# Cisco Secure Equipment Access

BDM Overview

July 2025

# Remote access to OT assets is key for operations

## Maintenance

Remote configuration and maintenance by vendors and third-party technicians.

## Troubleshooting

Remote experts helping quickly solve issues to maintain production uptime.

## Avoiding Truck Rolls

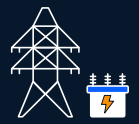
Large sites, distributed operations, limited resources. Remote access helps lower OpEx.

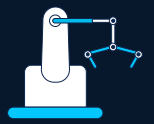

Roadways


Transportation


Renewables


EV chargers


Utilities


Manufacturing


Oil & Gas


Mining


Ports

Operations need remote access to all assets at anytime, for internal and external experts

# Who can you really trust?

**Identity Risks**
You can't be certain who is actually connecting.

**Trust Issues**
You can't trust the remote user to not mess around.

**Ownership Issues**
You can't ask the OT staff to control remote users.

**Scale and Cost Issues**
You have so many contractors and assets. Poor management is a risk.

Securing remote access is critical to protect industrial operations

# Existing options are either security backdoors or come with many trade-offs

## Ad-Hoc Software

Often installed on operator workstations

Backdoor to IT security policies

## Cellular Gateways

Dedicated hardware installed by machine builders

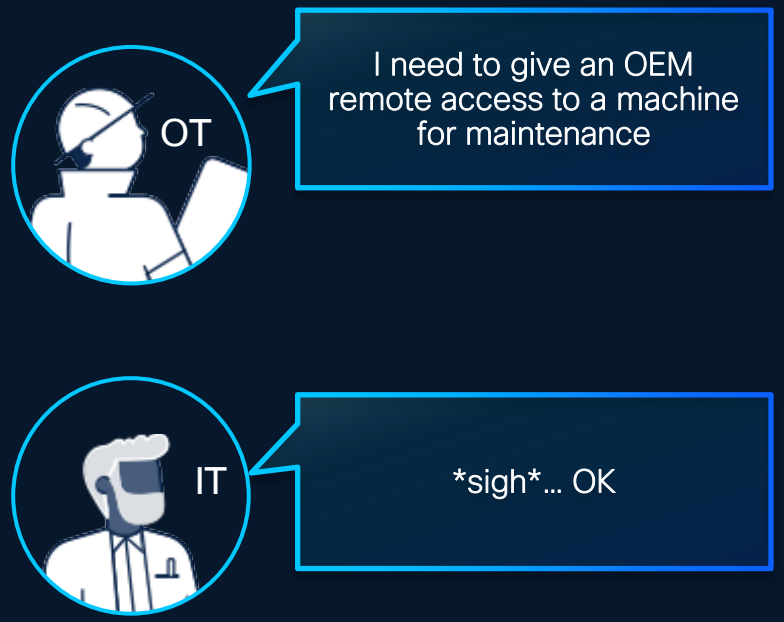
Backdoor to IT security policies

## VPN

Always-On, All-or-Nothing access

Need additional controls to deny full network access

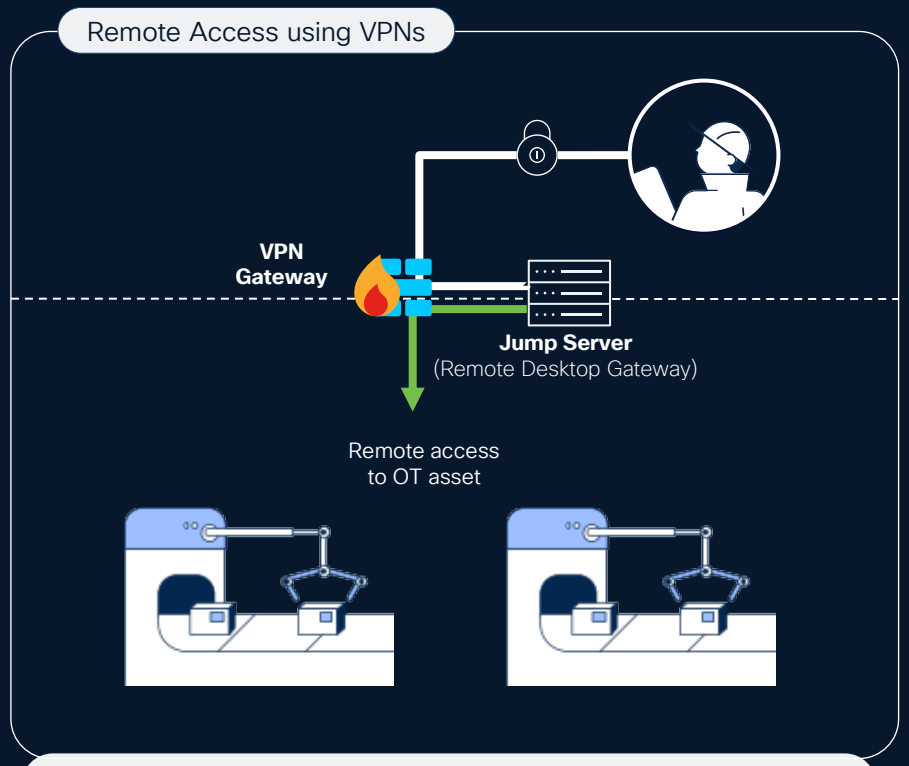
# “Secure” remote access typically means user frustration with cumbersome experiences




- 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 you to grant remote access?

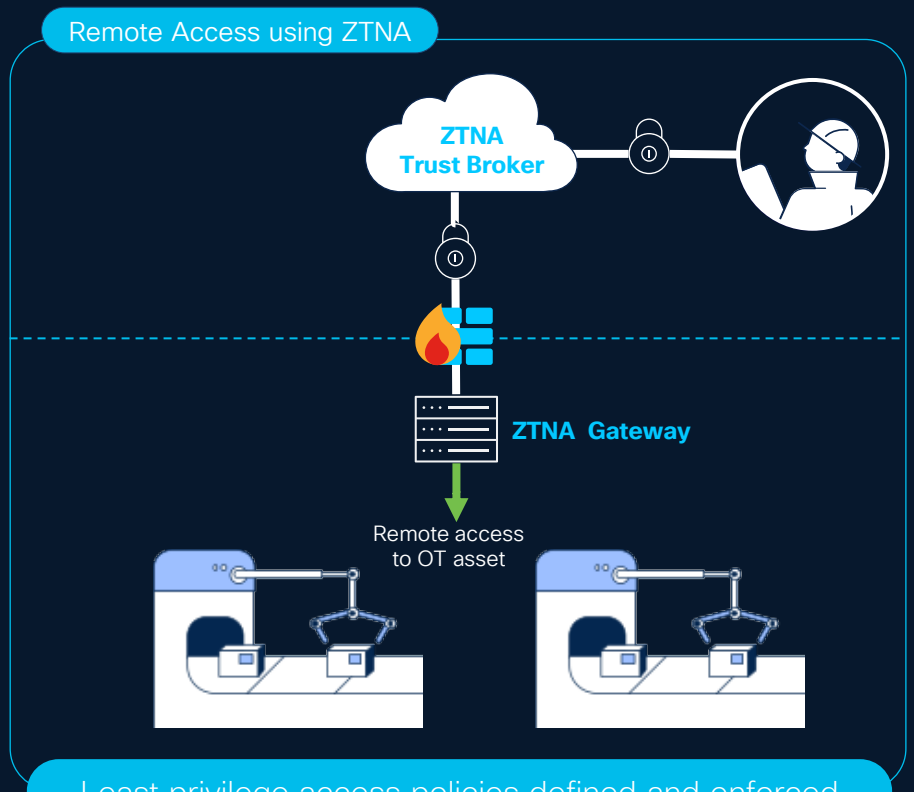
# Zero-Trust Network Access (ZTNA) simplifies enforcing secure remote accesses in industrial settings




Always-on solutions with all-or-nothing access

Least privilege access policies hard to enforce

Requires IT experts to configure and maintain




Least privilege access policies defined and enforced centrally for all sites in the ZTNA trust broker

Gateway establishes an outbound connection to the ZTNA broker simplifying deployment at scale

# Zero Trust Network Access (ZTNA) for OT Assets

The next generation remote access architecture

> ZTNA provides controlled **identity and context-aware** access to resources. It starts with a **default deny** posture and **adaptively offers the appropriate trust** required at the time. A **trust broker** mediates connections between applications and users. The result **reduces risk** and offers **more flexible and responsive** ways to connect and collaborate.

Gartner®

Market Guide for Zero Trust Network Access

- Least privilege access
- Assets hidden from discovery
- No lateral movement possible
- Device posture compliance
- Time/date restricted access
- Reduced attack surface
- More flexible and responsive

# Cisco Secure Equipment Access

## OT self service remote access with ZTNA control

### Zero-Trust Security Controls

MFA, posture check, just-in-time access
Deny by default, least-privilege access

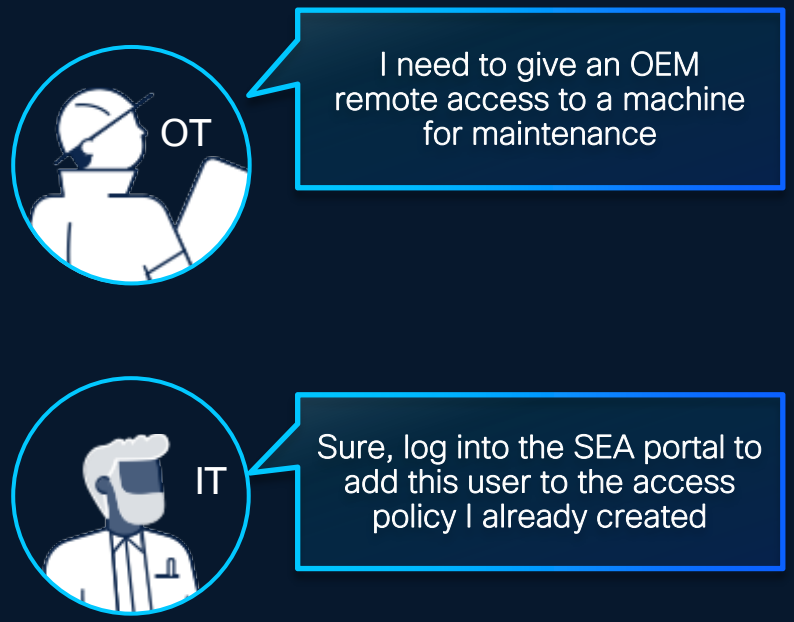
### Threat Detection and Monitoring

Identity anomaly detection
Session monitoring and recording

### Easy to Deploy and Manage at Scale

Centralized policy definition and enforcement
Network-embedded gateway

# OT Self-Service Remote Access




## IT controls security policy

Ensure all remote access sessions comply with security rules such as MFA, session recoding, schedules, and more

## OT grants access to asset when needed

Give the line of business the flexibility to manage users and assets to streamline operations and maintain uptime

Give OT the tools to run operations and eliminate shadow IT options

# Zero-Trust Security Controls

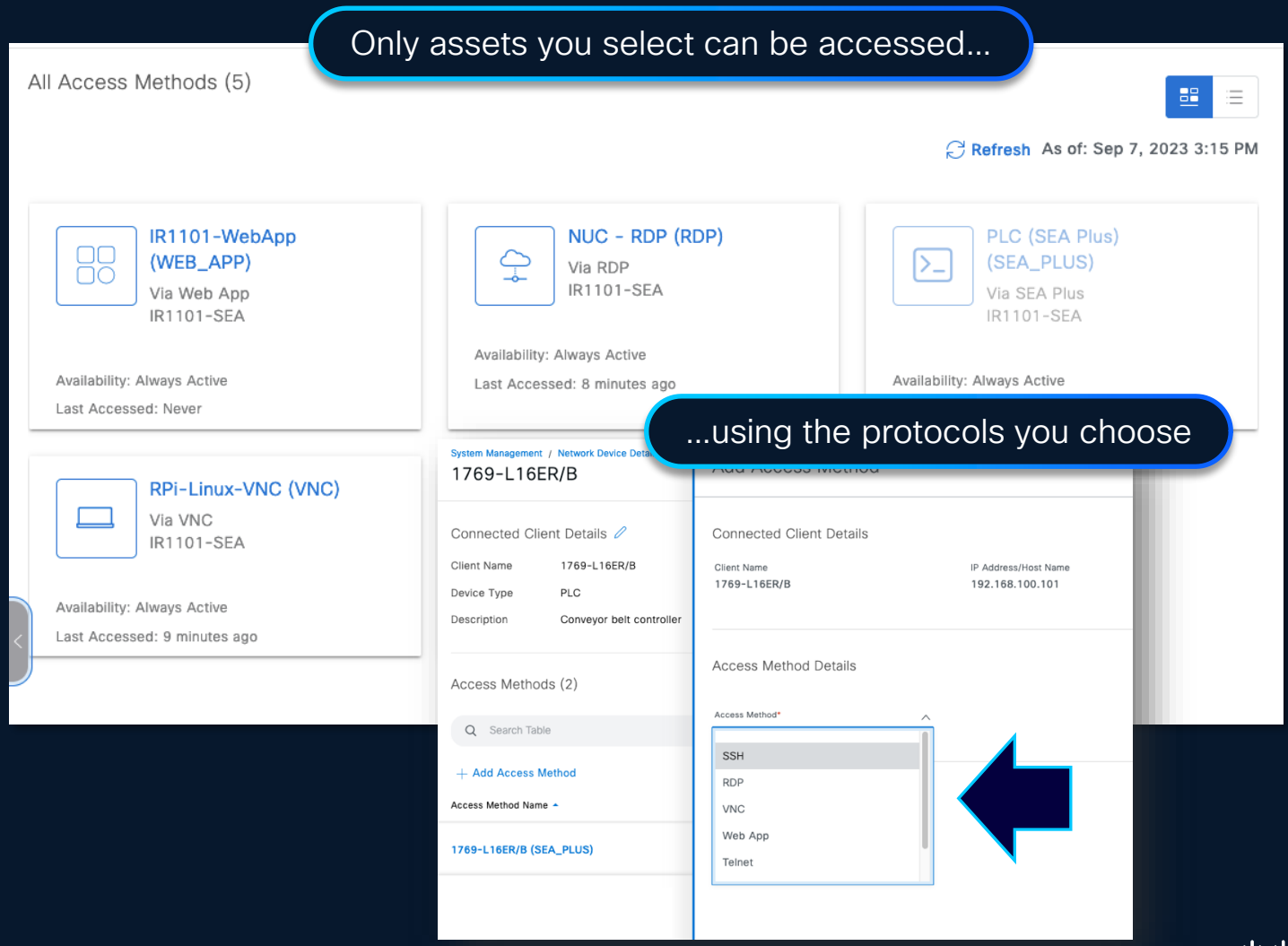
## Ensure only trusted users can connect and when.

- Verify user identities with MFA and SSO, integrating with your IdP
- Prevent malware intrusion by verifying compliance of remote user's computers using Cisco Duo
- Enforce schedules to allow access only at time of need

# Least Privilege Access Controls

## Never expose your entire network and prevent lateral movement.

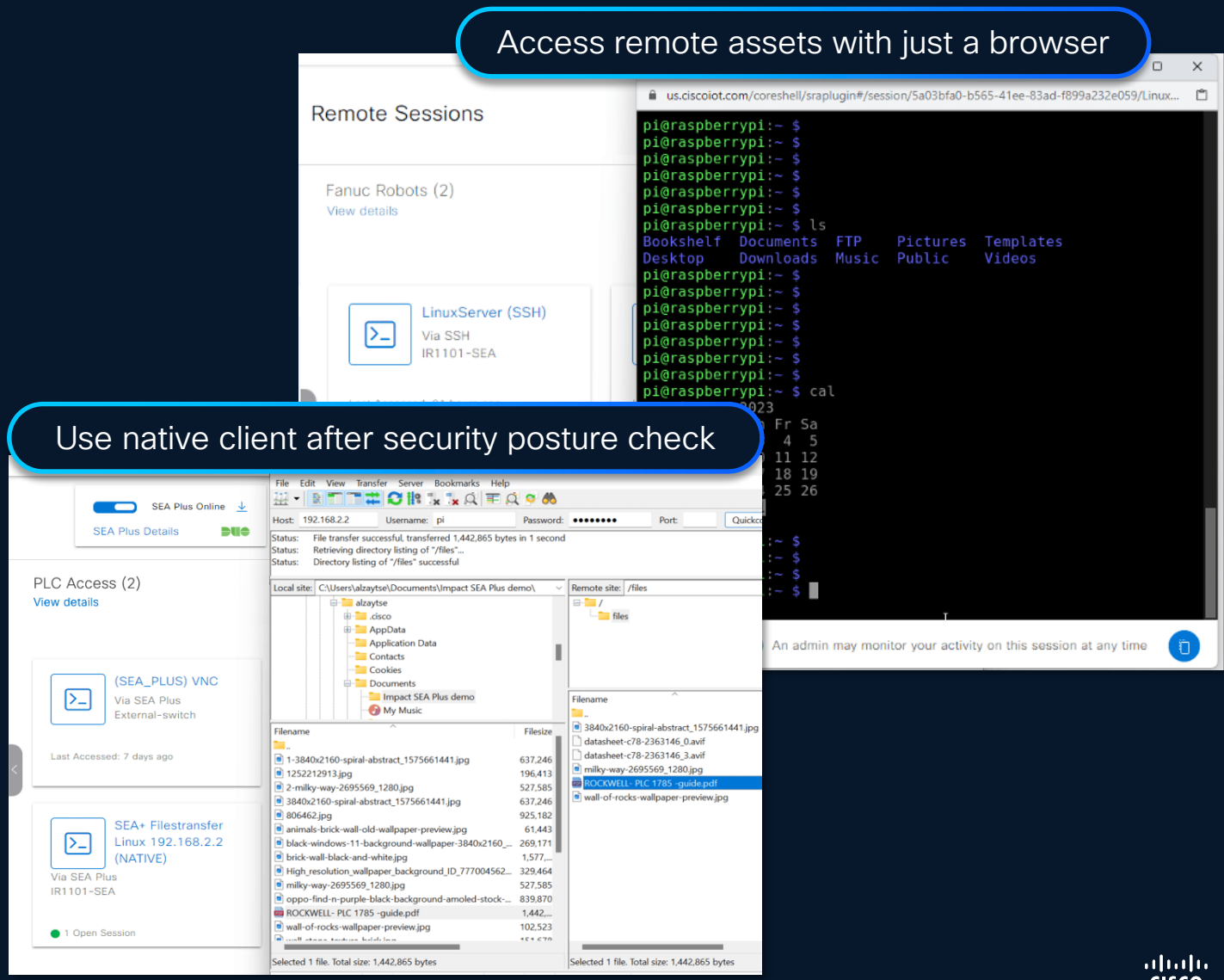
- Only assets you specify can be accessed by the remote users you choose
- Using only the protocols allowed
- Only on the days and times allowed



# Clientless and Agent-based Access

## Get total control of how users can access assets while offering flexibility and ease of use.

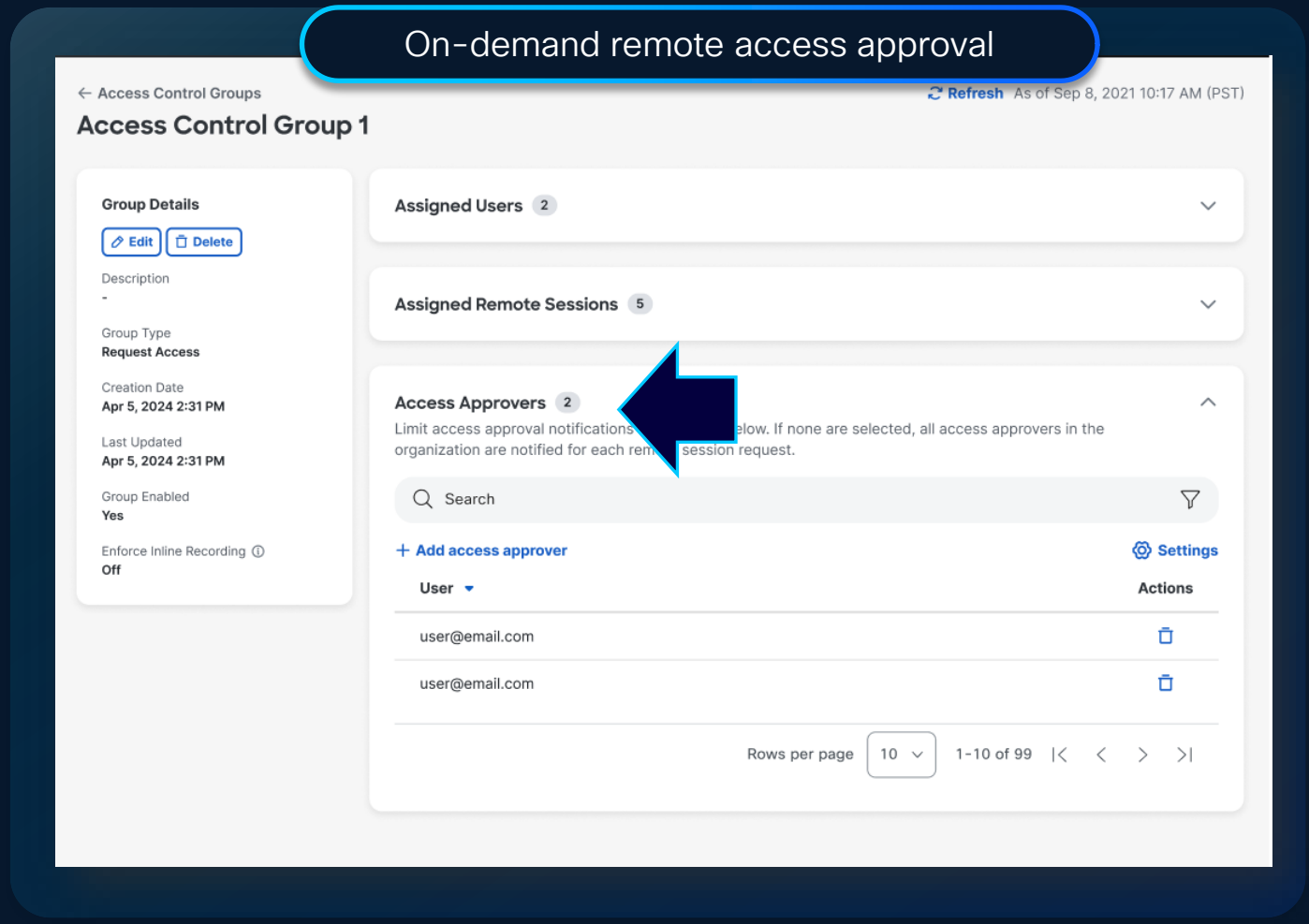
- Clientless: Users only need a browser to access remote assets using RDP, VNC, SSH, Telnet or HTTP(S)
- Agent-based: Use native desktop clients for advanced tasks, only once computer has been verified for compliance with health policies



# OT Self-Service: On-Demand Remote Access

## Help OT teams seamlessly drive operations with contractors while maintaining controls

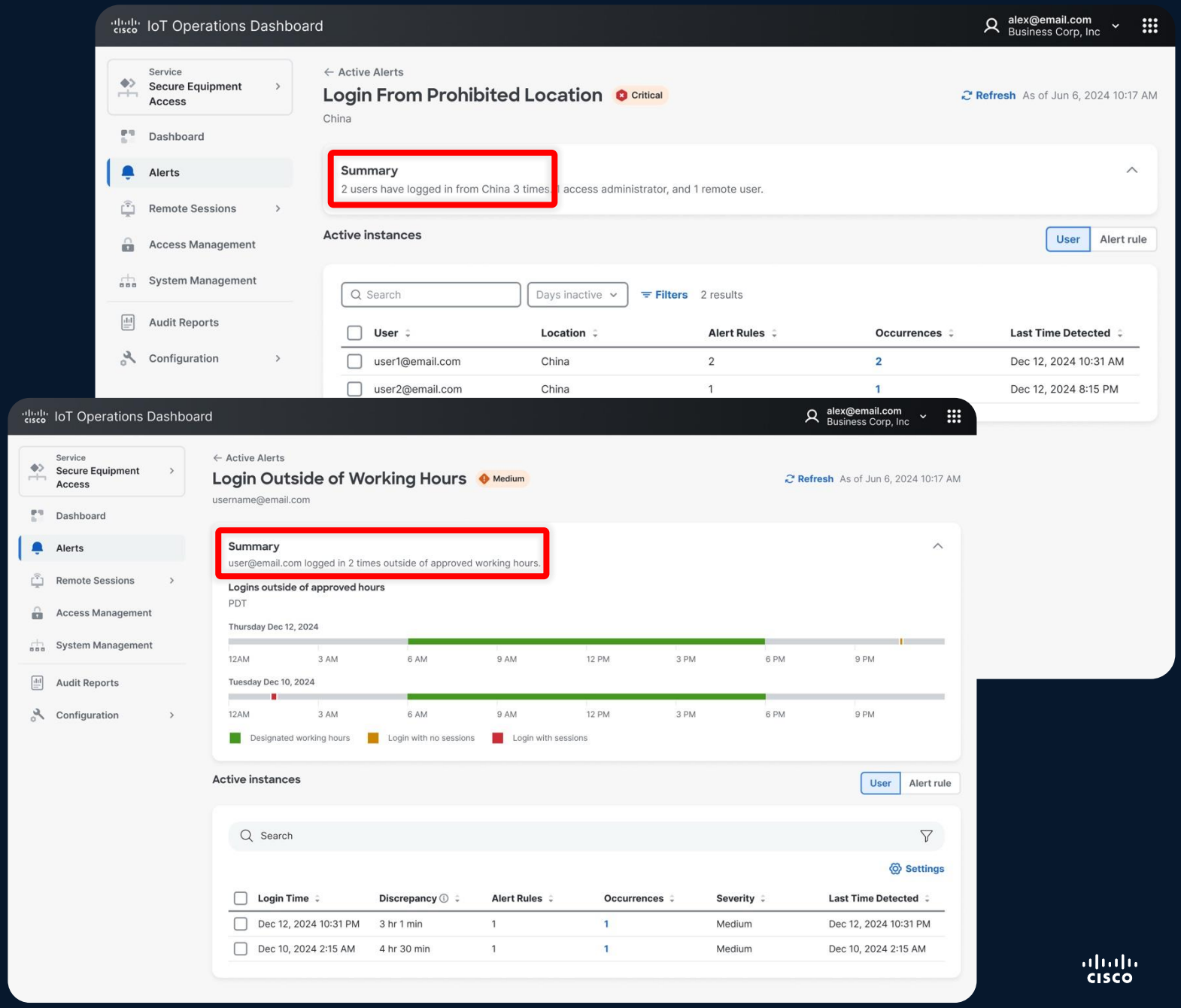
- Remote users can request access when they need it. No need to preconfigure ever changing users
- Privileged users receive email notifications and can grant access on-demand



# Remote User Identity Threat Detection

## Detect threats related to remote user identity

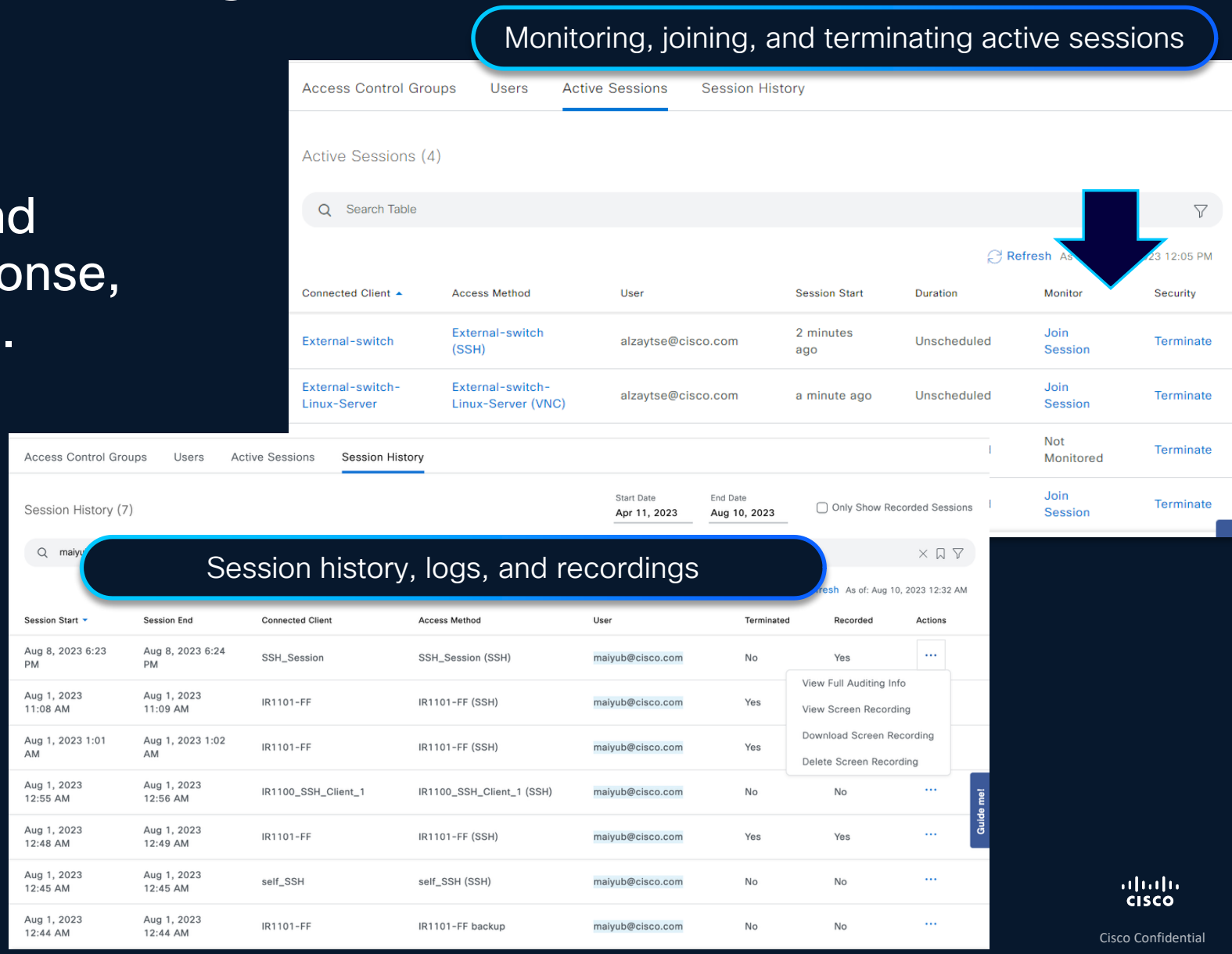
- Login from unapproved geolocation
- Login outside working hours
- Auto deactivation of unused accounts



# Session Recording, Monitoring, and Termination

## Real-time visibility on active and past sessions for incident response, investigations, and compliance.

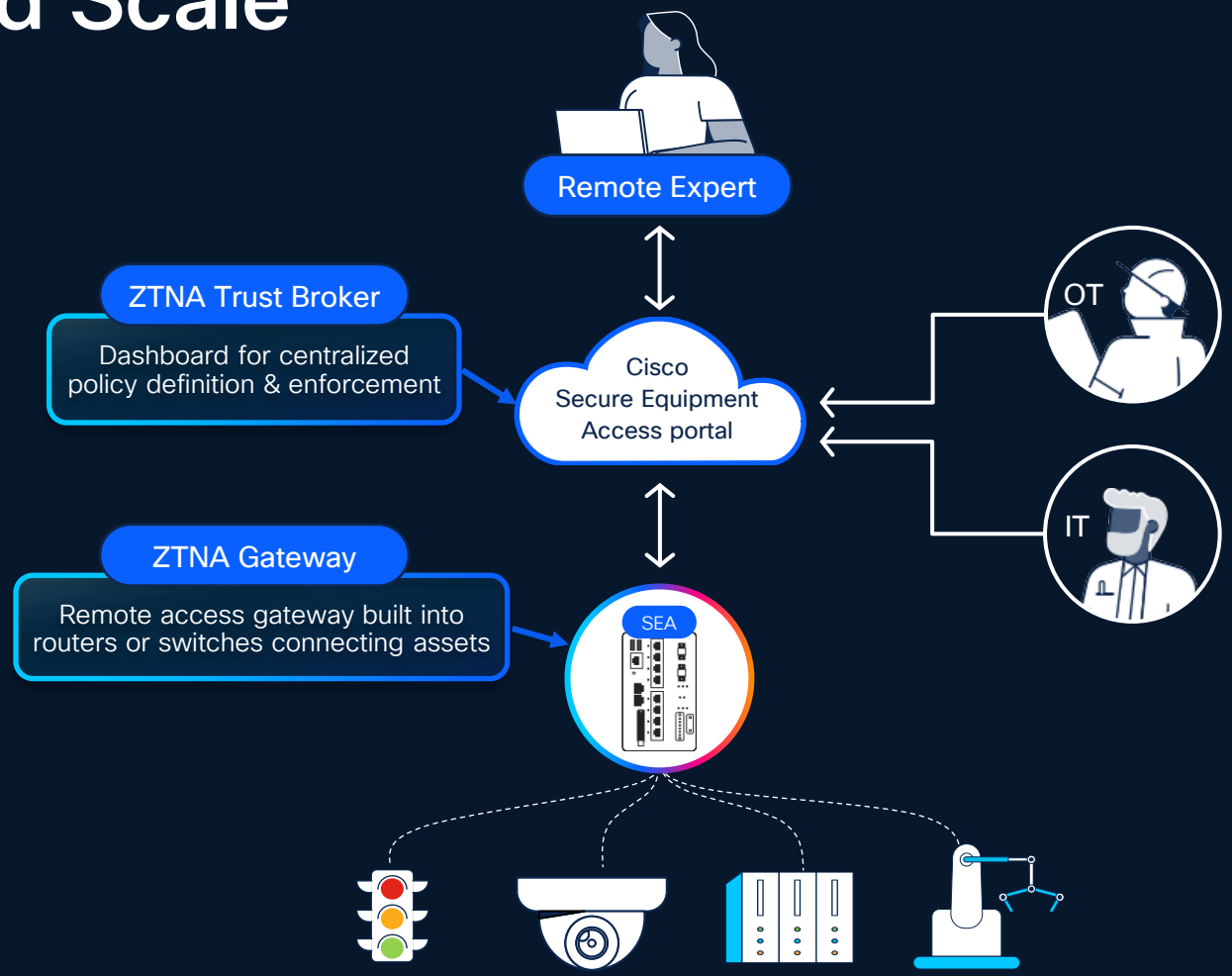
- Monitor active sessions from anywhere in the world
- Terminate remote user session if you detect suspicious activity
- Record or Join sessions for training or audit purposes



# Easily Deploy, Manage, and Scale

## A cloud service built into your industrial network

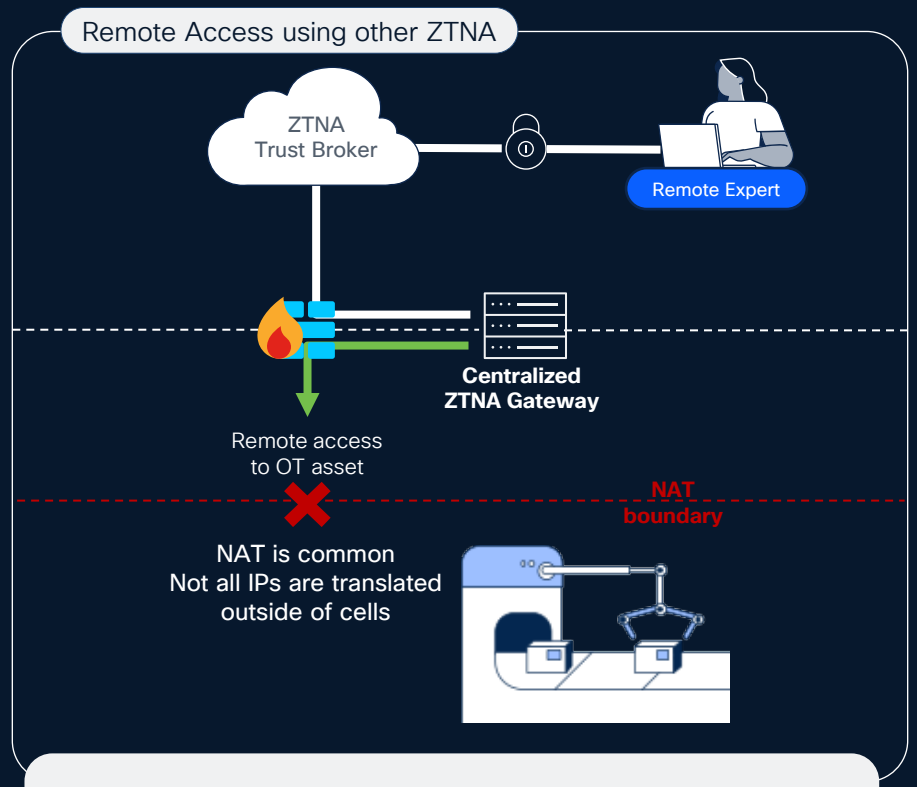
- Centralized policy definition for all assets and all sites
- Centralized enforcement increasing security and streamlining user experience
- Network-embedded gateways eliminating the need for dedicated hardware appliances



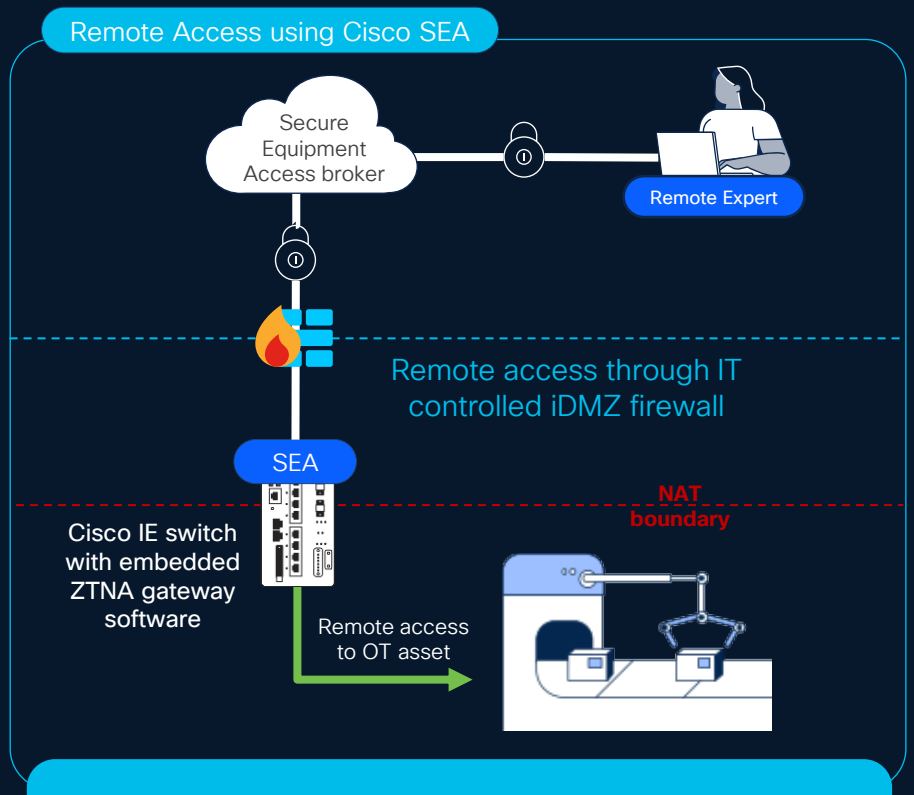

One-click zero trust remote access to any OT asset connected to Cisco industrial network

# Not all ZTNA solutions are suited for use in OT environment

Cisco SEA simplifies remote access to NATed industrial devices




Centralized ZTNA gateway is too far from OT assets, forcing users to expose private IPs outside Level-2, negating resource isolation and increasing attack surface

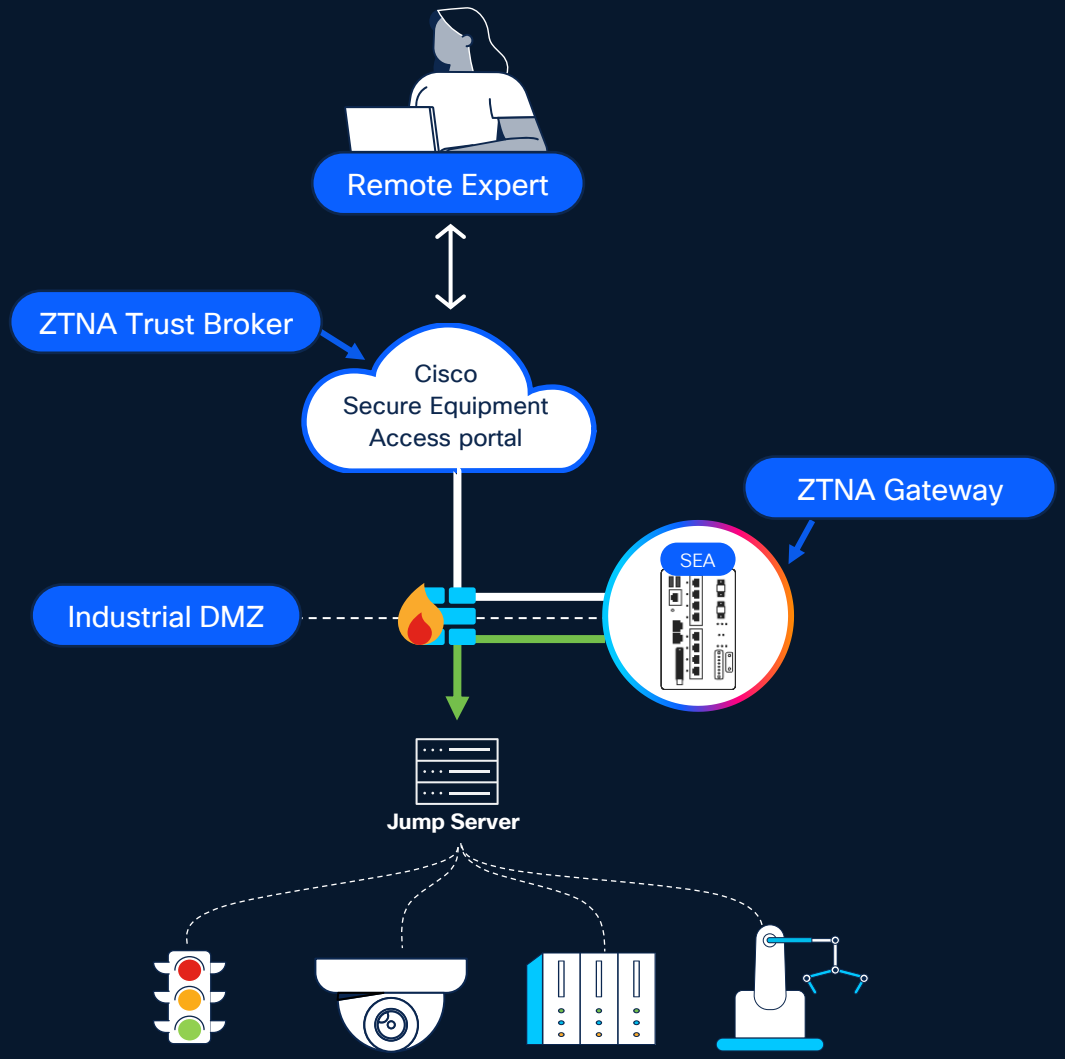



The switch or router connecting the NATed device is the ZTNA gateway, eliminating the need for complex network configuration for exposing private IP addresses

# Enhancing Existing Jump Servers with Zero-Trust

## Supercharge your existing remote access setup with modern security capabilities

- Keep existing jump servers to maintain workflows and simplify change
- Enforce robust access control with SEA ensuring only authorized users have access at specific times
- Gain new control with SEA recording sessions or inspecting file transfer*
- Simplify operations with cloud-based policy management that OT can use






* Feature available end of CY2025

# Platforms that support the SEA gateway

SEA Agent is the ZTNA gateway function embedded in network platforms

## Industrial Routers


IR1101


IR1800


IR8300 *Roadmap*

## Industrial Switches

IE3500
IE3400
IE3300


IE3500H
IE3400H


IE3100


IE3100H



IE9300

## Enterprise Switches


Catalyst 9300

Cisco Secure Equipment Access

# Modernize your OT remote access with zero-trust security built into your industrial network

## Better for Users

Empower operations with a solution designed for OT

## Easier for IT

Simplify deployment and management at scale

## Safer for Everyone

Reduce risk by enforcing zero-trust security controls

Industrial cybersecurity that’s safer and easier for everyone


CISCO

# Use Cases

# Remote access to Roadside Cabinets

## Challenges

- Thousands of intersections providing multiple traffic system functions
- Need secure and highly scalable WAN infrastructure
- Need wired or wireless connectivity depending on the location

## Solution

- Cisco Catalyst IR1101 Rugged router with fiber, copper, 4G or 5G modular backhaul connectivity
- Cisco Secure Equipment Access gateway software built-in

## Benefits

- No additional hardware to install in small cabinets
- Improved security with least-privilege remote access policy enforcement
- Streamlined operations and reduced cost by eliminating truck rolls
- Unified solution for both wired or wireless connectivity needs
- Secure, scalable, and easy to manage WAN infrastructure

# Remote access to Wind & Solar Farms

## Challenges

- Wind farms are installed in remote areas.
  Sending a technician can be too expensive or just not possible
- Smaller sites require a cost-effective, light-weight solution
- Cellular networks are generally the only connectivity option

## Solution

- Cisco Catalyst IR1101 Rugged router with 4G or 5G interface module
- Cisco Secure Equipment Access gateway software built-in

## Benefits

- No additional hardware to install in remote sites
- Streamlined operations, increased uptime, and reduced costs thanks to remote access and management of wind turbines
- Secure, scalable, and easy to manage WAN infrastructure
- Improved security with least-privilege remote access policy enforcement

# Remote access to Grid Substations

## Challenges

- Need scalable connectivity 10s/100s of thousands of secondary substations to control power distribution and support distributed renewable energy deployments
- Need secure and highly scalable WAN infrastructure
- Need wired or wireless connectivity depending on the location

## Solution

- Cisco Catalyst IR1101 Rugged router with fiber, copper, 4G or 5G modular backhaul connectivity
- Cisco Secure Equipment Access gateway software built-in

## Benefits

- No additional hardware to install in small cabinets
- Improved security with least-privilege remote access policy enforcement
- Streamlined operations and reduced cost by eliminating truck rolls
- Unified solution for both wired or wireless connectivity needs
- Secure, scalable, and easy to manage WAN infrastructure

# Remote access to Manufacturing Assets

## Challenges

- Numerous contractors and remote experts responsible form maintaining and troubleshooting plant assets
- Machines and systems generally have vendor-configured IP addresses that are NATed and not reachable from higher layers of the network

## Solution

- Cisco Industrial Ethernet rugged switches
- Cisco Secure Equipment Access gateway software built-in

## Benefits

- No need to configure and maintaining cumbersome VPN and jump-servers
- No additional hardware to install in production cells
- NATed assets can be remotely accessed without having to expose private IP addresses to the Internet
- Easy management of remote users and improved security with least-privilege remote access policy enforcement

# Customer stories

# Optimizing energy usage at scale

energybox

## Business needs

- Remotely manage customers' lighting, HVAC, and refrigeration systems to help reduce energy costs and improve margins
- Ensure remote equipment maintenance to avoid failure and unplanned downtime

## Solution

- Cisco Catalyst IR1100 Rugged Series routers
- Cisco Secure Equipment Access

## Outcomes

- Customer savings of $10,000 per site, per month
- Remote access to all locations from any device, with real-time notifications of equipment and system anomalies
- Secure remote management of Cisco routers and Energybox controllers saves thousands of dollars per site in truck rolls, $1M+ per software upgrade



cisco

# Secure remote access to OT assets for maintenance

## A leading auto parts manufacturer

### Business needs

- Provide remote access to third party contractors and vendors to specific machines and key assets
- Ensure plant security and production uptime, without exposing the network to cyber threats

### Solution

- Top of the line switches replaced by Catalyst IE3300 with embedded Cisco SEA gateway software

### Outcomes

- Secure remote access to PLCs distributed across plants without the burden of maintaining cumbersome VPN and jump-servers
- Zero Trust Network Access (ZTNA) resource isolation and access policy controlled through cloud-based SEA trust broker

# Remote access for maintenance of offshore wind farms

## A major offshore wind turbines operator

### Business needs

- Remote access to hundreds of offshore wind turbines for maintenance, as soon as each turbine is installed
- LTE connectivity to allow communication via service provider base station rather than expensive satellite communication

### Solution

- Cisco industrial networking devices with embedded Cisco SEA gateway software

### Outcomes

- Reduced cost by removing need for in-person visits via helicopter or sea vessel to manage each wind farm
- Remote visibility into wind turbines as soon as they are installed
- Streamlined operations with remote access and management of wind turbines using Secure Equipment Access
- Secure end-to-end connectivity

# Modernizing the roadside network

## A large US department of Transportation (DoT)

### Business needs

- Modernize roadside network to enable Intelligent Transportation Systems (ITS), reduce congestions, and improve road safety
- Eliminate issues due to cellular network compatibility
- Rugged hardware for harsh outdoor environments and extreme weather

### Solution

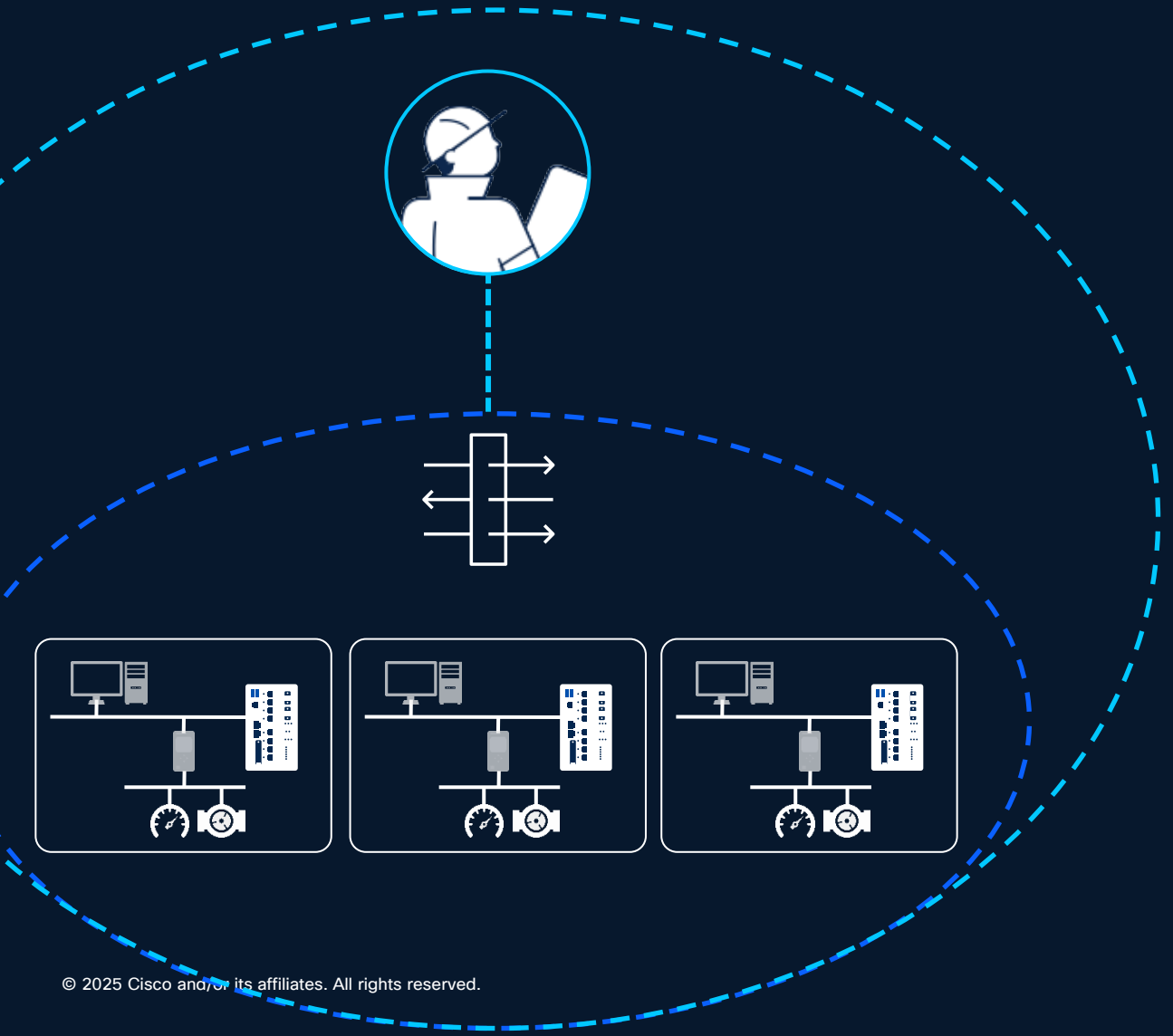
- Cisco Catalyst IR1100 Rugged routers and Catalyst Industrial Ethernet switches in the traffic cabinets
- Embedded Cisco SEA for remote access and Cyber Vision for visibility

### Outcomes

- Simplified setup in space-constrained cabinets with remote access, visibility and enforcement build into the switch or router
- Reliable roadside infrastructure using cellular backhaul enabling streamlined operations in the control center
- Reduced costs by eliminating truck rolls for maintenance
- Improved security by ensuring remote technicians can access only the roadside equipment they need, and only when needed
- Easy to scale to thousands of intersections

# Remote Access Architectures

# Virtual Private Network (VPN)



## Extends the network to remote users

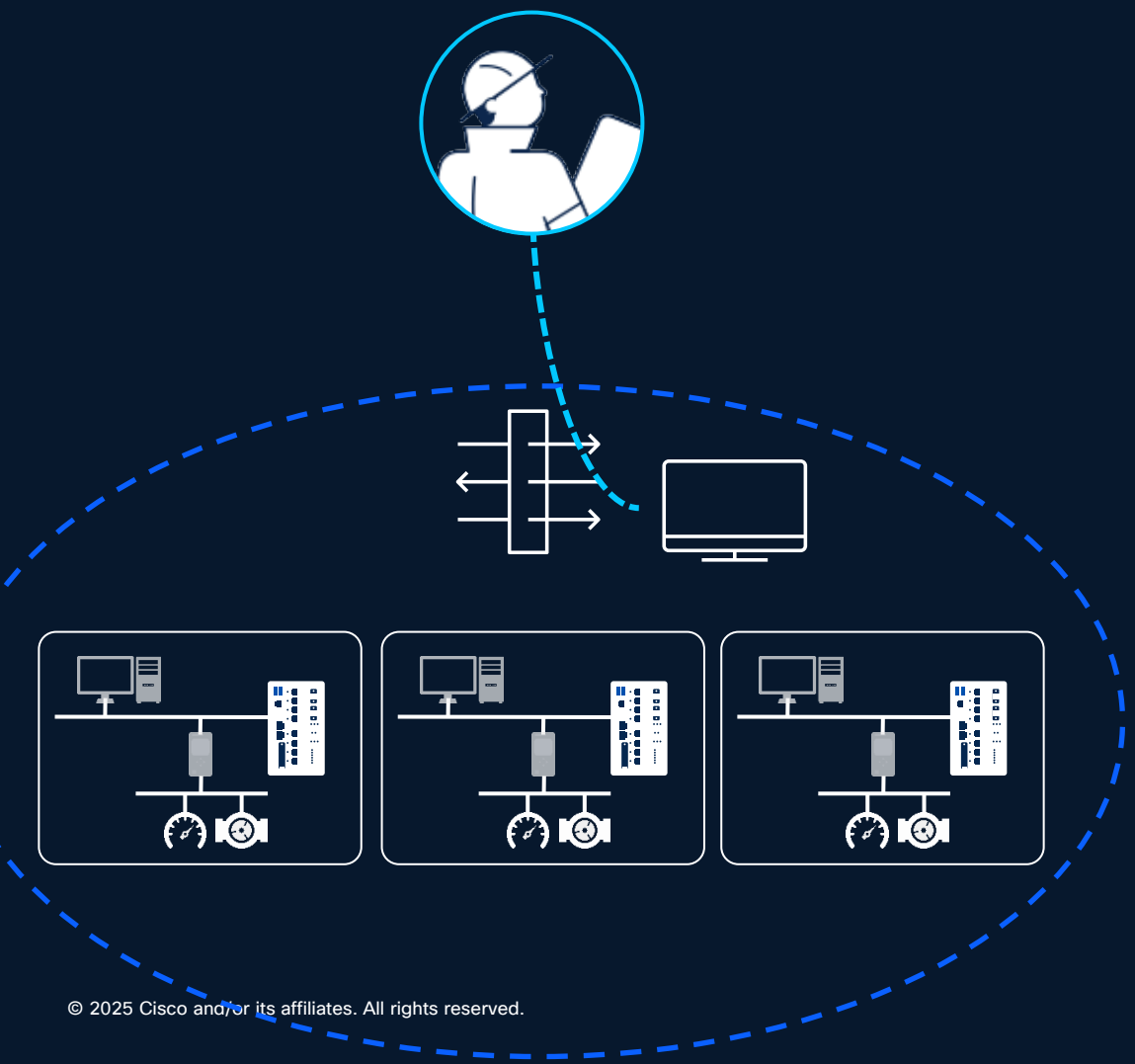
Pros

- 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**

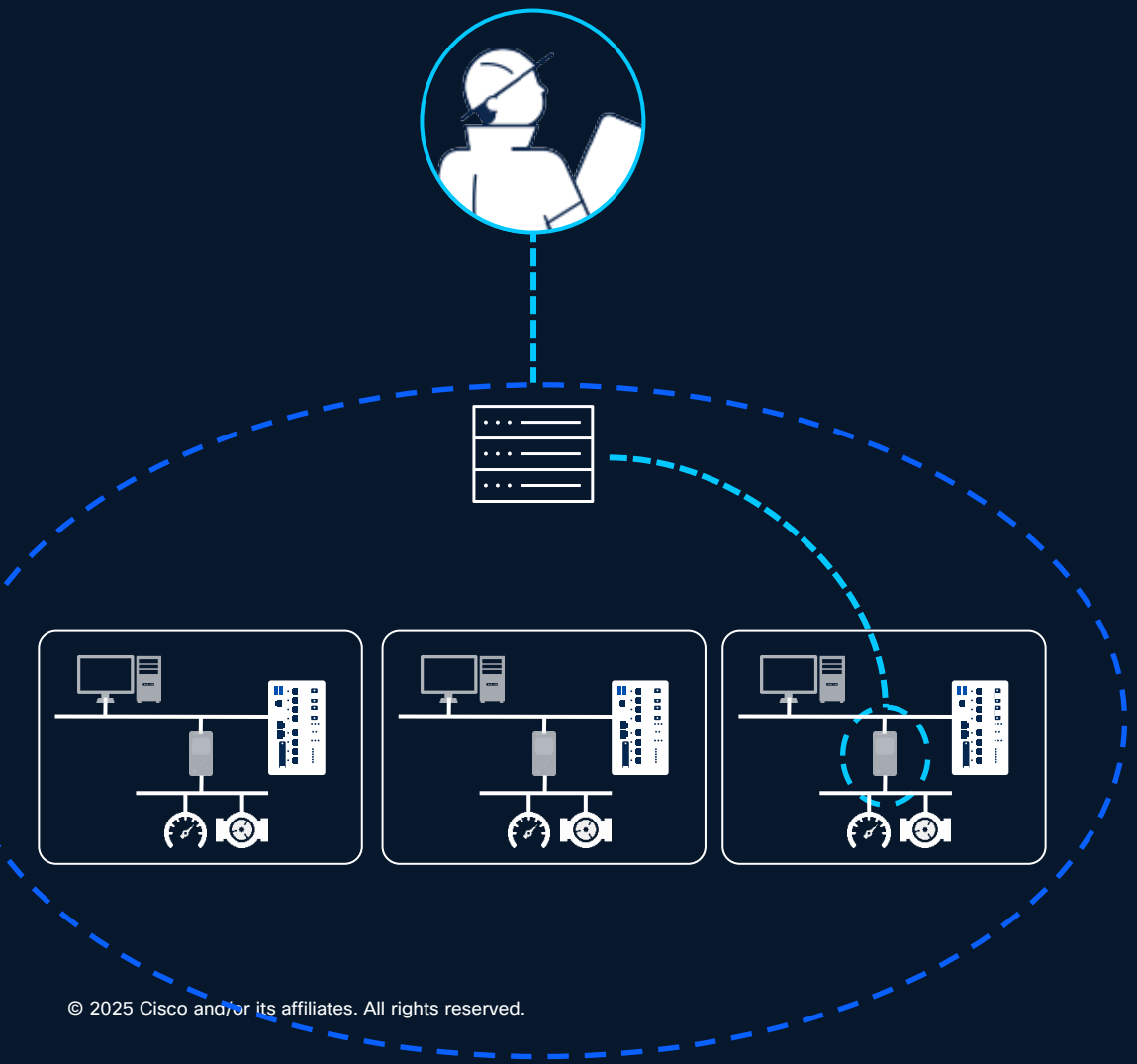
Pros

- 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

# 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 trust broker

Cons

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

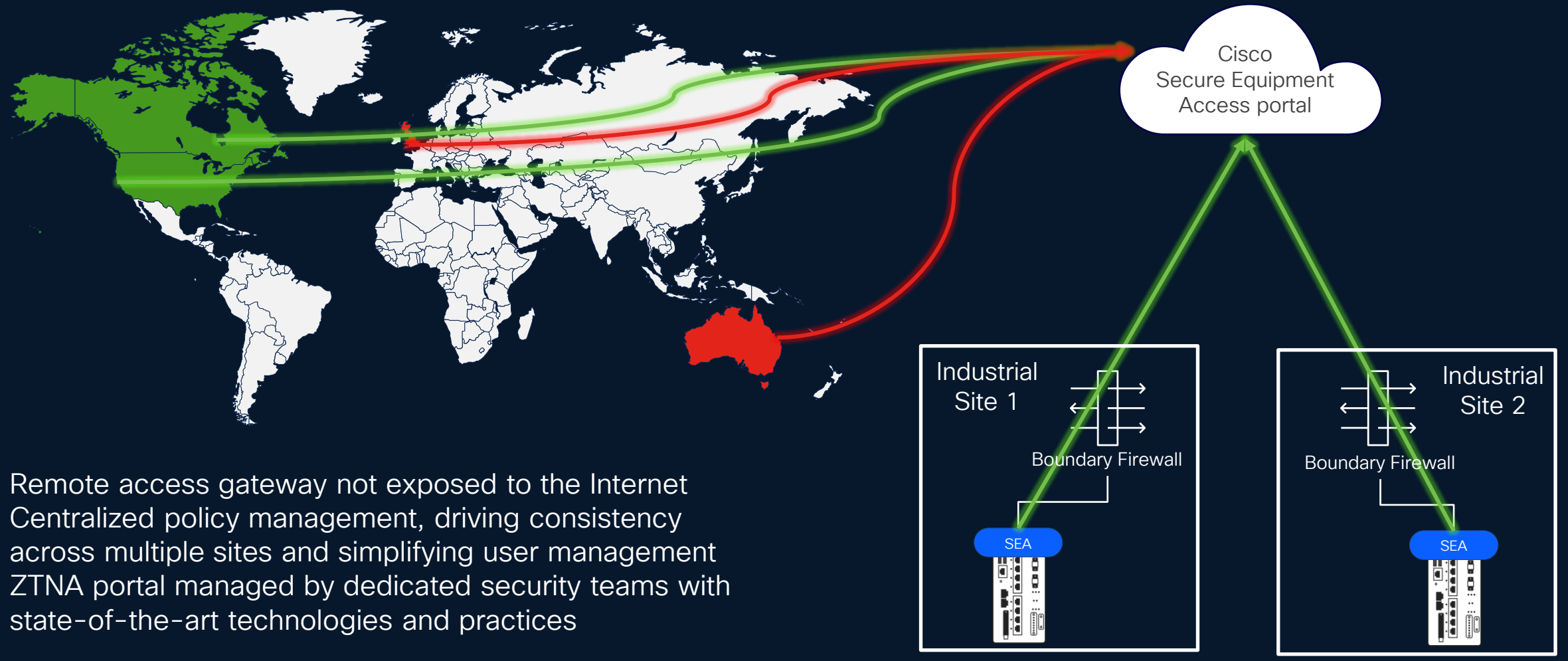
# Is cloud-based remote access risky?

# Remote VPN users have direct access to your network


VPN headend is generally on-prem, exposing part of the network to the public which invites exploitation

Complex setup required to protect against identity threats and lateral movement. Difficult to scale in a large industrial infrastructure

# ZTNA only needs a single trusted flow through the firewall

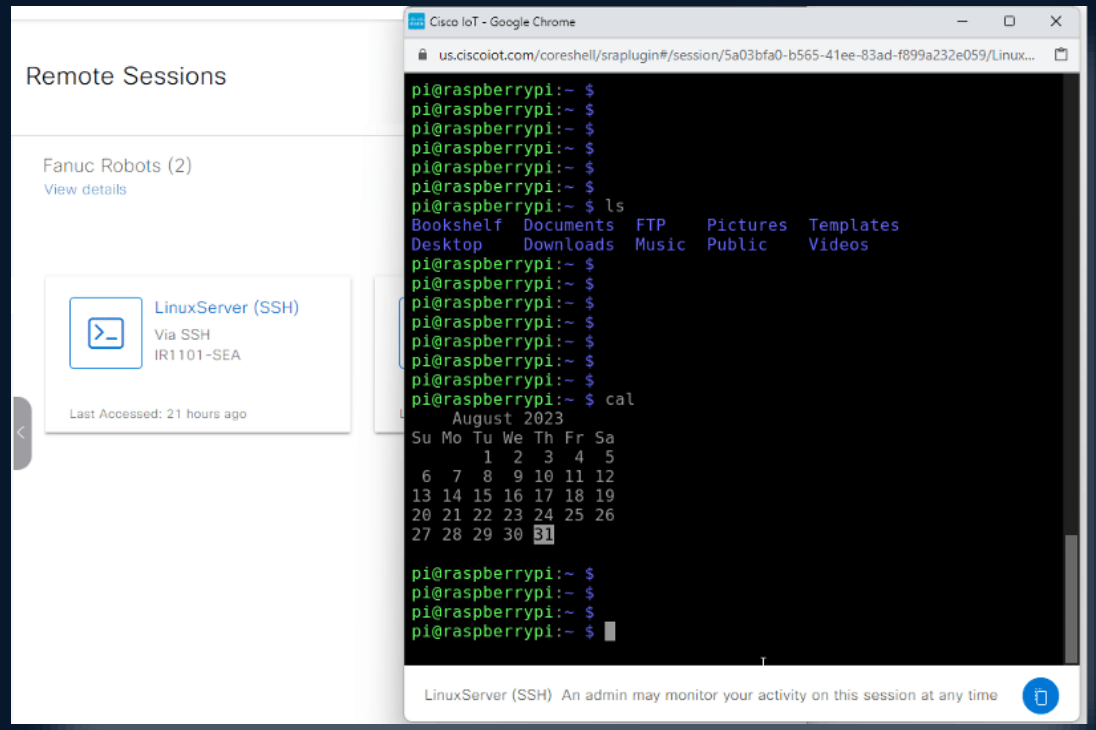



- Remote access gateway not exposed to the Internet
- Centralized policy management, driving consistency across multiple sites and simplifying user management
- ZTNA portal managed by dedicated security teams with state-of-the-art technologies and practices

*Clientless and Agent-based remote access*

# Cisco SEA and SEA Plus

# Cisco SEA is a client-less remote access solution




## No installation required

Users only need a browser to access remote assets using RDP, VNC, SSH, Telnet or HTTP(S)

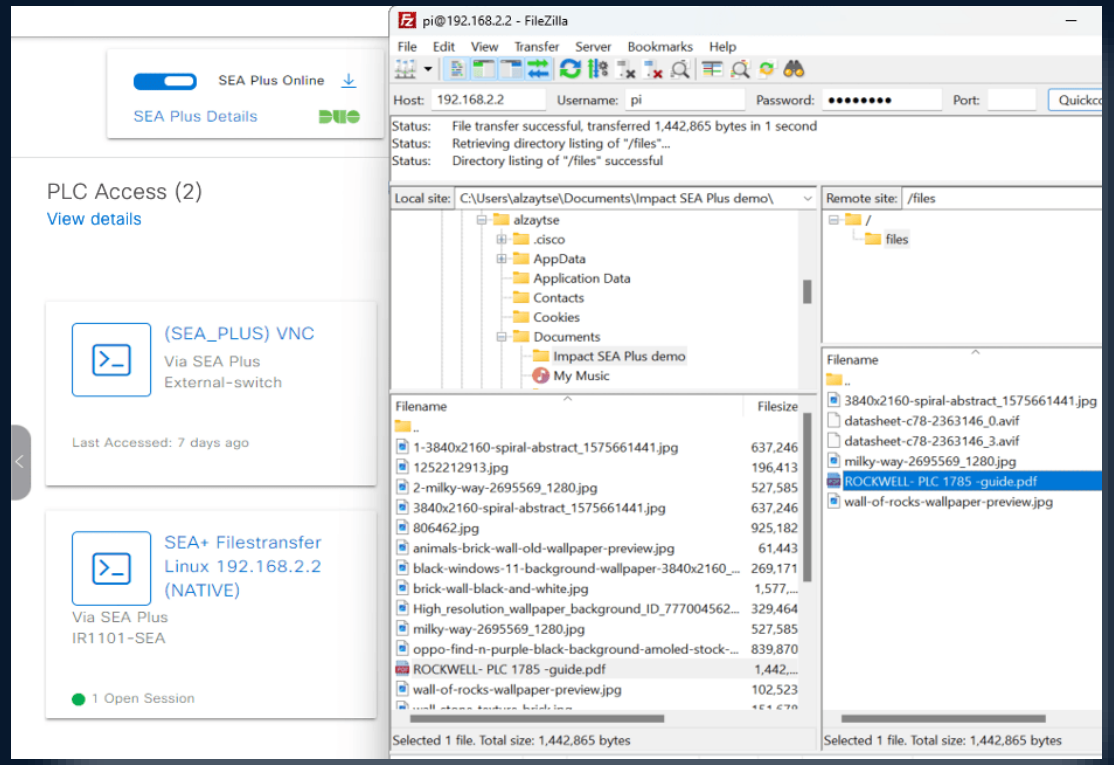
## Complete user isolation

Remote users only access the cloud broker and are never connected to remote network

## Session Proxy

The SEA Gateway running in a Cisco switch or router is a proxy over TLS/443

# Enabling IP access with Cisco SEA Plus




## IP access to specific assets only

When creating an SEA Plus session, native desktop clients can be used for advanced tasks

## Software agent needed

SEA automatically installs a lightweight agent on the user's computer to create a TUNTAP device

## Security posture check

SEA can verify the computer compliance with security hygiene policies using Cisco Duo

# Cisco SEA vs SEA Plus

## Clientless ZTNA

SEA sessions are straightforward
- Nothing to install
- Complete IP isolation

SEA sessions are ideal for most remote access needs:
- SSH, VNC, RDP, Telnet, Web

## Agent-based ZTNA

SEA Plus sessions need an agent
- Installation requires Windows admin privileges

SEA Plus sessions enable direct IP connectivity to the asset:
- Allows using desktop applications such as a PLC programmer tool or file transfer (ie. with SFTP)

Use both SEA and SEA Plus for different use cases. Both enforce ZTNA policies


CISCO