Cisco Secure Equipment Access

Zero-Trust Network Access (ZTNA) for operational environments

Remote access is key to being able to configure, manage, and troubleshoot Operational Technology (OT) assets without time-consuming and costly site visits. Enabling secure remote access at scale can be a daunting task: sites might be highly distributed, and assets are often sitting behind Network Address Translation (NAT) boundaries. Configuring firewall rules and deploying dedicated gateway hardware puts an extra burden on IT and OT teams.

With Secure Equipment Access (SEA), Cisco is solving these challenges. It combines all the benefits of a Zero-Trust Network Access (ZTNA) solution with a network architecture that makes it simple to deploy at scale in operational environments. There is no dedicated hardware to install and manage. No complex firewall rules to configure and maintain. The Cisco® industrial switches or routers that connect your OT assets now also enable remote access to them. And it features comprehensive security capabilities, with advanced cybersecurity controls and easy-to-build policies based on identities and contexts.

Benefits

- **Boosts operational efficiency:** Empower operations teams to easily gain remote access to OT assets, even those behind NAT boundaries.
- **Simple to install and scale:** Stop struggling with dedicated appliances and complex firewall setups. Cisco SEA is embedded in switches and routers.
- **Offers least-privilege access:** Allow select users to access only specific devices, using only certain protocols, and only at defined times.
- **Enforces strong security controls:** Authenticate users with MFA and SSO. Verify their security posture. Block asset discovery and lateral movement.
- **Takes control back:** Record sessions and build audit trails for investigation and compliance. Join and terminate active sessions.

Scalable, zero-trust remote access to OT assets

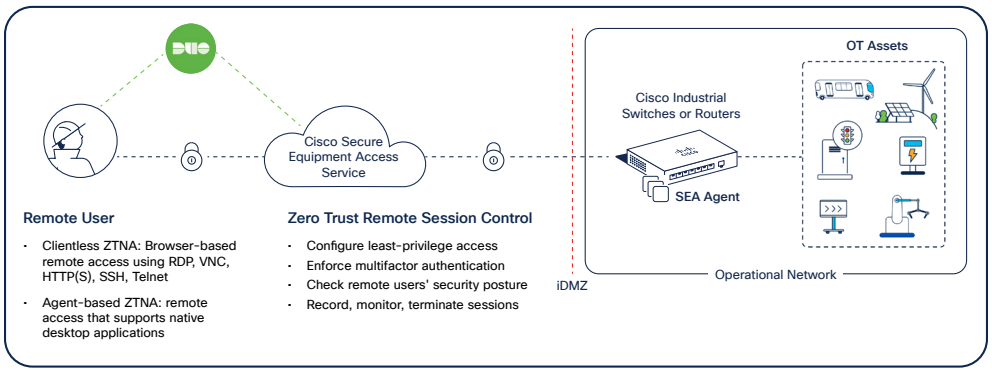

Figure 1. Cisco SEA is a hybrid-cloud zero-trust network access solution built for OT workflows

For more information

Talk to a Cisco sales representative or channel partner about how Cisco can help you secure your industrial operations. Visit cisco.com/go/sea and cisco.com/go/iotsecurity to learn more.

Zero-trust network access made for OT

Help ensure that employees, vendors, and contractors can access only devices you choose, using only the protocols you specify, and only on the day and time you allow. Cisco Secure Equipment Access enforces strong security controls such as MFA, SSO, posture check, and more. It centralizes configuration of remote access policies in the cloud to empower operations administrators to easily create credentials and avoid delays that could impact production uptime.

Secure remote access built into switches and routers

Distributing the ZTNA gateway functionality anywhere in the network lets you remotely access every asset, regardless of its IP address or your NAT strategy. The switch or router that connects assets now also provides secure remote access. It can also enforce microsegmentation policies to prevent lateral movement if the asset is used as a jump host. Only Cisco offers such an advanced and secure remote access capability today.

C45-3964499-00 10/23