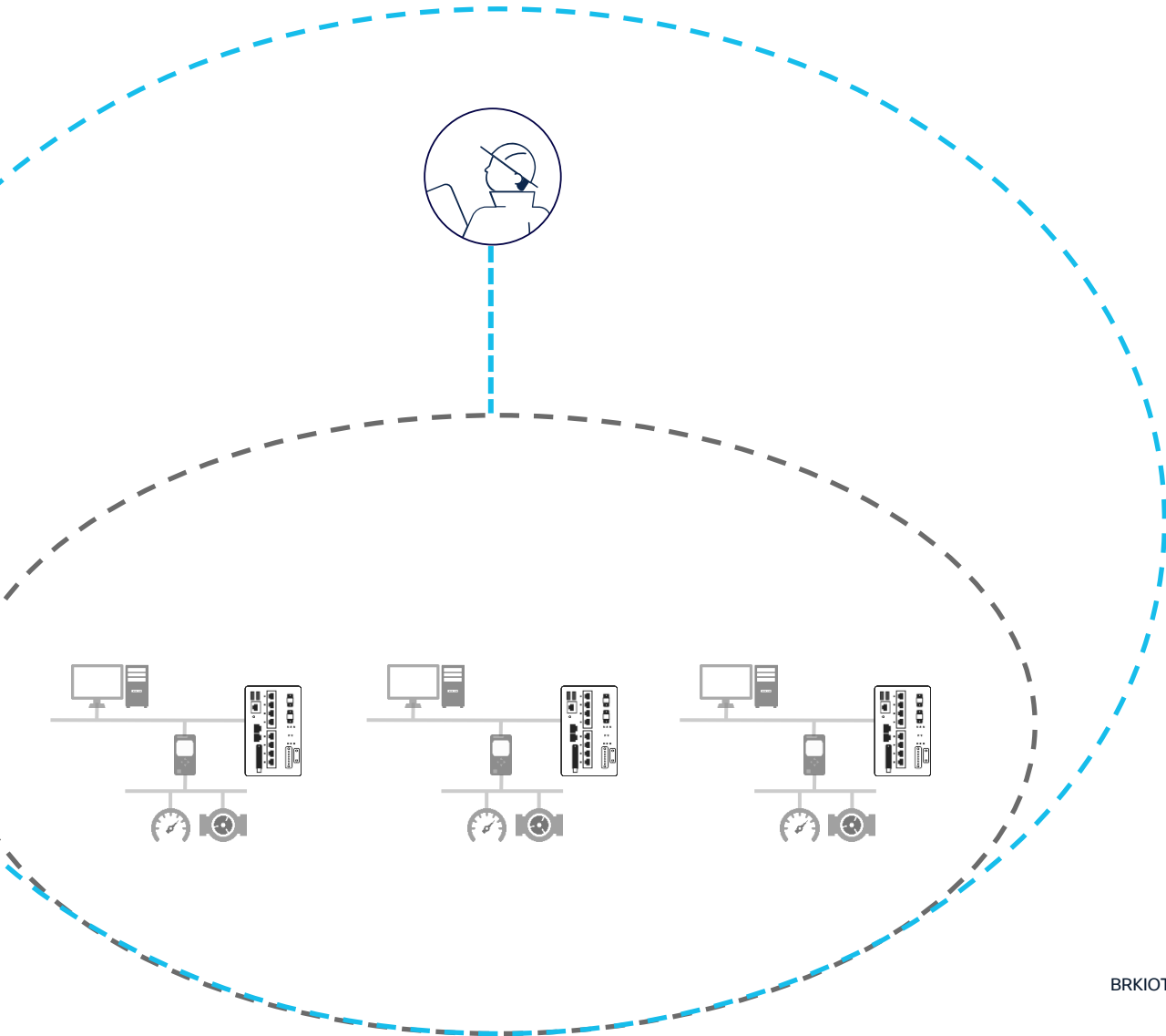
OT Network only needs a single trusted flow through the firewall



Consistent policies across multiple locations. Remote access gateway not exposed to the Internet

Remote Access Technologies

Virtual Private Network (VPN)



- Extends the network to remote users

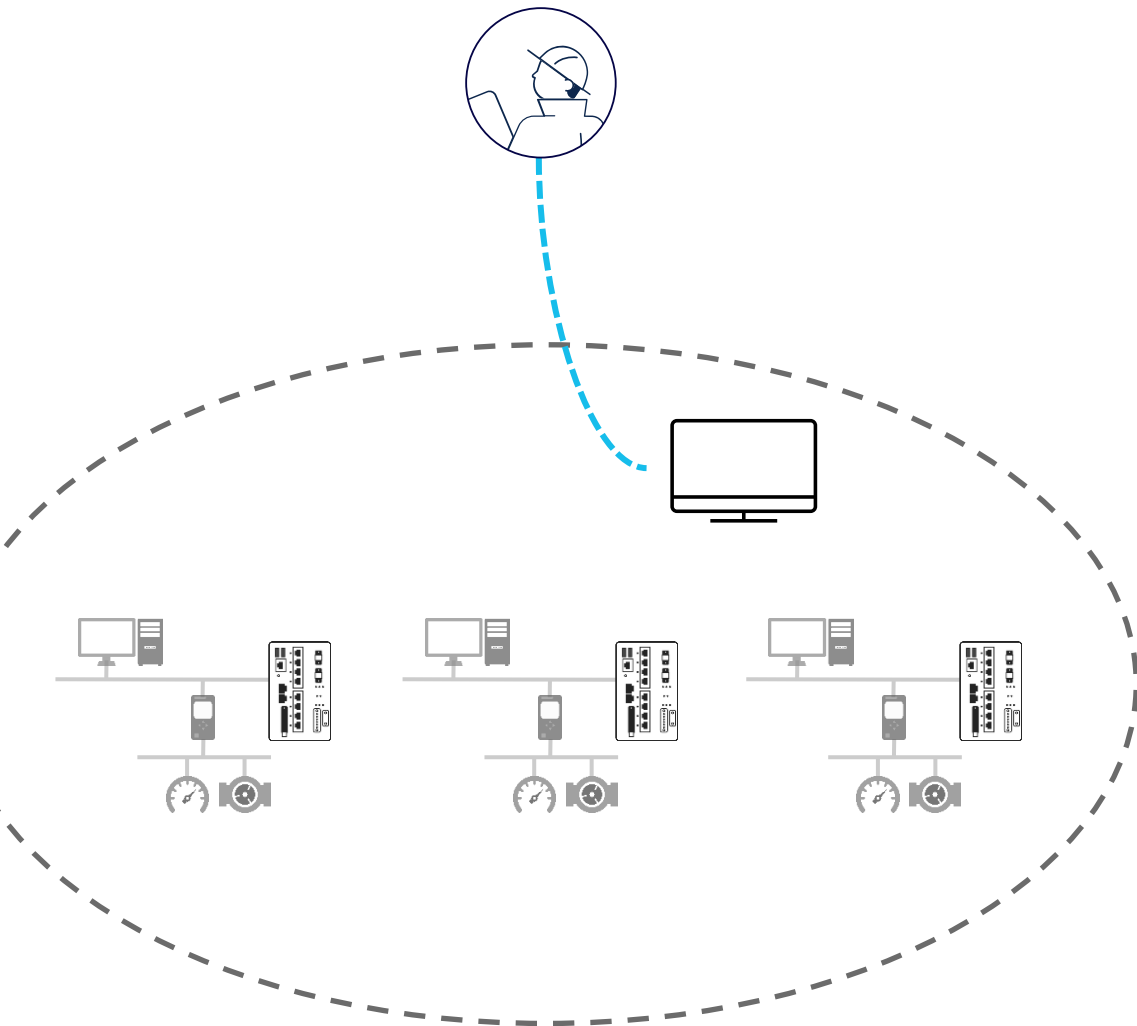
Pros

- Users can use applications hosted natively on their devices
- Minimal friction from end user experience

Cons

- Users have an IP address on your network
- Additional steps for lateral movement and reconnaissance to be prevented
- VPN headend has public IP that will be targeted
- Client can sometimes be a burden
- MFA an additional add-on

Jump Servers



- Users do all their tasks from a trusted device hosted in the network

Pros

- Minimize the risk of introducing malware from client device
- Devices can be locked down to only permitted applications
- Jump servers can reside in isolated state until needed

Cons

- Additional overhead often leads to over privileged jump servers
- Must maintain vendor applications
- MFA still not a hard requirement

Shift to Zero Trust Network Access (ZTNA)

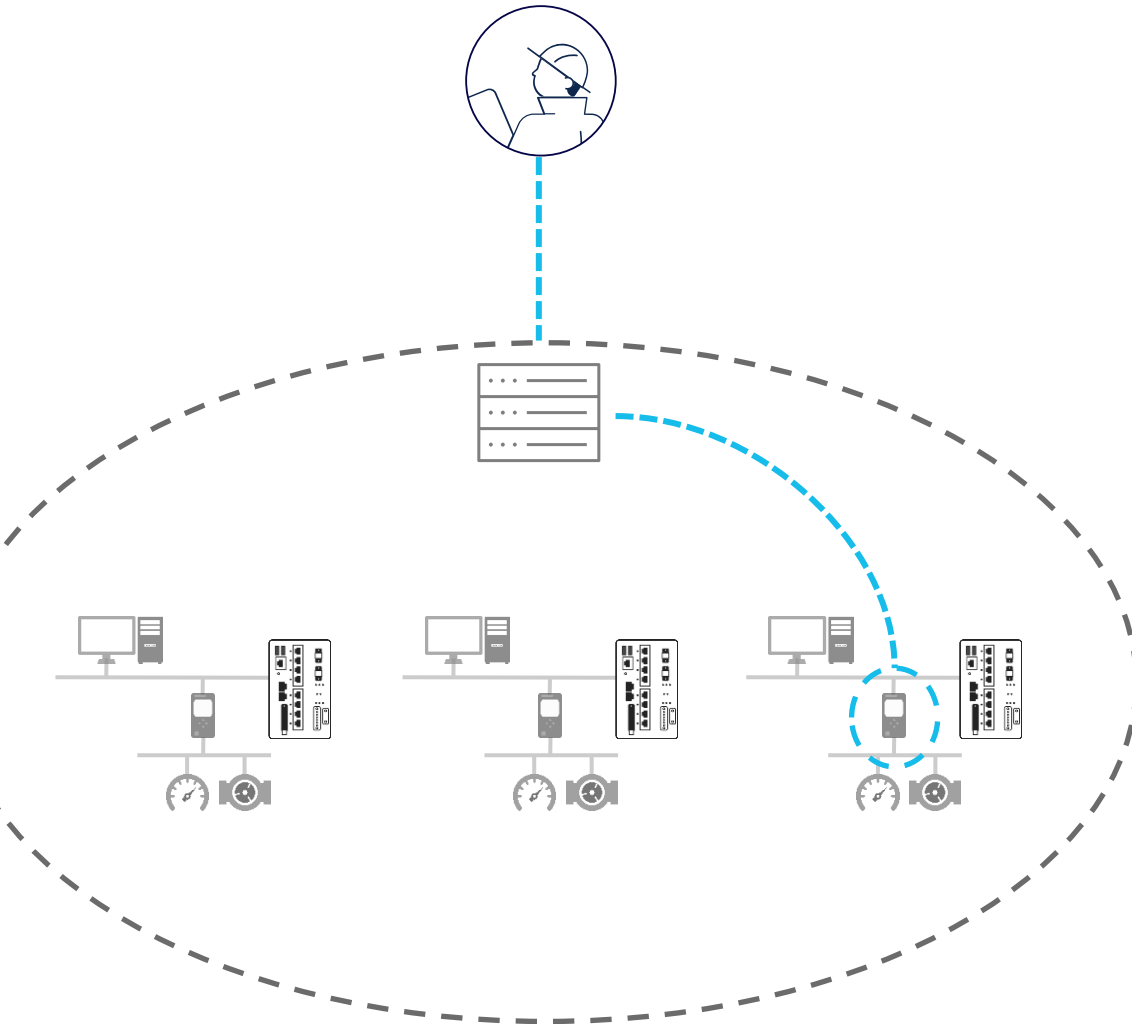
- Users have proxied access to specific endpoints / applications

Pros

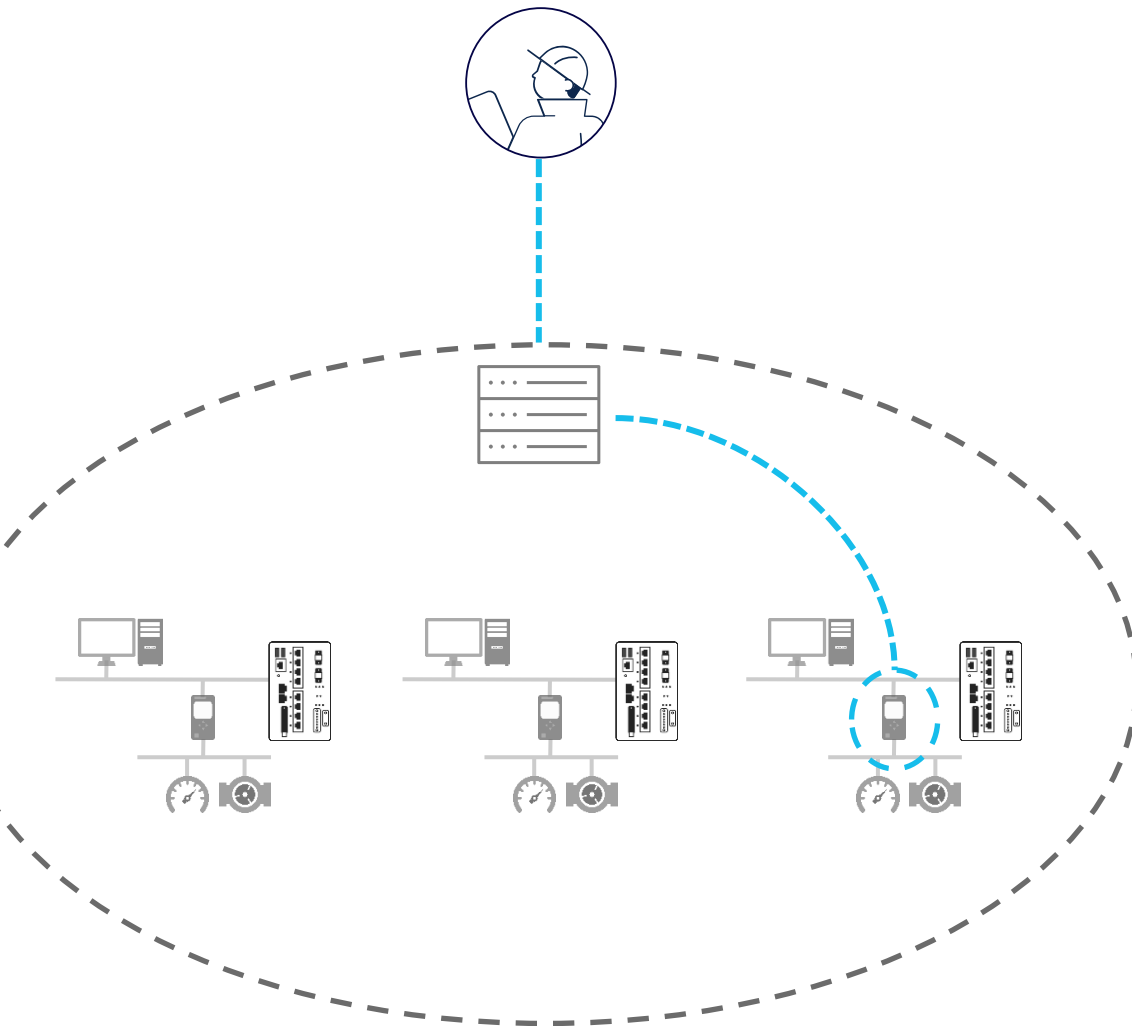
- Users only have access to what they need
- MFA is natively built in
- Clientless connectivity
- ZTNA gateway establishes outbound connection to a trusted cloud*

Cons

- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases



OT specific ZTNA capabilities



- ZTNA is a broad term, and needs capability extensions for OT

Pros

ZTNA+

- Scheduled Access
- Session Monitoring and Recording
- Session Approval flows

Cons

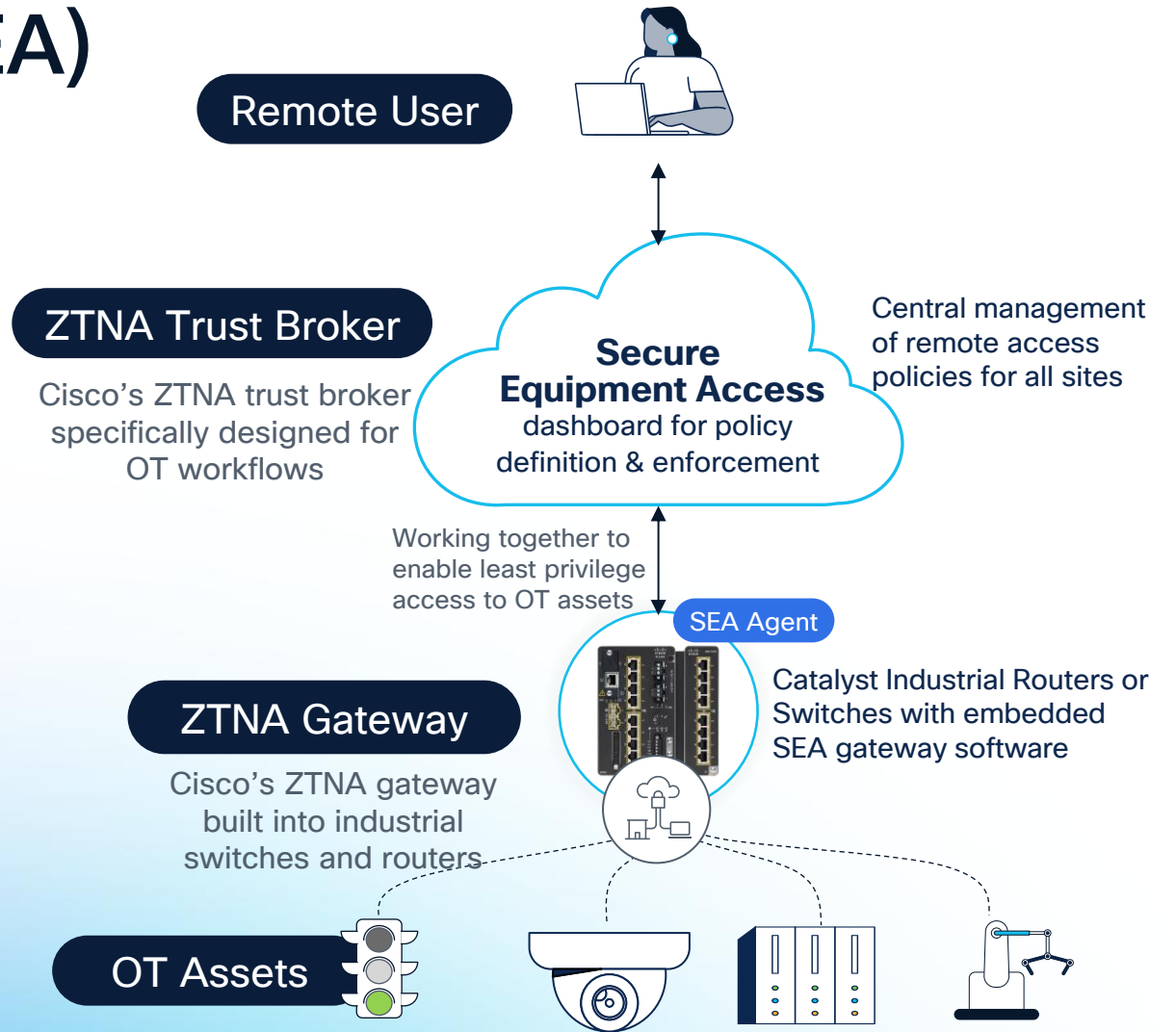
- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases

SEA overview

Secure Equipment Access (SEA)

Manage risks from suppliers with zero-trust remote access to OT assets

- ✓ Zero Trust MFA & SSO
- ✓ OT Asset Resource Isolation
- ✓ Clientless & Agent-based Access
- ✓ Remote User Host Posture Check
- ✓ Session Scheduling
- ✓ Session Recording, Monitoring & Kill
- ✓ Session Approval on Request



One-click **zero trust remote access to any OT asset** connected to Cisco industrial network

Platforms that support the SEA gateway

SEA Agent is the ZTNA gateway function embedded in network platforms

Industrial Routers



SEA Agent

IR1101



SEA Agent

IR1800

Industrial Switches

IE3500
IE3400
IE3300



SEA Agent

IE3500H
IE3400H



SEA Agent

IE3100



SEA Agent

IE3100H



SEA Agent



SEA Agent

IE9300

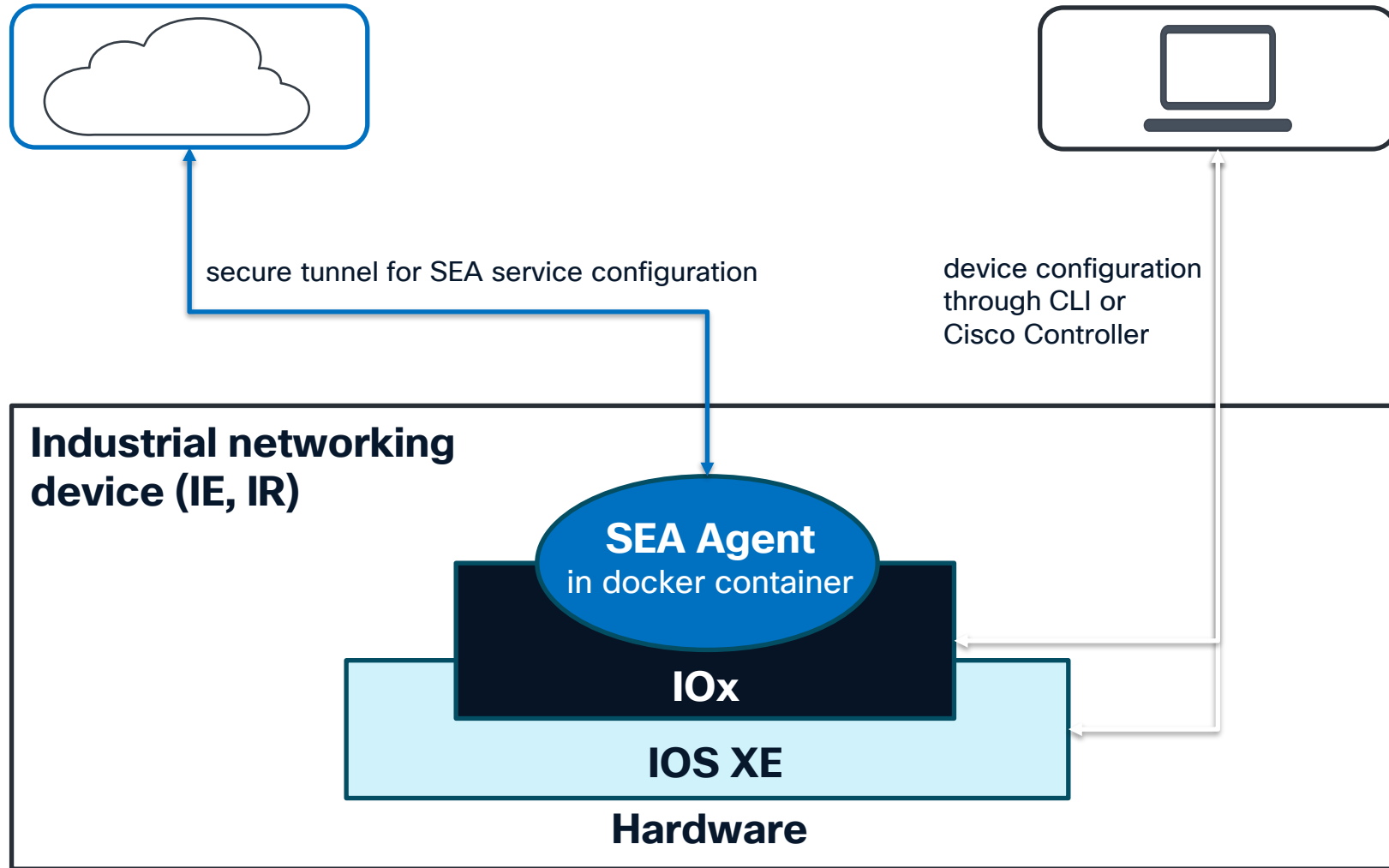
Enterprise Switches



SEA Agent

Catalyst 9300

One level deeper



SEA deployment examples and valuable product features

Customer 1: Sea port



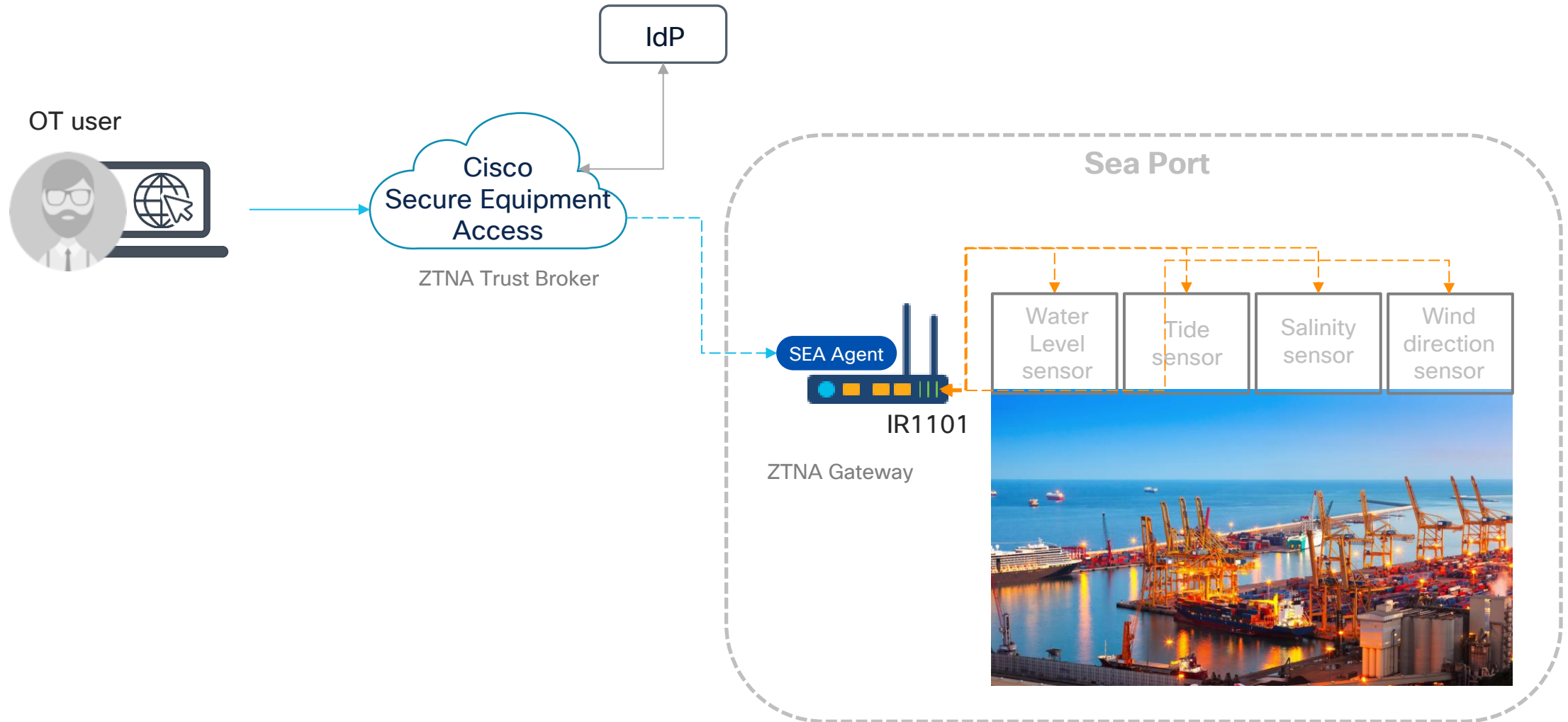
Sea port requirements for remote access

Goal: Secure remote access to assets in Sea port and on vessels. Secure collaboration with multiple partners through SSO

Requirements:

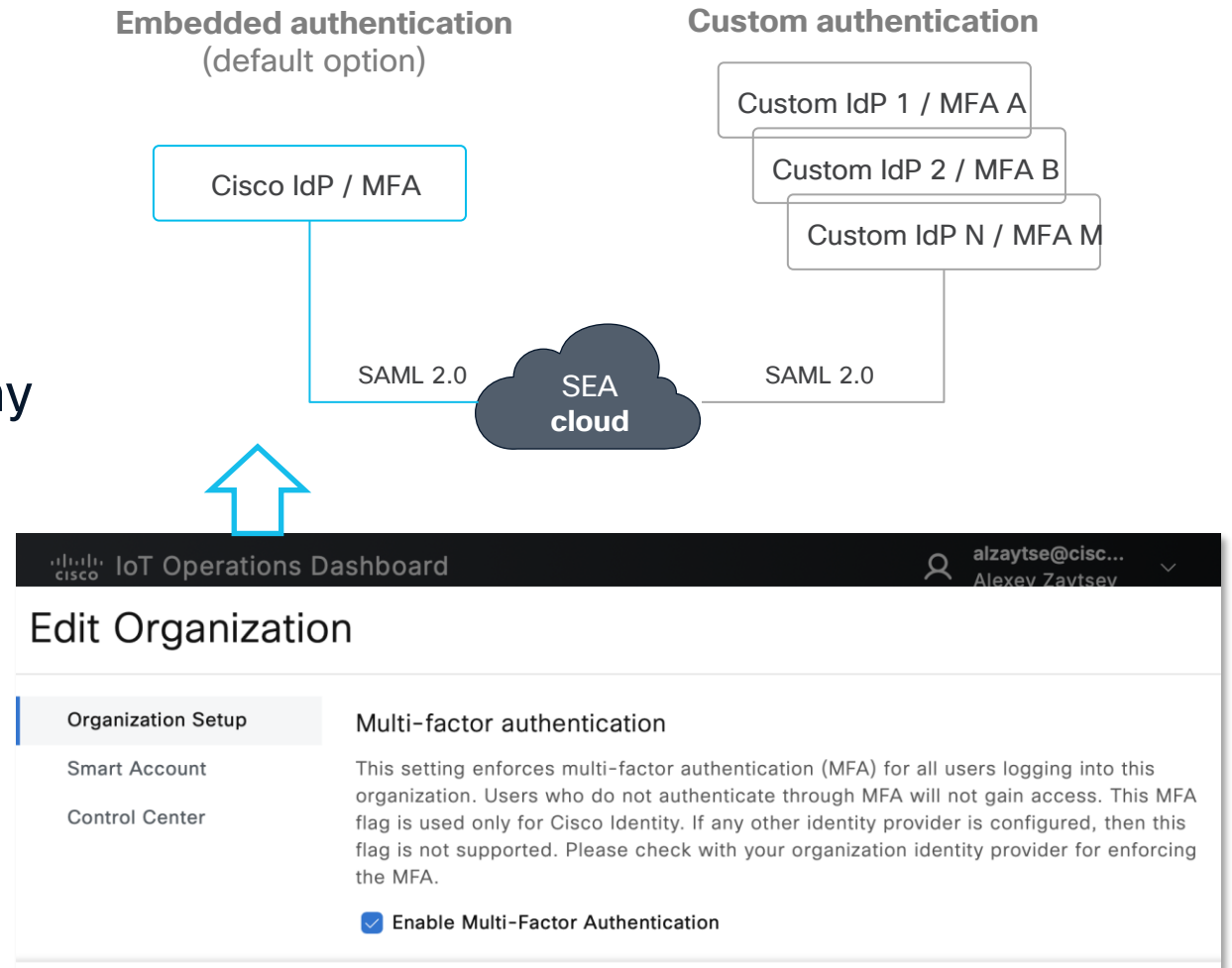
- Reliable remote access to port assets in harsh environment (sensors, cameras etc)
- RDP and SSH are main access methods
- SSO for authentication with multiple IdP support (several partners)
- Local authentication with MFA for quick addition of new users

SEA solution overview

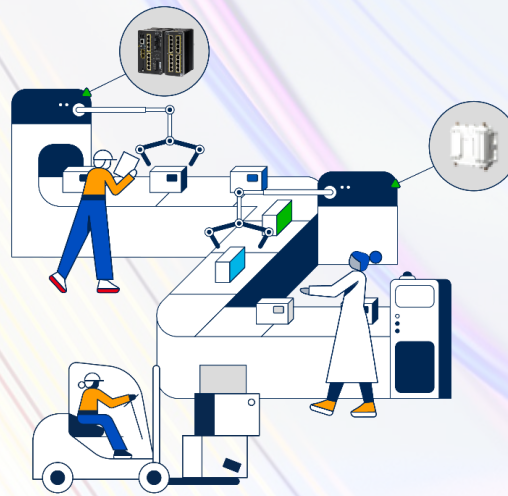


Embedded authentication and custom SSO in SEA

- Embedded authentication (id.cisco.com) with **MFA enforcement**. Authorization through RBAC in SEA.
- **Multi-IdP support** for SSO, per Org. Any IdP with SAML 2.0 support can be used. Any custom MFA beyond IdP is allowed.
- **IdP lock on the Org level**



Customer 2: Manufacturing



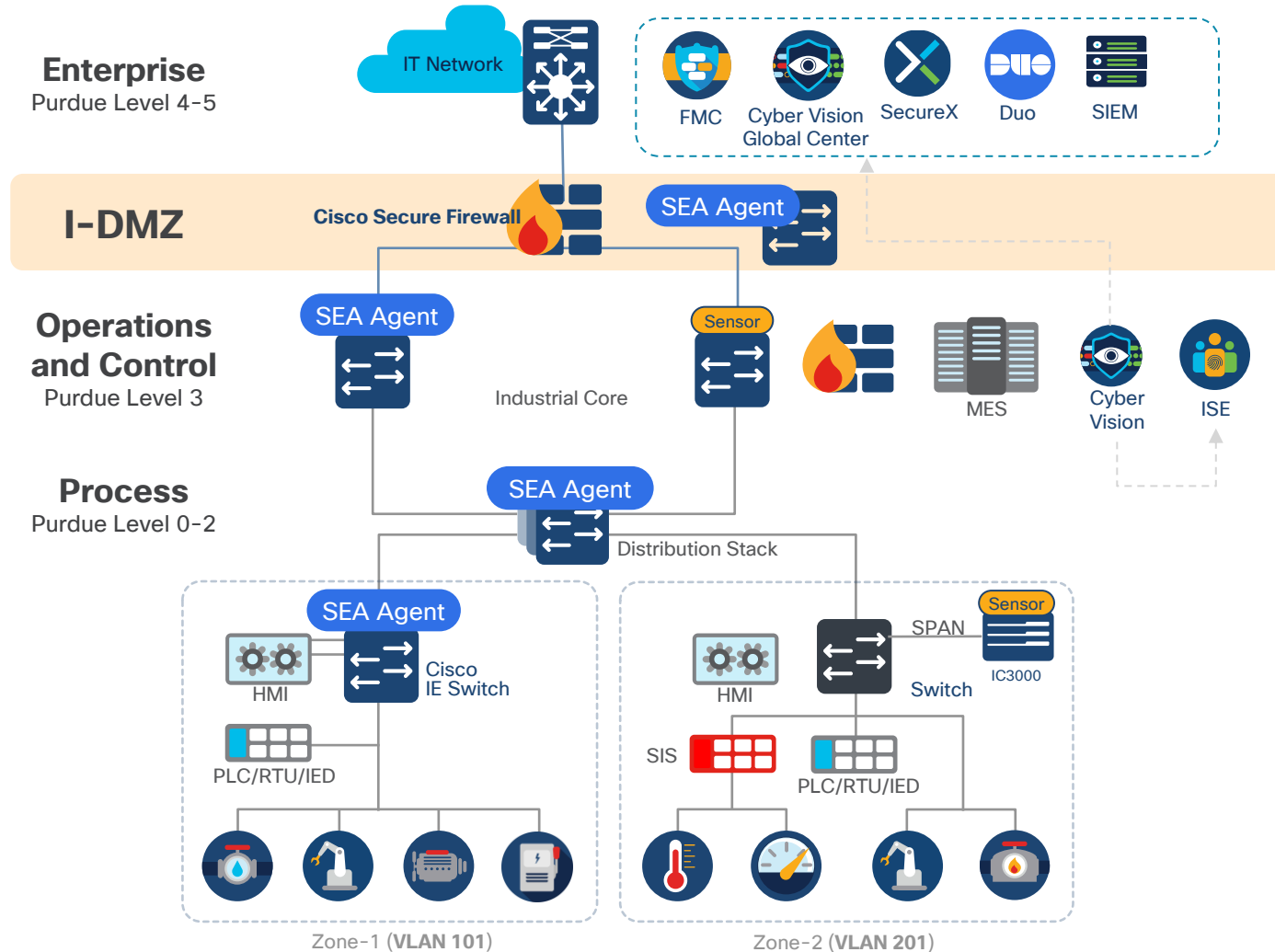
Manufacturing customer requirements for remote access

Goal: Secure remote access to assets on manufacturing plants for 3d party technicians and employees, adoption of Purdue model, services availability in segmented network

Requirements:

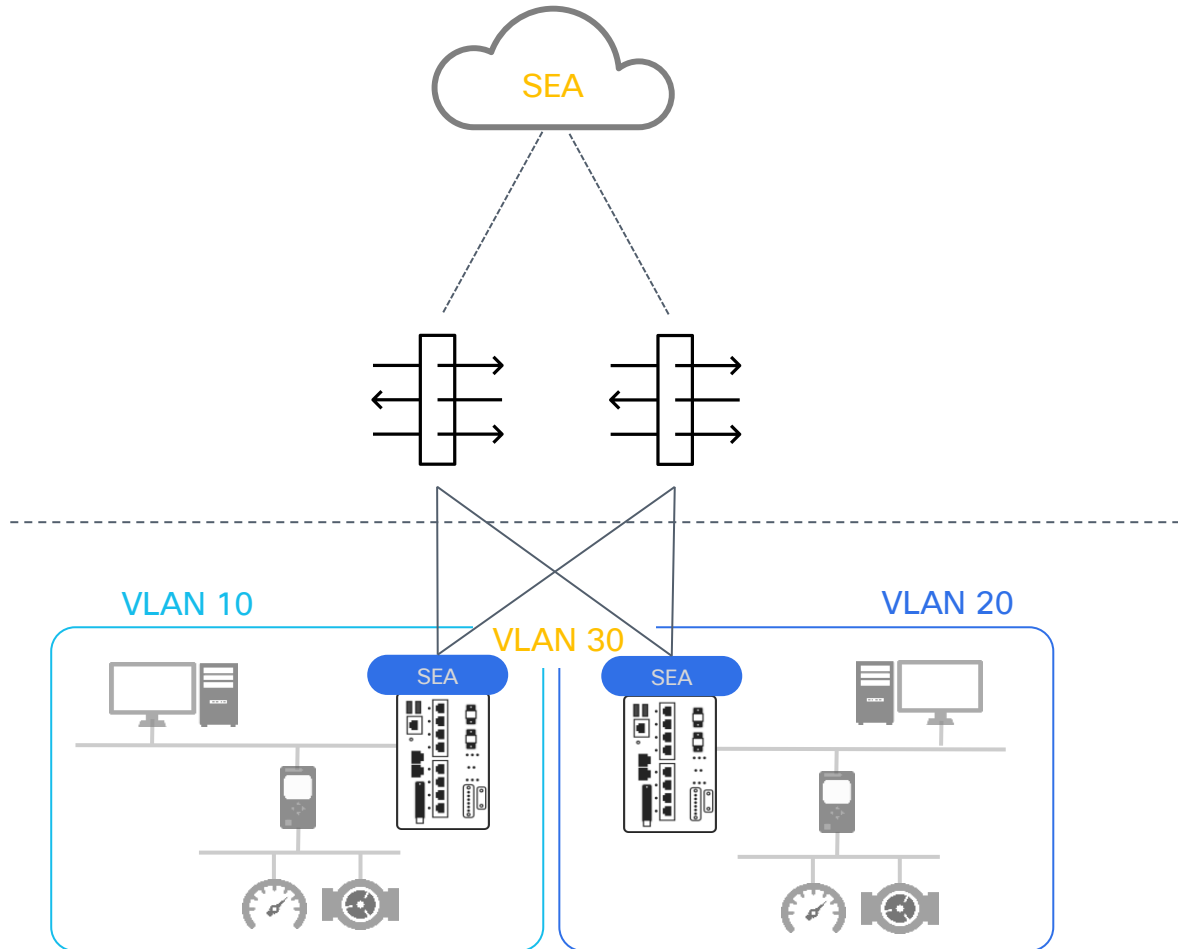
- Reliable remote access to industrial assets (PLCs, robots, workstations, HMIs, etc)
- RDP, WebApp, SSH, and SEA Plus are main access methods
- SEA Agent deployment can be on Purdue levels 0-3/3.5
- Remote access with network segmentation support through VLAN-awareness
- Simple and easy to follow deployment method required for SEA Agent

SEA Agent deployment flexibility. Purdue model



- SEA Agent deployed on a network device, can reach all end hosts if correct security rules are in place
- SEA Agent/s can be deployed on any Purdue level 0-3.5
- SEA Agent/s can be re-deployed to a different layer or hosting device in any moment
- SEA Agent establishes outbound tunnel to SEA cloud

Multi VLAN support. VLAN-aware deployment



- If SEA Agent is **on different VLAN**, it must find a routing point to reach asset
- SEA Agent now **supports multiple interfaces**
 - Up to 10 interfaces supported
- Both **DHCP and Static IP** supported

Add Network Device

Remote access enables you to onboard your remote users. For more information, see [Remote access documentation](#).

✓ Network Device Setup

2 Advanced Configuration

3 Deployment

VLAN

Management Interface ⓘ

VLAN ID *

IP Assignment *

Dynamic IP

Additional VLANs

☒ Enable Additional VLAN Configurations

Add up to 9 Additional VLANs ⓘ

+ Add VLAN

Delete

☐

VLAN ID

IP Assignment

☐

VLAN ID *

IP Assignment

Dynamic IP

☐

VLAN ID *

IP Assignment

Dynamic IP

SEA Agent deployment through guided CLI deployment flow

- Expanded capability for deployment via CLI on Cat9300 (and on IE3400/3300/93xx)
- CLI commands automatically generated for admin's review during the 'add network device' flow
- Step-by-step guidance for adding the generated CLI

The screenshot displays the Cisco IoT Operations Dashboard with the 'Add Network Device' workflow. The main interface shows three steps: Network Device Setup, Advanced Configuration, and Deployment. The 'Deployment' step is active, displaying generated CLI commands for enabling IOx and configuring VLAN, Proxy, and Runtime Options. A modal window titled 'Add Network Device' is overlaid, showing the 'Network Device Setup' step with fields for Selection Method (CLI Deployment), Network Device Name, Client ID, and Network Device Type.

Add Network Device

Remote access enables you to onboard your remote users. For more information, see [Remote access](#).

Network Device Setup

Selection Method: CLI Deployment

CLI Enrollment allows you to add Network Device.

Network Device Name *

Client ID

Network Device Type *
Select Network Device Type

Deployment

Copy the IOS commands below to the console on Network Device 'Paint Shop Line 1'. These commands are suggestions for downloading, installing, configuring, and running SEA on 'Paint Shop Line 1', although in some cases, additional manual configuration may be necessary in order to fully onboard the device.

Step 1

Enable IOx for application hosting.

```
config term
iox
exit
```

Step 2

Configure VLAN, Proxy, and Runtime Options. Download SEA agent application binary.

```
config term
vian 4094
interface AppGigabitEthernet1/0/1
switchport trunk native vian 4094
switchport trunk allowed vian add 1
switchport mode trunk
! Uncomment the command below to enable app signature verification.
! Note that this action may affect other IOX applications on the device.
! app-hosting signed-verification
no app-hosting appid SEA_agent_amd64_linux
app-hosting appid SEA_agent_amd64_linux
app-vnic AppGigabitEthernet trunk
vian 1 guest-interface 0
app-resource docker
```

[Exit](#) [Close](#)

SEA Alerts for detecting threats from remote users

New **rule-based Alerts framework** to trigger alerts such as:

- User A has **logged in from a prohibited location**
- Since their last login, User B has **changed login locations**
- User C is **logging in outside of working hours**

The screenshot displays the 'Alerts' dashboard. At the top, it shows 'Alerts 3' with a red warning icon, a 'Refresh' button, and the timestamp 'As of May 11, 2025 10:17 AM'. Below this, there are tabs for 'Active 3', 'Muted 1', and 'Cleared 1'. A summary bar shows '1 Critical' (red icon), '1 High' (orange icon), '1 Medium' (yellow icon), and '0 Low' (green icon). The main section features a search bar, '0 selected' status, and 'Clear' and 'Mute' buttons. A table lists the active alerts:

☐ Alert Type	Trigger	Instances	Category	Last Detected	Severity
☐ Login from prohibited location	China	2	User activity	May 10, 2025 10:30 AM	Critical
☐ Changed login location	user@email.com	1	User activity	May 7, 2025 11:03 AM	Medium
☐ Login outside of working hours	user@email.com	1	User activity	May 4, 2025 9:15 PM	High

At the bottom right, there is a 'Rows per page' dropdown set to '30', showing '1-12 of 12' items, and a pagination control with '1' selected.

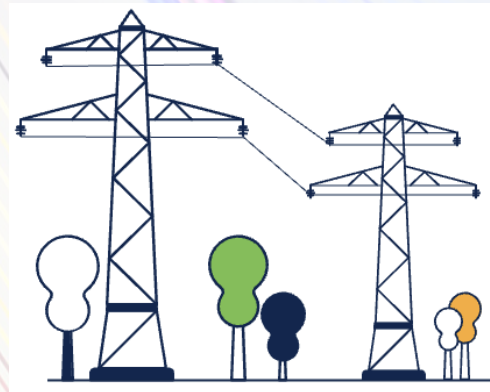
Identity threat detection and response (ITDR) focuses on identifying anomalies in human behavior, detecting potential unauthorized access, and responding to security incidents promptly.

Deactivating inactive user accounts

The screenshot displays the Cisco IoT Operations Dashboard. The top navigation bar includes the Cisco logo, 'IoT Operations Dashboard', and a user profile for 'Alexander Business Corp, Inc'. The left sidebar contains navigation links: 'Service Secure Equipment Access', 'Dashboard', 'Remote Sessions', 'Access Management' (highlighted), 'System Management', and 'Quick Wizard'. The main content area is titled 'Users' and shows details for 'blockeduser@email.com'. The user is marked as 'Blocked' with a red star icon. Below this, there are buttons for 'Unblock' and 'Edit expiration'. The 'User details' section lists the role as 'Remote User', the last remote access as 'Jun 5, 2024 10:30 AM', and the access expiration as 'Expired' with a yellow warning triangle. The 'Recent login metrics' section shows the device type as 'Mac', the browser as 'Firefox', the location as 'America/Los Angeles', and the last login as 'Jun 1, 2023 9:25 AM'. The 'Asset access' section shows '0 Assets accessible by this user while blocked', '10 No longer accessible', '1 Accessed in last 30 days', and '0 With unrestricted SEA Plus protocols'. The 'Remote session history' section shows '1' session. The 'Access control groups' section shows '2 Enabled groups' and '0 Disabled groups'.

- **Block remote users** due to inactivity – e.g., disgruntled ex-employee can exploit unrevoked access
- Dormant user accounts are a major vector for identity-based attacks = e.g., Unused 3rd party contractor account due to contract completion
- SEA admin can **set access expiration** time-to-live based on roles*

Customer 3: Utility



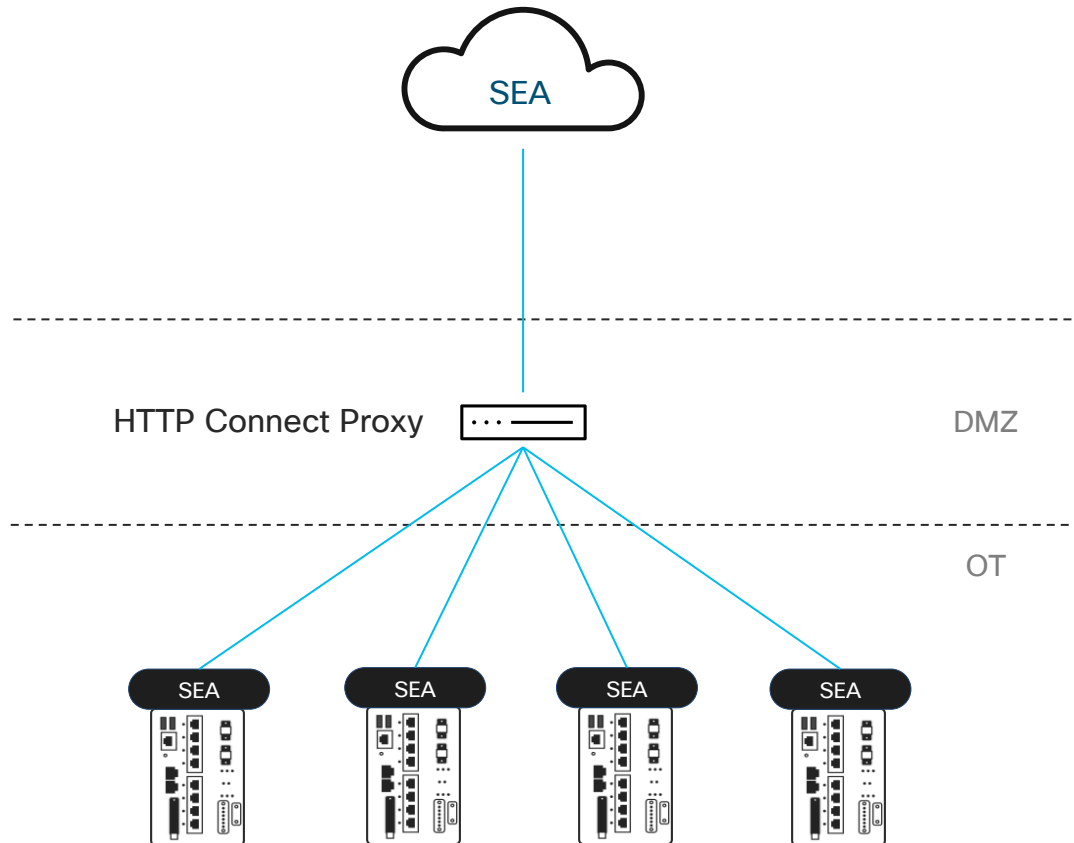
Utility customer requirements for remote access

Goal: Secure remote access to assets on virtualized electrical substations of the national power grid

Requirements:

- Reliable remote access to industrial assets (PLCs, HMIs, workstations, jump boxes, etc)
- SEA Plus, RDP, and WebApp are main access methods
- HTTP Connect Proxy support
- OT environment isolation into purposely designed islands with particular people and particular assets only
- Customer wants their subject matter experts to be between contractors and their assets with ability to approve access

HTTP Connect Proxy support for SEA tunnels



HTTP Connect Proxy

☒ Enable HTTP Connect Proxy

Choose an HTTP Connect Proxy Configuration Mode ⓘ

☐ Proxy URL ☒ Proxy Form

Enter the following information to enable Secure Equipment Access to the Connected Clients

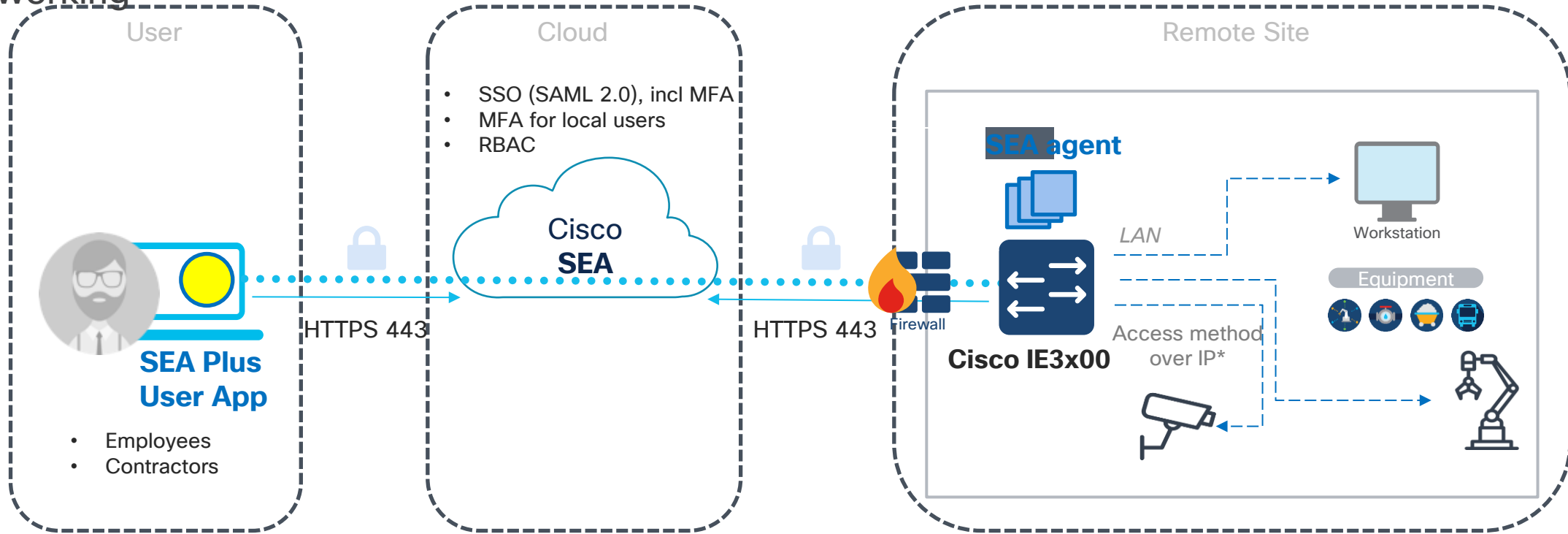
Server *	Port *
<input type="text" value="http://"/>	<input type="text"/>
Username	Password
<input type="text"/>	<input type="text"/>

- SEA Agent **can now connect to cloud via HTTP Connect Proxy**
- **SEA Agents in OT network can aggregate into a DMZ area** for reaching the cloud
- Note: The HTTP Connect Proxy is not a Cisco product or an extension of SEA. It's a capability that exists on web proxies.
- A HTTP Connect Proxy does not decrypt traffic. Encryption is maintained end-to-end between agent and cloud.

SEA Plus access method for PLC management

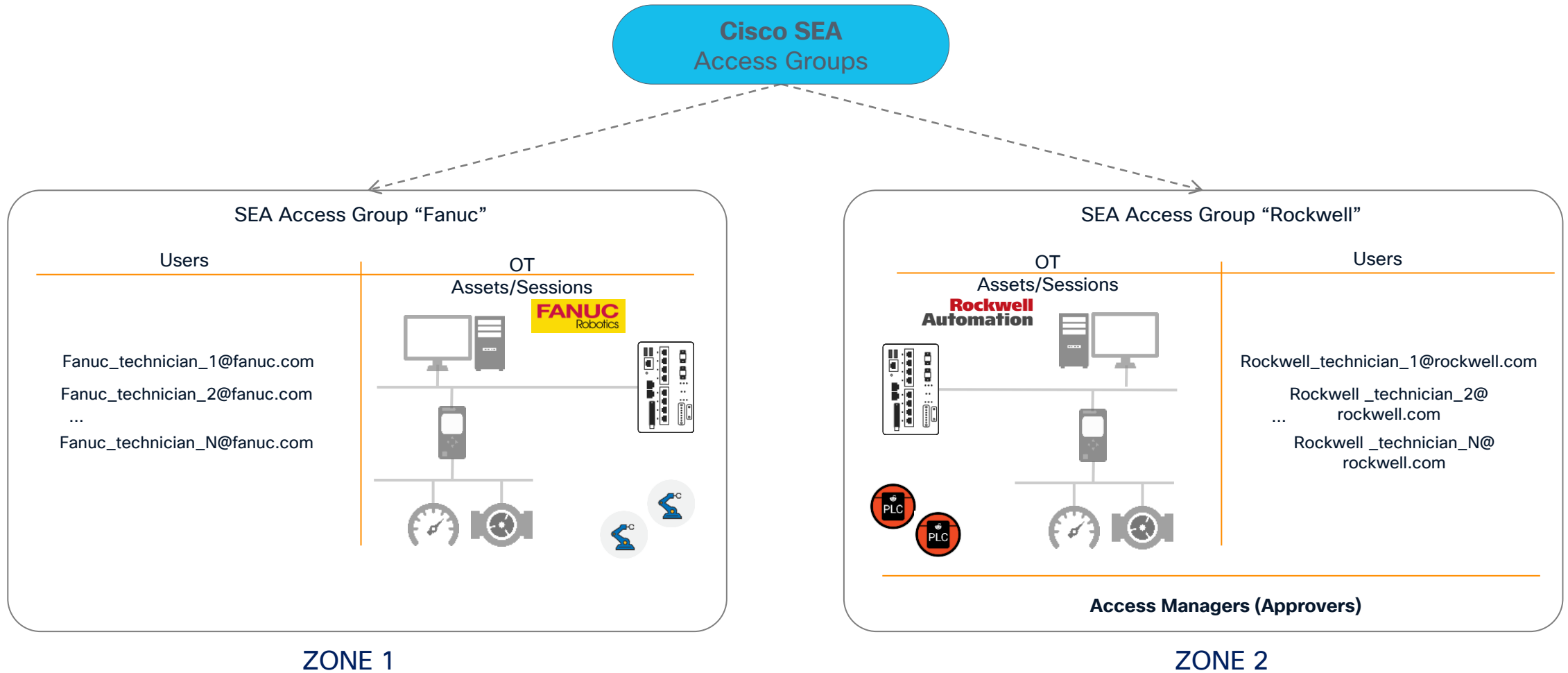
Agent-based secure remote access – SEA Plus.
Other VPN clients should be inactive while this app is working

Ability to configure any port for communications decreases attack surface and increases the security posture of the solution!



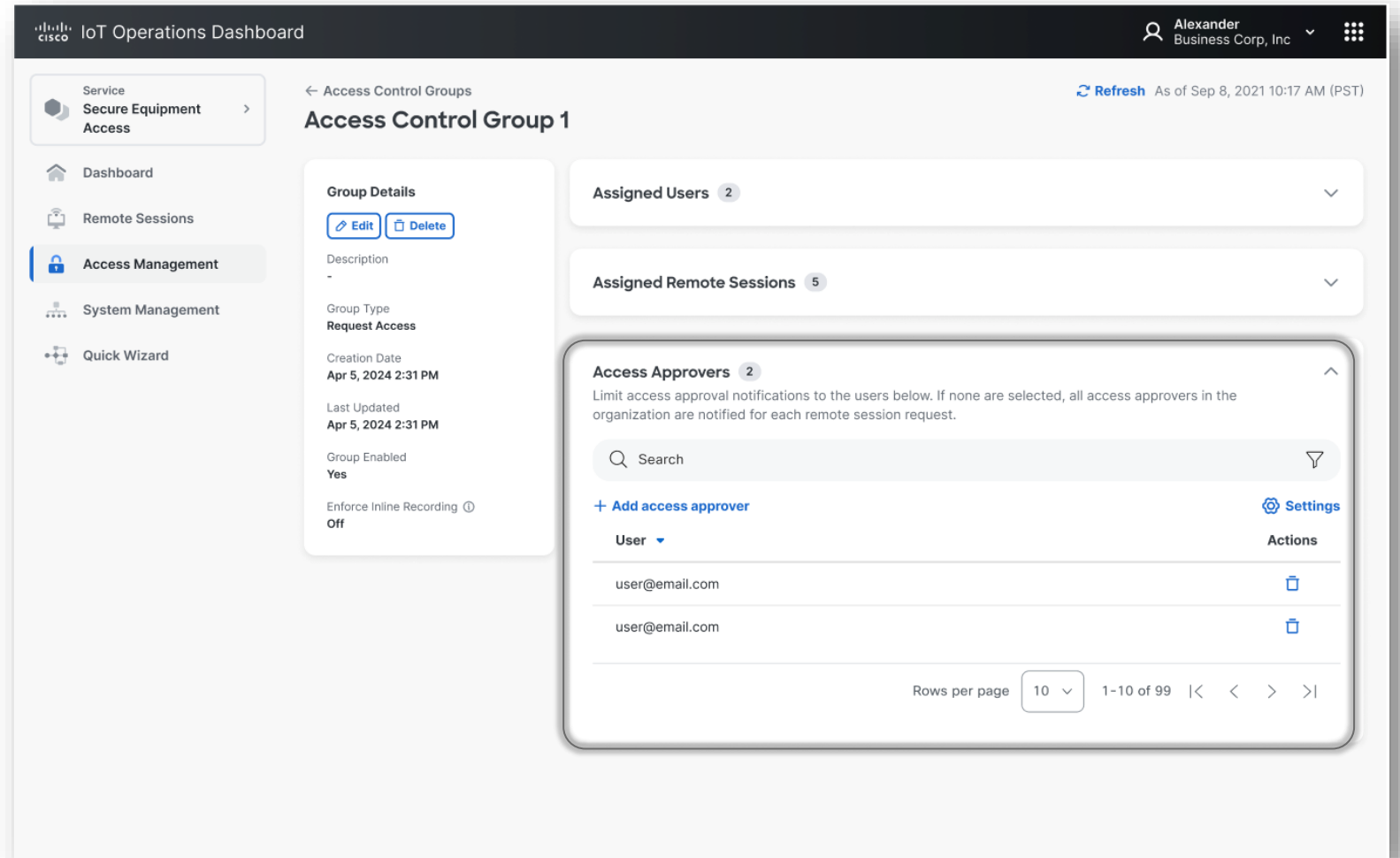
SEA Plus technology allows applications running on a user's computer to communicate with a remote system using any TCP, UDP, and ICMP protocols and for communication between a user and a remote system.

OT assets isolation and secure operations



SEA session access request/approval feature

- Just-in-time access functionality to enforce strict access to remote sessions
- Add privileged users who can approve session requests to access group
- Privileged users will only see requests corresponding to the access control groups associated to the approval group



Key takeaways

- Additional exposure to poorly implemented remote access solutions
- The threat of identity is at an all time high
- SEA provides both the flexibility and ease of use required for OT while being secure from the start
- Your remote solution should not only provide connectivity, but it should also provide security insights for your remote user activity
- Just in time access is key to remotely accessing the critical infrastructure

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

