

Secure Remote Access for Industrial Operations

Protecting industrial networks against risks from remote users with a Zero-Trust Network Access (ZTNA) architecture purpose-built for OT workflows





Contents

- Overview 3
- Industrial remote access imperatives 3
 - Dealing with the scale and complexity of industrial networks 3
 - Provisioning remote access rapidly..... 4
 - Managing policies across numerous distributed industrial sites 4
 - Maintaining remote access credentials 4
 - Handling IP address reuse and Network Address Translation (NAT) 4
- Using enterprise remote access solutions in industrial settings..... 5
 - Virtual Private Networks (VPNs)..... 5
 - Jump servers 6
 - Zero-Trust Network Access (ZTNA)..... 7
- Cisco Cyber Vision’s SEA: ZTNA purpose-built for industrial settings..... 8
 - Core components 9
 - Least-privilege access control..... 10
 - Agentless and client-based access 10
 - Identity Threat Detection and Response (ITDR)..... 11
 - Session management and auditing 11
 - Self-service OT remote access..... 12
- Cisco Cyber Vision’s SEA deployment overview 12
 - Architecture options 12
 - Gateway deployment and management 13
 - Enhancing existing jump servers with zero-trust controls 14
 - Benefits of a cloud-based ZTNA trust broker 15
- Summary..... 15

Overview

Remote access is key for operations teams to manage and troubleshoot Operational Technology (OT) assets at scale without time-consuming and costly site visits. Industrial equipment—from traffic controllers along roadways to machines on the manufacturing floor—frequently requires specialized technical support from the respective manufacturers or from remote experts. However, the increasing need for remote connectivity to critical equipment opens the attack surface to threat actors, and if implemented incorrectly, can lead to a breach.

Remote access solutions come in many forms, and choosing one that will meet business needs and control cyber risks at the same time can be confusing. In many organizations, machine builders, maintenance contractors, or the operations teams themselves have installed their own solutions: cellular gateways that nobody knows about or remote access software that IT is not controlling. These backdoors are at odds with the OT security projects undertaken by the IT/security teams and create a shadow IT situation that makes it difficult to control who is connecting, what they are doing, and what they can access.

On the other hand, VPNs installed by IT teams in the Industrial Demilitarized Zone (IDMZ) have the drawback of being always-on solutions with all-or-nothing access to OT assets. Restricting access to them requires additional tools and IT skills. This creates difficulties and frustration when the OT team needs to quickly add or modify access rights. The challenge is compounded by frequent changes in remote users and the large number of assets requiring access.

Zero-Trust Network Access (ZTNA) solutions are gaining increased momentum for enforcing least-privilege remote access policies in enterprise networks, but they don't translate well to OT. This solution brief describes how Cisco® Cyber Vision's Secure Equipment Access addresses these challenges. It is a subset of the Cisco Validated Design guide (CVD) on Industrial Security and summarizes the design guidance and capabilities contained within the guide. For more information on any of the technologies and best practices found in this solution brief, see the [Cisco Industrial Security Design Guide](#).

Industrial remote access imperatives

Modern industrial environments demand sophisticated remote access capabilities to maintain operational continuity. Critical sectors including manufacturing, power generation and distribution, water treatment, transportation systems, oil and gas processing facilities, and many more rely on remote experts for configuring, maintaining, and troubleshooting OT assets. Enabling secure remote access to these assets introduces several challenges.

Dealing with the scale and complexity of industrial networks

When securing remote access to enterprise networks, organizations typically configure policies for a well-defined, relatively static group of users who need access to a limited set of resources, such as file servers or business applications. In contrast, securing remote access in industrial environments involves managing an ever-changing list of remote users, each requiring access to a different OT asset among thousands. These remote users often work for maintenance contractors or equipment vendors. Restricting what they can access—and when—is key.

Provisioning remote access rapidly

This dynamic environment poses a problem of scale, amplified by the need to quickly grant access—even during nights or weekends—to address operational contingencies such as emergency equipment failures, new asset deployment, troubleshooting operations, and regulatory inspections. Traditional solutions often involve complex, time-consuming provisioning processes that impede operational responsiveness and might sometimes cause production downtime.

Managing policies across numerous distributed industrial sites

In addition to the scale issue, many industrial organizations such as those in the utility, transportation, or energy sectors, have OT assets installed in a large number of distributed sites. Remote experts might be responsible for maintaining assets on several sites. Having a centralized way to configure and manage access policies across all sites is critical to simplifying operations and ensuring that users are granted only what's needed and that old credentials are deleted promptly.

Maintaining remote access credentials

The Colonial Pipeline attack in 2021 exemplifies the catastrophic impact of poor management of remote access credentials. DarkSide ransomware operators gained access to the enterprise network through compromised VPN credentials, which forced the security team to isolate the OT network from critical IT resources such as ordering and billing systems. This response resulted in a complete shutdown of fuel distribution operations. Credential management is critical for securing remote access. Multifactor Authentication (MFA) is an efficient way to control who can connect, but policies associated with each user need to be properly maintained as well.

Handling IP address reuse and Network Address Translation (NAT)

Many industrial operations, especially in manufacturing sectors, are made of complex systems configured by machine builders using the same IP addresses. As IT is generally not allowed to modify the configuration of these machines, many are installed behind NAT boundaries, which makes them unreachable by remote access gateways deployed in the IDMZ. The complexity now falls on the networking team to expose these private IPs to the higher layers of the Purdue model.

Using enterprise remote access solutions in industrial settings

Virtual Private Networks (VPNs)

Traditional VPN implementations extend network privileges to remote users, creating opportunities for lateral movement and reconnaissance. Once authenticated, users typically gain broad network access that exceeds operational requirements. VPNs essentially extend the entire network, not just the single machine they need to service, to the remote user's device. This violates least-privilege security principles and greatly expands the attack surface.

Restricting what remote users can access using VPNs requires additional network access controllers, which introduce operational overhead and make management even more complex for non-IT skilled workers. Enforcing additional security controls such as device posture checks, remote desktops, or joining and recording sessions requires installing additional jump servers, which is often not an option, especially in field networks where space inside cabinets might be an issue.

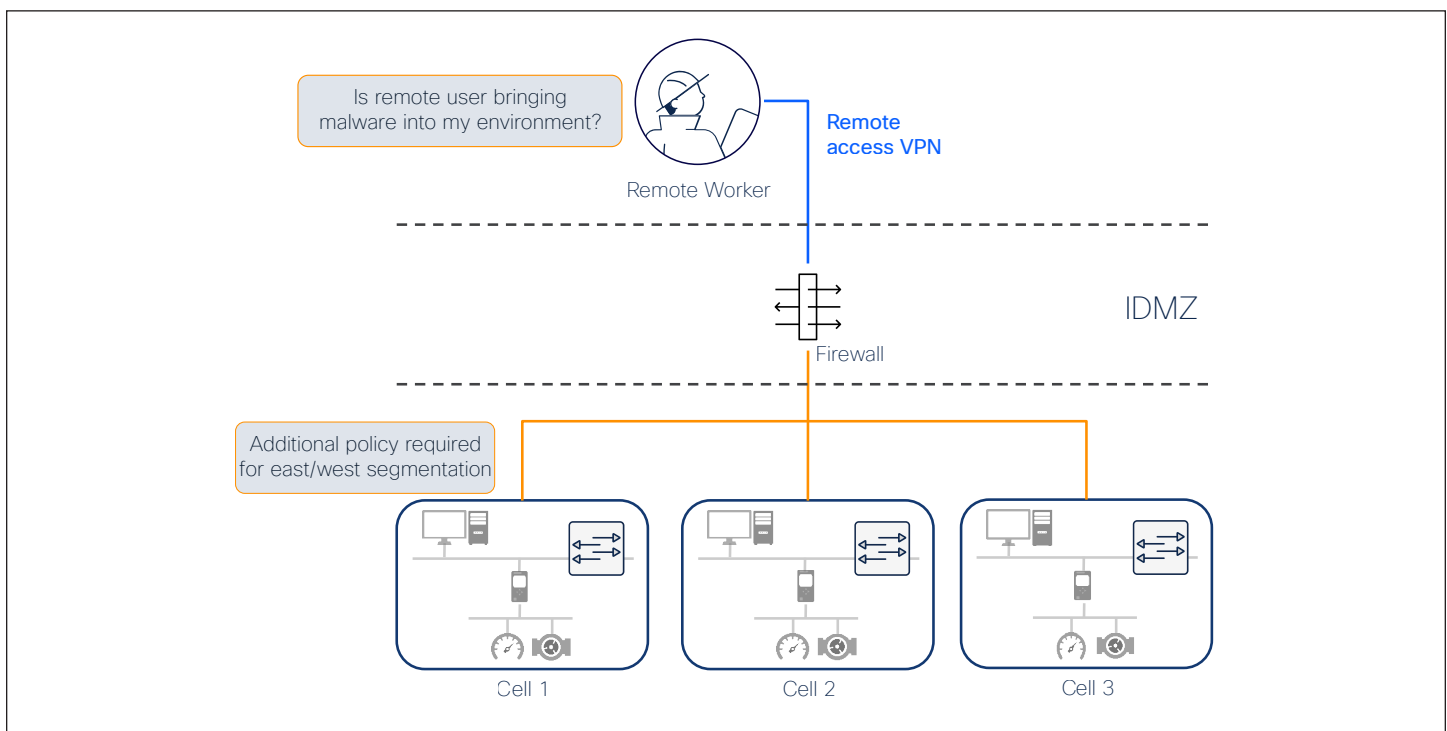


Figure 1. Restricting what users can do over the VPN requires additional tools and overhead

While all the necessary security checks and controls are possible with a traditional VPN-based solution, the operational overhead often leads to lackluster policies and wide-open access policies after remote access has been granted.

Additionally, VPN access is commonly maintained by a separate entity in the organization, which causes delays for vendor connectivity and slows down the line of business. As a result, even in the IT world, there has been a shift toward looking for VPN alternatives.

Jump servers

A common way to add security controls to VPNs is by using jump servers. After a VPN connection is established, policy is placed on the firewall to allow users to access only a set of jump servers. All activities performed on the OT network must originate from a jump server, which is a trusted device fully controlled by the networking team.

While jump servers help prevent malicious software from being introduced to the network, they do not help solve the challenge of controlling what a user can do once they have access to the jump server. Best practices would leave jump servers in a quarantined state, where they are denied any access to the OT network until called upon. As necessary, security administrators will open specific policies to control what a user can and cannot do from that server. However, the operational burden of doing that can be overwhelming, and in reality, jump servers expose themselves to the same frailties as the VPN solution.

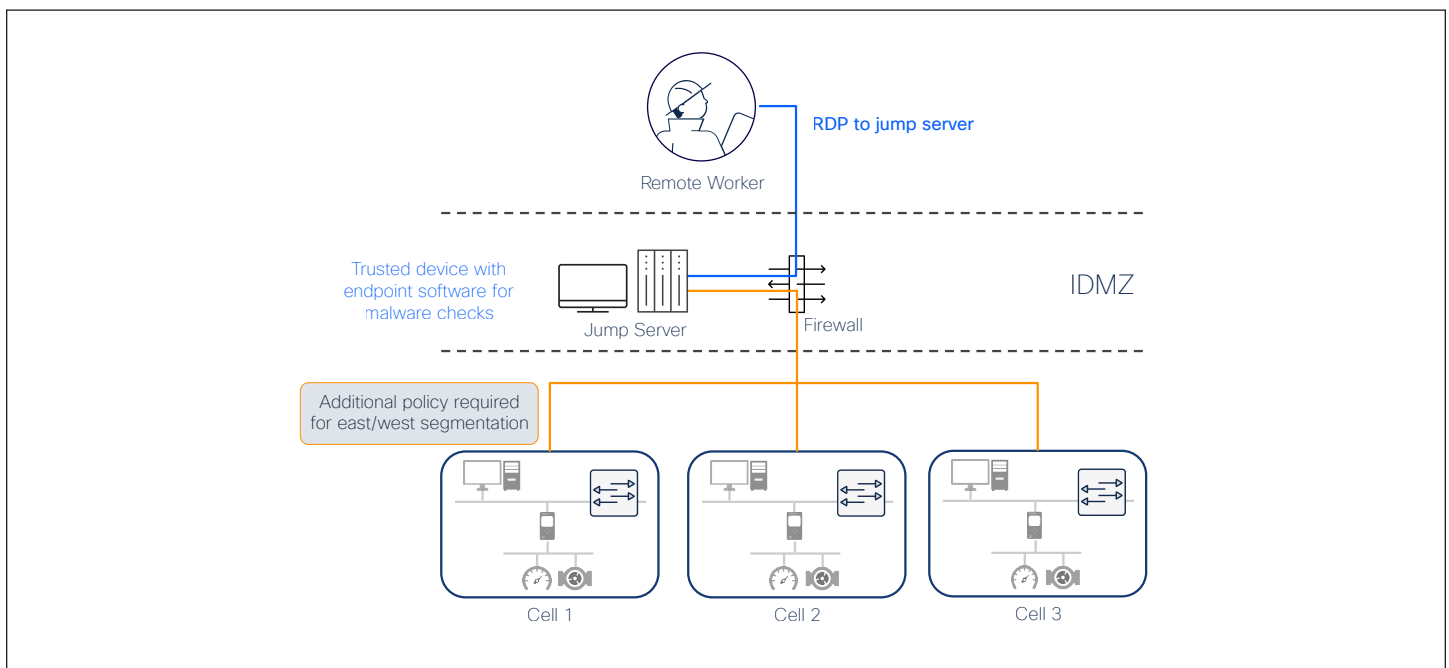


Figure 2. Jump servers help control malicious traffic, but security policies are still needed

Zero-Trust Network Access (ZTNA)

Industrial organizations are starting to deploy ZTNA solutions as alternatives to always-on VPNs. ZTNA is a security service that verifies users and grants access only to specific resources at specific times based on identity and context policies. It starts with a default deny posture and adaptively offers the appropriate trust required at the time.

ZTNA solutions consists of a trust broker, typically a cloud service, that mediates connections between remote users and OT assets. The trust broker communicates with a ZTNA gateway deployed in the industrial network. The gateway establishes an outbound connection to the trust broker, which in turn cross-connects to the remote user, thereby creating a communication path to the OT assets.

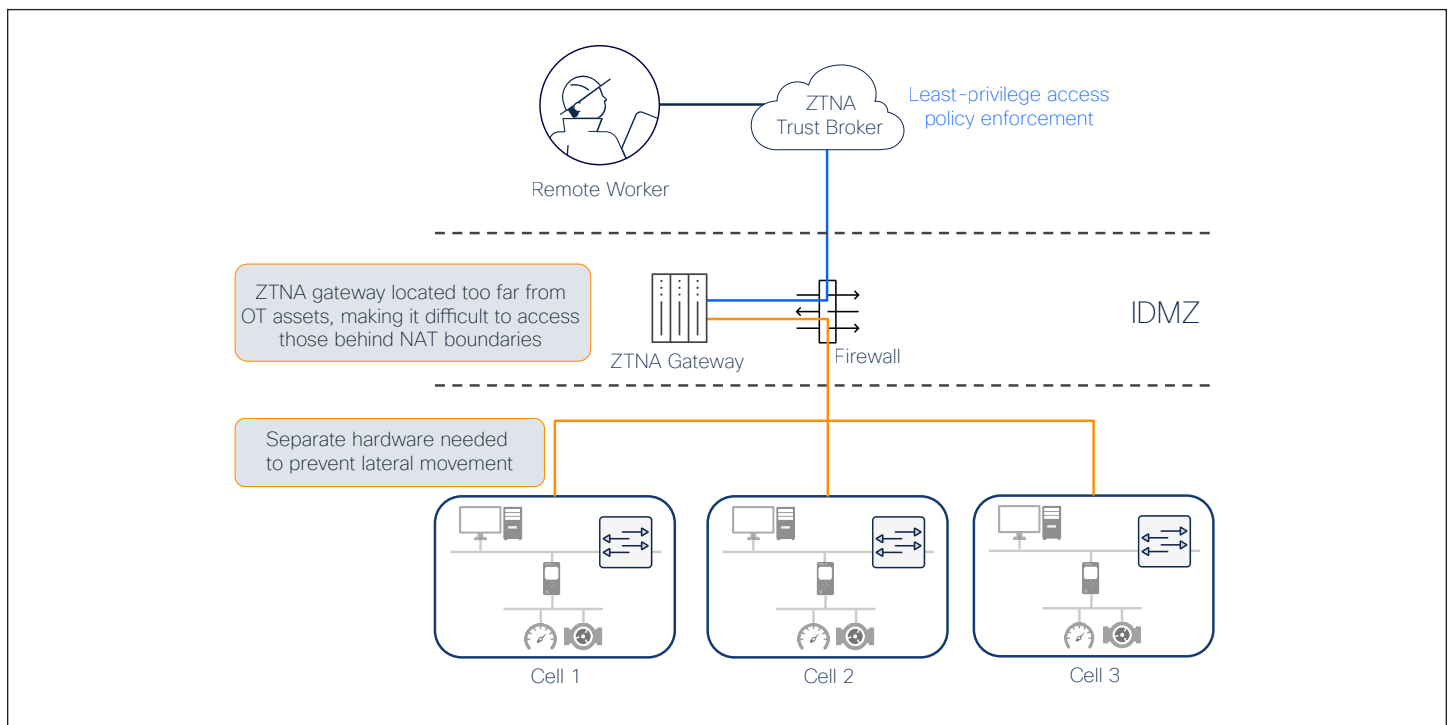


Figure 3. ZTNA solutions are made of a trust broker and gateways deployed in the industrial network

However, in field networks like traffic control cabinets at roadway intersections, or utility pole-mounted capacitor bank control cabinets, installing dedicated ZTNA gateways is not an option due to space issues. When space is available, having to maintain dedicated ZTNA gateway hardware just to access a few OT assets puts an undesirable burden on customers and increases costs.

In larger industrial networks, such as manufacturing plants, the ZTNA gateway is centralized in the IDMZ to avoid the cost and complexity of distributing dedicated hardware in the OT network. But this centralized architecture puts the ZTNA gateway too far from the OT assets and suffers the same drawback as the legacy VPN design:

- In such environments IP addresses are often reused, and many assets sit behind NAT boundaries, making them unreachable to the ZTNA gateway in the IDMZ. The complexity then falls on the end customer to expose these private IPs to the higher layers of the Purdue model.
- In addition, because the ZTNA gateway is far from the OT assets, preventing lateral movement of remote users between OT assets becomes challenging.

Both of these aspects negate key tenets of ZTNA, namely resource isolation and limiting lateral movement.

Cisco Cyber Vision's SEA: ZTNA purpose-built for industrial settings

With Cyber Vision's [Secure Equipment Access](#) (SEA), Cisco is solving the challenges of deploying ZTNA in industrial settings. In addition to secure remote access, the platform offers a complete set of capabilities to help protect industrial networks from cyberthreats:

- Comprehensive visibility into OT assets, their vulnerabilities, and communication activities
- OT risk management with smart scoring of asset vulnerabilities and detection of malicious traffic and abnormal asset behaviors
- Adaptive network segmentation to help protect operations by making it easy for OT and IT teams to work together in defining and enforcing access policies that will not disrupt production
- Self-service remote access to empower operations teams while enforcing least-privilege zero trust access policies to control risks from remote users

Cyber Vision's SEA is a cloud service that runs in Cisco network equipment, making it very simple to deploy and manage at scale. It empowers operations teams, vendors, and contractors to easily connect to remote OT assets. It lets organizations enforce least-privilege access policies based on identities and contexts. It is designed to be very simple to configure, so the line of business can easily create remote access credentials when needed while maintaining security controls and respecting security policies defined by the IT and security teams.

Core components

With Cyber Vision’s SEA, remote users just need a web browser to access remote industrial assets. They connect to the SEA cloud portal, where they are authenticated and offered access only to the devices you choose, using only the protocols you specify, and only on the day and time you allow.

The SEA cloud portal is a ZTNA trust broker that handles policy definition and enforcement. Security teams now have a single interface to manage users, assets, and policies for all sites. It uses Cisco or third-party Identity Providers (IdP) to authenticate users, enforce Multifactor Authentication (MFA), and enable Single Sign-On (SSO). It gives the organization control over remote access usage with comprehensive session monitoring, Identity Threat Detection and Response (ITDR) capabilities, and the ability to join and terminate live sessions. It helps meet regulatory requirements by offering comprehensive audit logs, including recordings of remote access sessions.

SEA’s ZTNA gateway is a free software feature running in select [Cisco industrial switches and routers](#). Not only does it eliminate the need for sourcing and deploying dedicated hardware, but it also allows for deployment of any number of gateways, anywhere they are needed, even in the lowest Purdue levels, greatly simplifying secure remote access to OT assets sitting behind NAT boundaries.

The SEA gateway software is an IOx application, the virtualization environment offered by Cisco IOS® XE, Cisco’s networking operating system. It runs in a dedicated CPU core in the hosting device, which means SEA can access all the resources it needs with no impact on the performance of the switch or router. For the up-to-date list of Cisco switches and routers supporting the SEA gateway software, please refer to the [SEA data sheet](#).

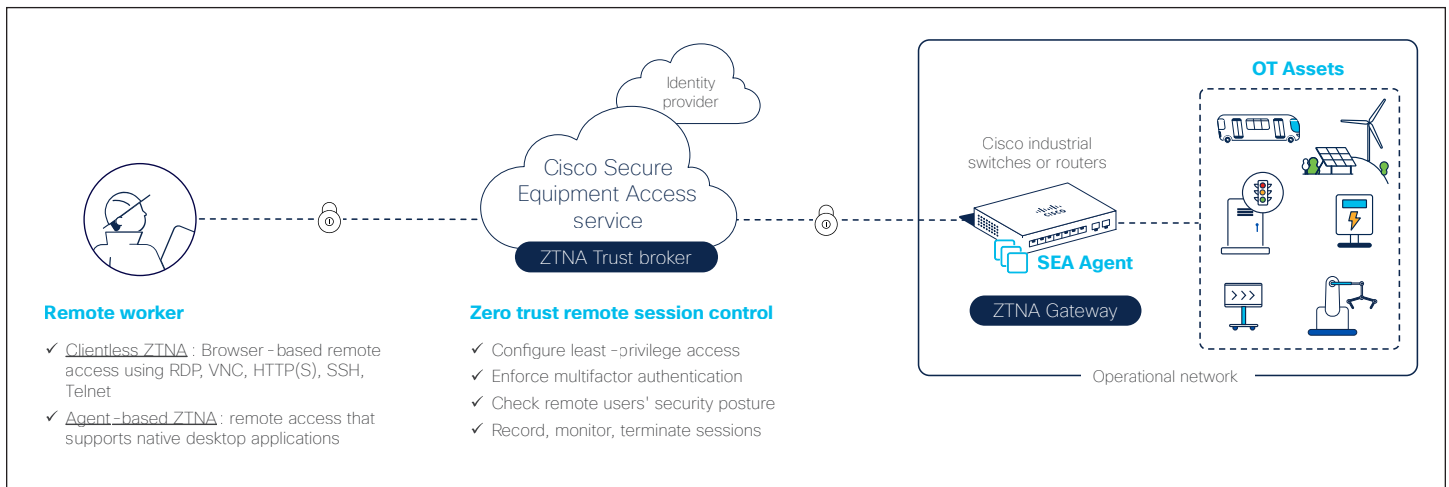


Figure 4. Cisco Cyber Vision’s Secure Equipment Access architecture

Least-privilege access control

With Cyber Vision's SEA, remote access is denied by default. Users are given access only to the assets they truly need to do their job—and no more. Administrators define policies based on identities, remote assets, schedules, and access methods. This granularity helps ensure that access is provided only to users or groups of users who need it, when they need it, and from locations and devices that are trusted. To protect the network from discovery and lateral movement, SEA provides the following capabilities:

- **Identity authorization:** SEA verifies user identity at every access attempt and assigns the corresponding access policy. Access to the full network is never granted.
- **Time-based access:** SEA grants access only when needed and restricts it to the resources required for a given access attempt. Remote access for the OT network is off by default, and access is granted at time of need, for a specified period, before being turned off again by the system.
- **Session request:** Just because a session has been scheduled does not always mean that it is safe to allow a remote access request. SEA offers a session approval flow, in which remote access will be granted only when an administrator approves a remote user's request.

Agentless and client-based access

With Cyber Vision's SEA, remote users use a web browser to connect to the SEA trust broker, which proxies sessions to the assets. User never have access to the network. Not only does this makes users' lives simpler, but it allows the administrator to restrict the access methods they can use. Access policies must specifically allow one or several methods:

- **Agentless:** Users interact with OT assets via their web browser. RDP, VNC, HTTP(S), SSH, or Telnet access methods can be used. Sessions are proxied by the SEA trust broker.
- **Client-based:** SEA establishes a secure IP communication channel between the user's computer and the OT asset, so that any desktop application can be used for advanced tasks such as file transfer or PLC programming using native applications. A lightweight software client is automatically installed on the user's computer. Rules can be created to restrict access to specific TCP/UDP ports. Posture checks can be triggered using [Cisco Duo](#) to help ensure that the remote user's computer complies with security policies and to prevent malware intrusion, for instance.

Identity Threat Detection and Response (ITDR)

Cyber Vision's SEA enables administrators to proactively identify and respond to potential identity threats. It continuously monitors identity-related issues when remote users try to connect, for instance, when a user is connecting from an unusual or prohibited location, outside normal working hours or times and days configured by an administrator.

In addition, the SEA dashboard highlights user activity data, such as the number of remote sessions initiated by each user, the number of computers each is using and their types, and more. It can be configured to automatically lock user accounts when inactive after a certain number of days.

Not only does this help security professionals maintain an accurate list of authorized users and prevent intrusions due to poor credential management, but it also gives them valuable insights into user behavior, enabling them to detect and mitigate potential identity risks.

Session management and auditing

The Cyber Vision SEA dashboard gives administrative users a comprehensive view of active remote access sessions as well as session history so they can act and maintain an audit trail for regulatory compliance:

- **Authentication logs:** Show where and how users authenticate, with usernames, location, time, device posture, and access logs.
- **Administration logs:** Show the sessions that were created, who created them, and what access control measures were put in place for the end users.
- **Session monitoring:** Enables an administrative user to join a session and view in real time what is happening. For example, when an external technician delivers remote support for an asset, an internal OT operator may want to monitor the actions taken during the remote access session.
- **Session termination:** Enables an administrator to terminate either an active session that should never have become active in the first place or a session being monitored in which the remote user attempts to deviate from their permitted actions.
- **Session recording:** Enables remote sessions to be recorded and stored for use in an audit trail. If a breach were to occur, having the ability to look back at what remote users did to a system aids incident investigation.

Self-service OT remote access

Cyber Vision's SEA supports Role-Based Access Control (RBAC) and offers a set of predefined and customizable user roles. Based on their identities, users are offered specific rights. Administrators see all OT assets and can define policies. Basic users see only the assets they have been granted access to.

Other roles allow administrators to delegate credential creation and management, so that OT teams can manage remote users and assets themselves to meet the need of operations. Because SEA is an easy-to-use web portal, OT teams now have a self-service solution to quickly enable remote access in the case of an emergency while complying with security policies defined by the IT and security teams.

Cisco Cyber Vision's SEA deployment overview

Architecture options

Cyber Vision's SEA is a hybrid-cloud ZTNA solution. All users interact only with the SEA trust broker running in the Cisco cloud. SEA gateways are always installed on-premises. Depending on the industrial network's architecture, the placement of the SEA gateway will vary:

- **In distributed industrial networks**, such as those in transportation or utility sectors, for instance, the SEA gateway software is installed in [Cisco industrial routers](#) connecting remote sites to the internet where the SEA cloud broker is located. Cisco industrial routers, being full-featured Next-Generation Firewalls (NGFW), offer unmatched cybersecurity capabilities in addition to advanced routing and SD-WAN features.
- **In distributed networks with a hub-spoke model**, the SEA gateway can be installed in a Cisco switch or router at the hub location. This allows use of SEA even when routers connecting remote sites don't support SEA or are configured to communicate with the hub site only.

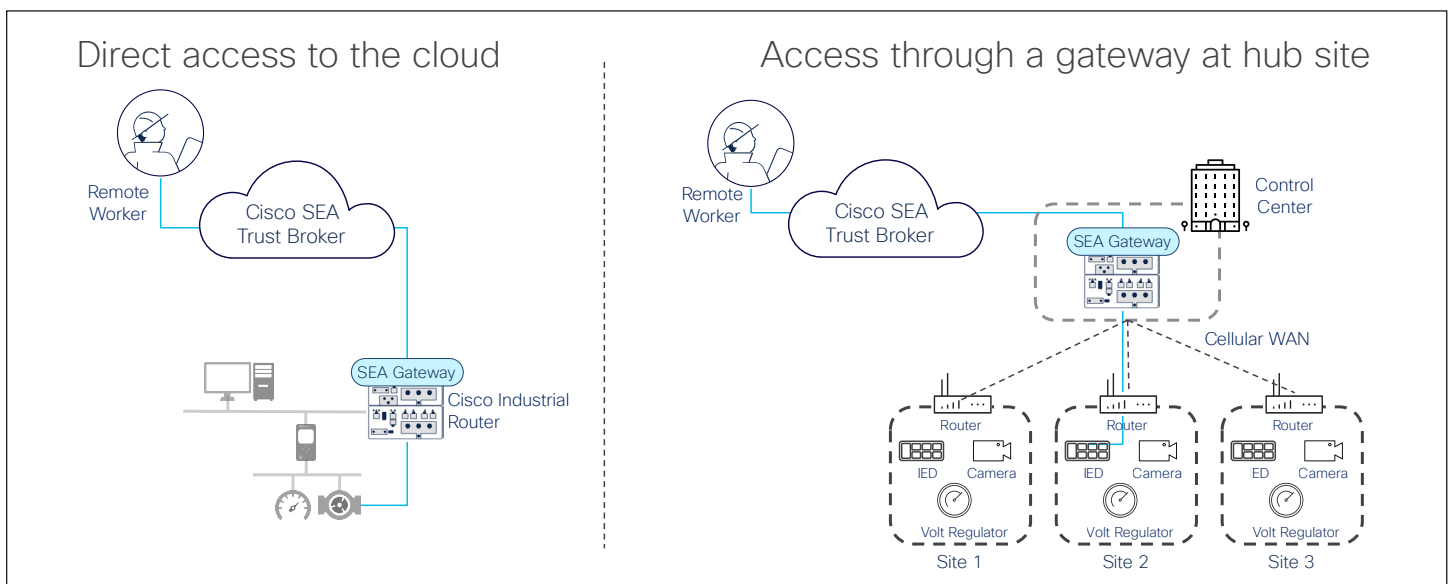


Figure 5. Architecture options for remote access in distributed field networks

- In plant industrial networks**, such as those in manufacturing or chemical plants, for instance, the SEA gateway software can be installed in the IDMZ on enterprise-class switches such as the [Cisco Catalyst™ 9300 Series](#), aligning with existing security mechanisms that may already exist. However, the true benefits come when installing the SEA gateway software in [Cisco Industrial Ethernet switches](#) connecting OT assets at Purdue levels 1 and 2 throughout the plant network. This greatly simplifies the task of configuring remote access to assets sitting behind NAT boundaries, as there is no need to expose these private IP addresses to the IDMZ, eliminating a potential attack vector.

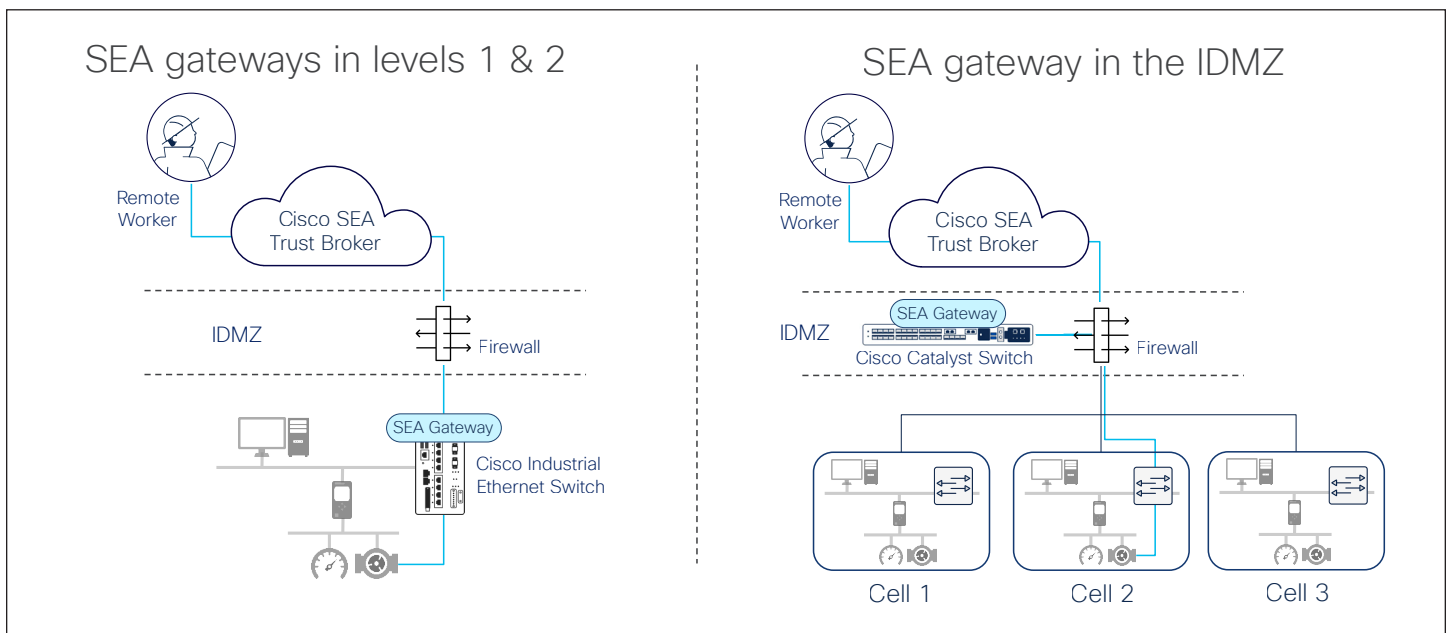


Figure 6. Architecture options for remote access in plant networks

Firewalls and segmentation policies need to be configured only once to allow SEA gateways to access the SEA trust broker, eliminating the need for error-prone configurations every time a new asset needs to be remotely accessed. Isolated zones remain protected, as only communications authorized by the SEA trust broker are allowed into the zone. The OT network itself does not need connectivity to the cloud, as the SEA gateway software can connect to the cloud-based trust broker using its own VLAN interface. In addition, the SEA gateway connection to the cloud broker can go through an existing web proxy in the IDMZ.

Gateway deployment and management

A typical SEA deployment might involve a large number of gateways, raising questions about deploying and managing the solution at scale. Cyber Vision's SEA makes it simple by centralizing gateway deployment, management, and update. It offers two methods, one generic for all hosting platforms and one specific to routers that are part of an SD-WAN architecture:

- **SEA gateway activation through the SEA trust broker:** Deploying the SEA gateway software on supported Cisco switches and routers can be done in a centralized manner from the SEA cloud-based trust broker portal.
- **SEA gateway activation through Cisco Catalyst SD-WAN Manager:** Deploying the SEA gateway software on supported Cisco industrial routers can be done through Catalyst SD-WAN Manager, which also enables administrators to configure these routers.

Enhancing existing jump servers with zero-trust controls

Some organizations might not yet be ready to deviate from their traditional remote access solution based on jump servers, such as engineering workstations placed throughout the industrial network. Vendors use RDP over a VPN connection to access one of these workstations and perform remote maintenance of their machines. Cyber Vision's SEA can help secure access to these jump servers, adding advanced user authentication, access control, and auditing capabilities.

With Cyber Vision's SEA, remote vendors will now connect to the SEA trust broker using a web browser where they are authenticated using MFA. A SEA gateway installed in the IDMZ will proxy the remote access session to the jump server, where an RDP session can be initiated as before. In this architecture, user management is centralized, multifactor authentication can be enforced, access can be restricted to specific schedules, sessions are logged and can be recorded, and firewall configuration is simplified, as only the SEA gateway needs cloud access.

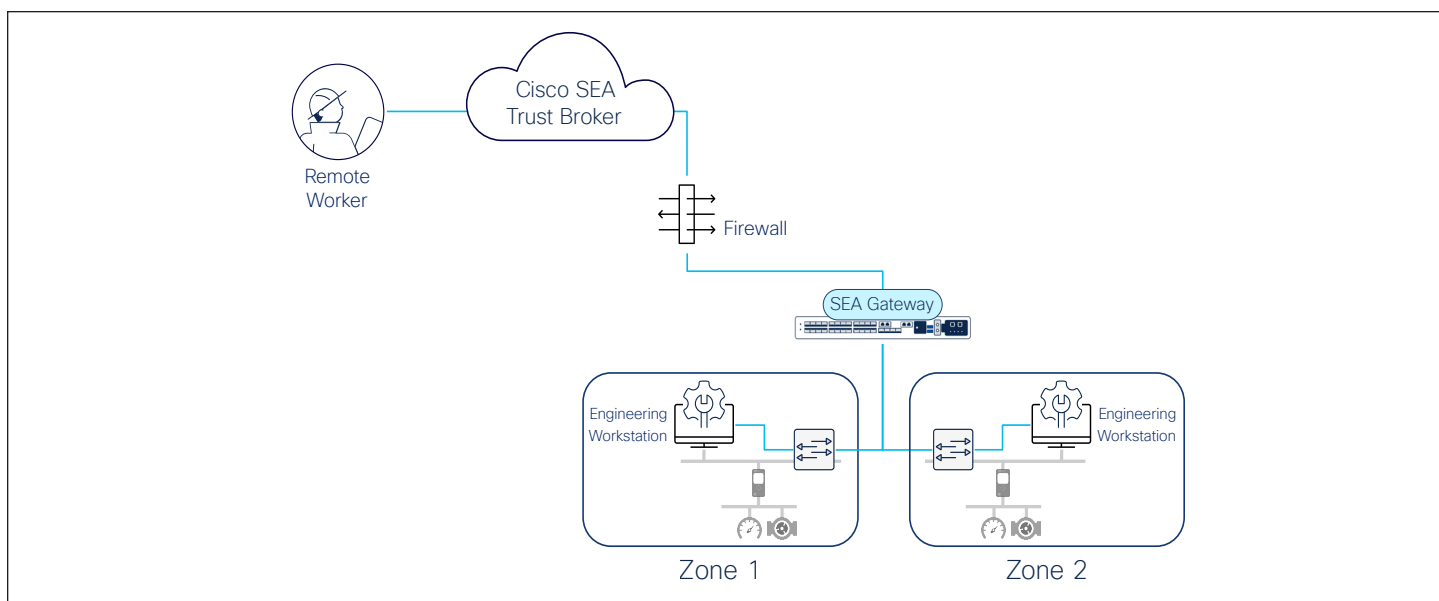


Figure 7. Using Cyber Vision's SEA with existing jump servers

Benefits of a cloud-based ZTNA trust broker

There are many misconceptions about the cloud, especially its use in operational environments. However, remote access is a solution that cannot avoid connectivity. Remote users originate outside of the network. If not using a cloud-based trust broker, operators must maintain policy across every site individually. If a security administrator wants to make an organization-wide policy change, they must make sure each firewall boundary is configured correctly to enforce this change.

Because SEA first brings all remote users to a trusted cloud resource, it gives security administrators a single point of control for those users. Identity can be verified, device posture can be checked, geolocation can be looked up, and any other policy controls can be enforced. The organization's firewall simply needs a single rule allowing communications between the SEA gateway and the cloud broker, rather than opening multiple connections from different users, introducing risks due to poor firewall rules management.

The ZTNA trust broker is the main component of the solution. It is the central location for defining and enforcing policies for all sites. It makes secure remote access much easier to manage. Running the trust broker in Cisco's elastic cloud resources enables high availability and performance. It also benefits from a dedicated team of security experts to help ensure that the solution is always up to date and uses state-of-the-art security technologies to prevent breaches.

Summary

Industrial cybersecurity demands architectural approaches that address the unique requirements of OT environments while transcending the limitations of conventional remote access. Traditional solutions introduce fundamental vulnerabilities through broad network access, complex management requirements, and architectural limitations that are incompatible with industrial operational needs.

Cisco Cyber Vision's Secure Equipment Access delivers transformative capability with a distributed architecture that fuses the ZTNA gateway with the network. This approach offers operations teams a self-service, easy-to-use, simple-to-deploy remote access solution while providing granular, policy-driven access controls aligned with the organization's security and regulatory compliance requirements.

As industrial organizations embrace digital transformation, the distributed zero-trust architecture provides a scalable, secure foundation for remote access that addresses contemporary threat landscapes while supporting operational innovation and efficiency optimization.

For over 20 years, Cisco has been helping industrial organizations around the globe digitize their operations by developing a market-leading networking and security portfolio that is purpose-built for industrial use cases. Our deep understanding of operational technology requirements, plus our comprehensive networking and cybersecurity portfolio, is a rare combination.

Cyber Vision’s Secure Equipment Access is part of the [Cisco Industrial Threat Defense](#) solution designed to help IT, OT, and security teams work together to protect industrial operations. Operations teams will appreciate the ease of use and simple deployment, as well as the broad support for various Industrial Automation and Control System (IACS) vendors and protocols. IT network managers will appreciate the ability to apply skills, technology, and applications already deployed in the enterprise when looking to integrate production environments. Security teams will have visibility into industrial assets and security events with context enriched by control engineers.

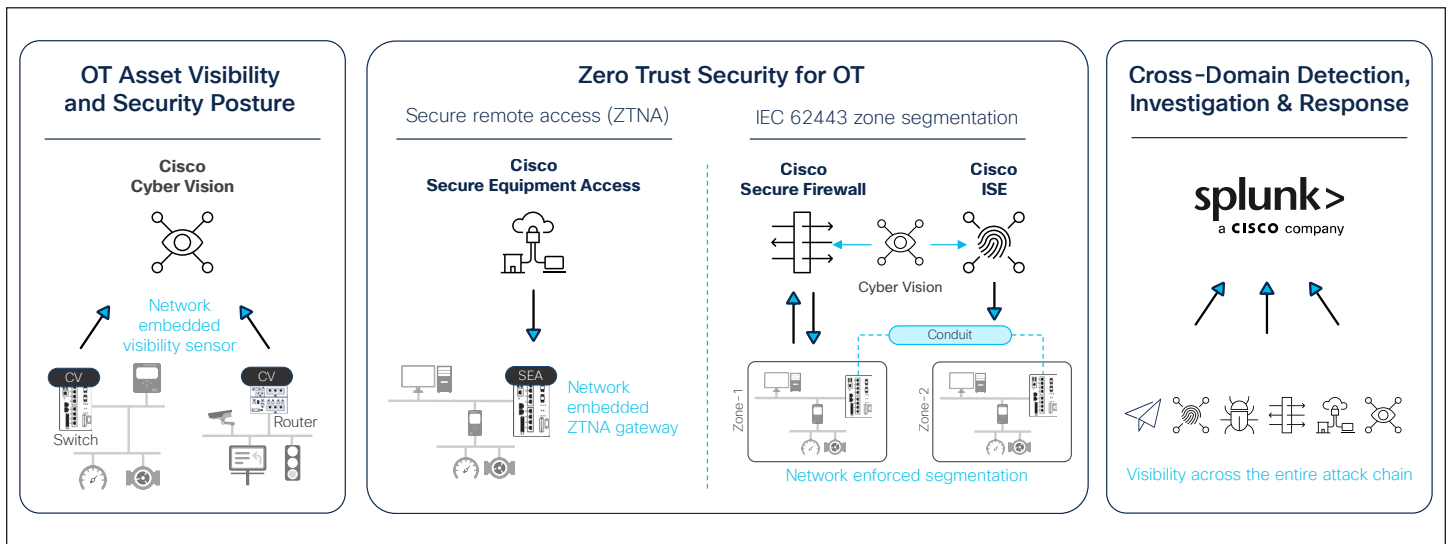


Figure 8. Cisco Industrial Threat Defense

Talk to a [Cisco sales representative](#) or channel partner about how Cisco can help you secure your field industrial network. Visit cisco.com/go/iotsecurity or cisco.com/go/sea to learn more.